TERMO DE REFERÊNCIA

Contratação de solução de gerenciamento unificado de ameaças (UTM) e de rede WAN definida por software (SD-WAN) composta por hardware, software, licenciamento, treinamento, suporte, garantia e implantação.

Elaborado por:	Título do Documento:	Versão:	Revisão:
EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO	**TERMO DE REFERÊNCIA**	**2**	**2**
Processo:		Data:	
PA-PRO-2019/04878		**05/12/2019**	

ÍNDICE

1. DEFINIÇÃO DO OBJETO (ART. 18, §3º, I)

Contratação de solução de gerenciamento unificado de ameaças (UTM) e de rede WAN definida por software (SD-WAN) composta por hardware, software, licenciamento, treinamento, suporte, garantia e implantação.

2. FUNDAMENTAÇÃO DA CONTRATAÇÃO (ART. 18, §3º, II)

2.1. MOTIVAÇÃO DA CONTRATAÇÃO (ART. 18, §3º, II, A)

Necessidade de prover uma camada adicional de segurança em cada unidade judiciária onde será implantada a solução, permitindo maior visibilidade do tráfego gerado em cada unidade, além da possibilidade de mitigar ameaças e riscos de segurança tanto no que se refere a sistemas e serviços de TI internos, além de ameaças externas que possam comprometer a confidencialidade, a integridade e a disponibilidade dos serviços oferecidos.

Soma-se ao fato supramencionado, a necessidade de gerenciar a conectividade WAN das unidades judiciárias de forma proativa, através da priorização de demandas, melhor utilização dos links WAN e maior disponibilidade dos serviços demandados, com o objetivo de permitir que a atividade fim do Tribunal seja realizada com maior qualidade.

2.2. OBJETIVOS A SEREM ALCANÇADOS POR MEIO DA CONTRATAÇÃO (ART. 18, §3º, II, B)

Melhorar a segurança da informação de nível operacional no âmbito do TJPA, auxiliando na prevenção de riscos e ameaças, tanto internas quanto externas, além da mitigação dos efeitos de potenciais ataques virtuais que possam comprometer os dados institucionais tratados no Tribunal. Melhora da experiência do usuário na utilização de serviços que demandam conectividade WAN, além da redução de custos no que diz respeito a possibilidade de contratação de diversos tipos de conectividade WAN (MPLS, Internet, 4G, etc), o que possibilita pelas escolhas mais vantajosas para a Administração.

2.3. BENEFÍCIOS DIRETOS E INDIRETOS RESULTANTES DA CONTRATAÇÃO (ART. 18, §3º, II, C)

O principal objetivo do presente projeto é melhorar a experiência na utilização dos serviços e sistemas de TI para os magistrados e servidores que trabalham em unidades judiciárias localizadas no interior do Estado e que carecem de melhores condições de trabalho no que se refere à conectividade WAN, possibilitando redução de custos para a Administração.

Como benefícios diretos, cita-se a possibilidade de garantir maior disponibilidade dos serviços e sistemas de TI, já que a solução de UTM/SD-WAN permite a utilização e o gerenciamento de diversos links WAN de diversas tecnologias diferentes (MPLS, Internet, 4G, etc) ao mesmo tempo, permitindo mitigar problemas de conectividade nas unidades de forma transparente para usuários e magistrados. Também a segurança operacional é um benefício direto, pois é possível mitigar diversas modalidades de ataques cibernéticos, o que auxilia na proteção de dados sensíveis que trafegam dentro da infraestrutura de TI do Tribunal.

Como benefício indireto, cita-se a possibilidade de melhoria na produtividade dos usuários internos da rede do TJPA e a entrega de serviços com maior valor agregado pelo Tribunal.

2.4. ALINHAMENTO DA CONTRATAÇÃO AO PLANEJAMENTO ESTRATÉGICO (ART. 18, §3º, II, D)

Do Planejamento Estratégico do Poder Judiciário 2015/2020, em seu **MACRODESAFIO 11: MELHORIA DA INFRAESTRUTURA E GOVERNANÇA DE TIC**, temos a **INICIATIVA ESTRATÉGICA 11.1: MODERNIZAÇÃO DA INFRAESTRUTURA DE TIC**, que orienta para "Garantir a evolução, melhoria e expansão contínuas dos recursos tecnológicos disponíveis aos magistrados e servidores, buscando aumentar a produtividade, reduzir custos e melhorar a qualidade dos serviços prestados; Promover a melhoria da qualidade da guarda, tráfego e usos de dados; Fortalecer o fluxo e o armazenamento de dados; bem como garantir uma rede eficiente de transmissão e troca de dados, célere e confiável, entre as unidades judiciárias e administrativas da Justiça Paraense, em todos os níveis."

Nessa mesma iniciativa estratégica, destaca-se a **AÇÃO 11.1.1: Reestruturar a arquitetura de rede lógica das unidades judiciárias e administrativas**, que prevê a necessidade de "remodelar a infraestrutura das redes de comunicação de dados e voz das unidades judiciárias e administrativas da RMB e do interior, visando otimizar a utilização dos recursos tecnológicos, adequar o desempenho e a disponibilidade dos sistemas de TIC aos respectivos acordos de nível de serviço, garantir a conformidade com os padrões mínimos de segurança e de gerenciamento de serviços, mitigar o aprisionamento a fornecedores, além de reduzir os custos financeiros e operacionais", contemplada na **ETAPA 11.1.1.5: Implantar solução de rede "WAN definida por software (SD-WAN)"** e **ETAPA 11.1.1.6: Implantar "solução de gerenciamento unificado de ameaças" (UTM).**

É importante destacar por fim, que a solução em estudo está alinhada à recente Resolução nº. 211/2015 do Conselho Nacional de Justiça – CNJ, que instituiu a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD) para o sexênio 2015-2020, em harmonia com os macrodesafios do Poder Judiciário, em especial o que estabelece a "melhoria da infraestrutura e governança de TIC". Este alinhamento fica comprovado pela leitura do Art. 24 da referida ENTIC-JUD, abaixo transcrito, cuja execução prevê que todas as unidades do TJPA possuam enlaces de comunicação com capacidade suficiente para o desempenho satisfatório da atividade jurisdicional, bem como ambientes e soluções de alta disponibilidade, redundantes e capazes de atender à continuidade do negócio em situações adversas.

> *"Art. 24. O nivelamento da infraestrutura de TIC deverá obedecer aos seguintes requisitos mínimos: (...)*
>
> *V – links de comunicação entre as unidades e o órgão suficientes para suportar o tráfego de dados e garantir a disponibilidade exigida pelos sistemas de informação, especialmente o processo judicial, com o máximo de comprometimento de banda de 80%; (...)*
>
> *VII – 1 (um) ambiente de processamento central (DataCenter) com requisitos mínimos de segurança e disponibilidade (...) que abrigue (...) ativos de rede centrais, para maximizar a segurança e a disponibilidade dos serviços essenciais e de sistemas estratégicos do órgão.*

2.5. REFERÊNCIA AOS ESTUDOS PRELIMINARES DA STIC (ART. 18, §3º, II, E)

Este Termo de Referência foi elaborado considerando o Documento de Oficialização da Demanda (DOD) e os demais documentos produzidos na fase de Estudos Preliminares (a saber: "Análise de Viabilidade da Contratação", "Sustentação do Contrato", "Estratégia para Contratação" e "Análise dos Riscos da Contratação"), todos juntados ao expediente **PA-PRO-2019/04878**.

2.6. RELAÇÃO ENTRE A DEMANDA PREVISTA E A CONTRATADA (ART. 18, §3º, II, F)

Entende-se que as demandas previstas e projetadas pelo Grupo de Arquitetura Tecnológica da SECINFO do TJPA para serem atendidas pela solução a ser implantada, decorrente de eventual contratação, serão atendidas em sua plenitude, respeitando-se os devidos pressupostos de previsibilidade em projetos de TIC. Ressalta-se ainda, que a **ETAPA 11.1.1.5: Implantar solução de rede "WAN definida por software (SD-WAN)"** e **ETAPA 11.1.1.6: Implantar "solução de gerenciamento unificado de ameaças" (UTM)** do Plano de Gestão 2019-2021, que possuem como meta, cada uma, atender 50 unidades judiciárias do TJPA, será atendida pois a solução que pretende-se adquirir poderá atender 52 unidades judiciárias

2.7. ANÁLISE DE MERCADO DE TIC (ART. 18, §3º, II, G)

2.7.1. SOLUÇÕES DISPONÍVEIS E/OU CONTRATADAS POR OUTROS ÓRGÃOS

O Grupo de Arquitetura Tecnológica do TJPA teve a oportunidade de visitar entidades públicas e privadas em Belém e fora de Belém (PA-MEM-2019/18370 e PA-MEM-2019/30280) que já haviam implantado em seus ambientes tecnológicos, dentro das peculiaridades de cada entidade, a solução de UTM/SD-WAN, como por exemplo, o Supremo Tribunal Federal (STF), o Tribunal de Contas da União (TCU), a Procuradoria Geral da União (PGR), o Sistema de Cooperativas de Crédito do Brasil (SICOOB) e o Banco da Amazônia (BASA). Sem realizar visitas técnicas, também foram avaliadas outras soluções, como a do Ministério do Planejamento, Desenvolvimento e Gestão (MPDG), o Banco do Nordeste (BNB), a Polícia Civil do Distrito Federal (PCDF), o Tribunal de Contas do Estado do Pará (TCE/PA) e Companhia Brasileira de Trens Urbanos (CBTU).

Através das visitas técnicas e das análises das soluções, houve a oportunidade de avaliar duas modalidades de solução de UTM/SD-WAN, que foram a modalidade tradicional, onde a entidade adquiriu equipamentos próprios e a implantação e administração da solução fica a cargo da mesma, e a modalidade baseada em serviços, onde os equipamentos são "terceirizados", normalmente vendidos como um serviço adicional a contratação de links de internet através das operadoras de telecomunicações, onde as operadoras administravam a solução de UTM/SD-WAN. Por exemplo, no Tribunal de Contas da União, a solução UTM/SD-WAN foi contratada através da modalidade serviços e administrada pela operadora vencedora, juntamente com links MPLS redundantes vindo das capitais para o prédio sede localizado em Brasília. Abaixo, na figura 1, consta a topologia desenhada pelo TCU.

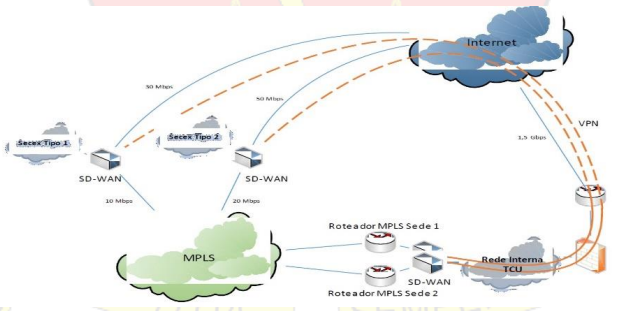

Figura 1 - Topologia da solução de UTM/SD-WAN do TCU (Fonte: Pregão Eletrônico 93/2018/TCU).

Outro exemplo, no Banco do Nordeste, a solução UTM/SD-WAN também foi contratada através da modalidade serviços e administrada pela operadora vencedora, juntamente com links MPLS e de internet vindo das

unidades distribuídas para os sites primário e secundário do BNB, localizados em Fortaleza. Abaixo, na figura 2, consta a topologia desenhada pelo BNB.

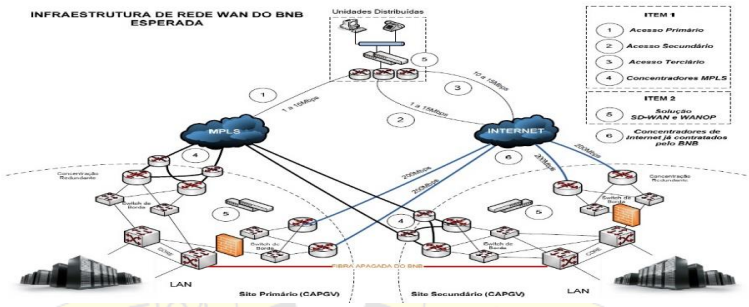

Figura 2 - Topologia da solução de UTM/SD-WAN do BNB (Fonte: Pregão Eletrônico 44/2018/BNB).

Comparada as duas modalidades e avaliando as peculiaridades dos dados que trafegam nas redes de comunicação do TJPA, foi tomada uma decisão estratégica pelo TJPA onde a modalidade de solução adotada seria a tradicional, devido a sensibilidade dos dados que trafegam através das redes de comunicação de dados do TJPA, não seria possível permitir que a solução fosse administrada por terceiros, onde serviços críticos poderiam ficar expostos de maneira desnecessária, decidiu-se que a administração desta solução ficaria a cargo da equipe técnica do TJPA.

Também por questões estratégicas, foi constatado que a contratação deste serviço juntamente com links de internet poderia resultar em um aprisionamento a fornecedores específicos e, por consequência, em maiores custos para a Administração.

Adicionalmente, dentro da modalidade tradicional, existem duas abordagens: a abordagem “On-Premise” onde a gerência dos equipamentos se dá através de software tradicional, implantado nas dependências do demandante, e a abordagem em nuvem, onde a gerência dos equipamentos se dá através de um sistema de gerência em nuvem, fora das dependências do cliente. Por questões estratégicas e para prevenir possíveis vazamentos de dados para fora das dependências do TJPA escolheu-se, dentro da modalidade tradicional, a abordagem “On-Premise”. Abaixo, na figura 3, um esboço da topologia de UTM/SD-WAN nas unidades judiciárias do Tribunal.

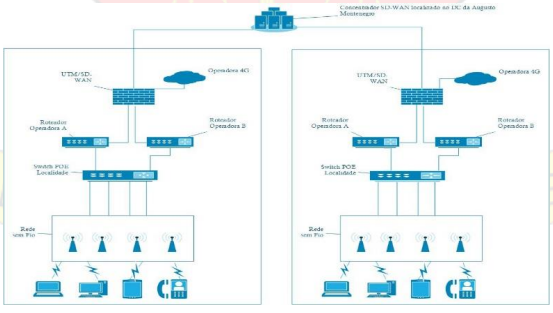

Figura 3 – Esboço de Topologia da solução de UTM/SD-WAN do TJPA nas unidades judiciárias.

2.7.2. DEFINIÇÃO E JUSTIFICATIVA DA ESCOLHA DA SOLUÇÃO

Após análise de diversas soluções oferecidas pelo mercado, incluindo visitas técnicas em entidades públicas e privadas que já possuem a referida solução em funcionamento, respeitadas as peculiaridades de cada entidade, análises feitas pelo Grupo de Arquitetura, em conjunto com as equipes técnicas do TJPA, além da recomendação emitida por entidades de nível internacional responsáveis pela análise de soluções de TIC, como o Gartner e o NSS Labs, a disponibilidade de atas de registro de preço para adesão imediata e o custo total em relação ao orçamento disponível para aquisição, além do custo benefício entre o valor que será pago e o que a solução oferece (capacidade dos equipamentos, tempo de licenciamento, suporte e garantia, implantação, treinamento, SLA para suporte e garantia, dentre outras características), a solução do fabricante Fortinet, adquirida pelo Ministério do Planejamento, Desenvolvimento e Gestão (MPDG) através do Pregão Eletrônico 05/2017/MPDG foi escolhida.

Sendo de reconhecida qualidade, a solução traz benefícios importantes que podem auxiliar na manutenção e aumento da disponibilidade dos serviços oferecidos pelo TJPA que utilizam circuitos WAN, fazendo parte de um conjunto de soluções que tem como objetivo melhorar a experiência de trabalho dos magistrados e servidores do Tribunal.

Ainda nesse sentido, a solução escolhida possui um conjunto de serviços que se mostra vantajoso em relação ao preço que será pago, como garantia, suporte e licenciamento por 60 meses, o que fornece um tempo de vida útil compatível com o tempo de vida médio para as soluções de TI existentes no mercado.

2.8. NATUREZA DO OBJETO (ART. 18, §3º, II, H)

Os serviços objeto da contratação em questão possuem **características comuns de mercado**, claramente definidas nas SEÇÕES 2.3 – DETALHAMENTO DOS REQUISITOS TÉCNICOS E DE NEGÓCIO e 5.2 – DESCRIÇÃO DA SOLUÇÃO da "ANÁLISE DE VIABILIDADE DA CONTRATAÇÃO" já mencionada, consoante o contido no parágrafo único do art. 1º da Lei 10.520/2002.

Adicionalmente, admite-se que a execução do objeto possui **natureza continuada**, cujo escopo prevê o fornecimento em um período de até 60 (sessenta) meses.

2.9. PARCELAMENTO E ADJUDICAÇÃO DO OBJETO (ART. 18, §3º, II, I)

2.9.1. PARCELAMENTO DOS ITENS QUE COMPÕE A SOLUÇÃO DE TIC

No presente caso, por tratar-se de processo de adesão as Atas de Registro de Preço nº 11/2018-MPDG e nº 03/2019/MPDG, não caberá a realização de Licitação, não havendo o que se falar em relação ao parcelamento do objeto.

Adicionalmente, em função das características próprias da solução, que não pode prescindir do fornecimento de todos os componentes, funcional e estrategicamente indissociáveis entre si para sua integração completa, conclui-se pelo não parcelamento do objeto especificado.

2.9.2. FORMA DE ADJUDICAÇÃO DA CONTRATAÇÃO

Por tratar-se de processo de adesão as Atas de Registro de Preço nº 11/2018-MPDG e nº 03/2019/MPDG, faz-se necessário que a adjudicação se dê com a empresa NCT INFORMATICA LTDA, vencedora do certame licitatório conduzido pelo MPDG, e signatária das ARPs mencionadas.

2.10. FORMA E CRITÉRIO DE SELEÇÃO DO FORNECEDOR (ART. 18, §3º, II, J)

A aquisição se dará por intermédio de adesão as Atas de Registro de Preço 11/2018-MPDG e 03/2019-MPDG, fruto do Pregão Eletrônico 05/2017/MPDG, conforme o exposto nos subitens da Seção 3 do documento "Análise de Viabilidade da Contratação", onde por questões estratégicas e de custo, foram apresentadas contratações efetuadas por outros órgãos públicos em situações, resguardadas as peculiaridades, não tão vantajosas quanto aquela que o TJPA pretende adquirir. Pelos motivos expostos, não cabe a realização de procedimento licitatório.

2.11. IMPACTO AMBIENTAL DECORRENTE DA CONTRATAÇÃO (ART. 18, §3º, II, K)

Considerando a análise apresentada nos Estudos Preliminares referenciados na SEÇÃO 2.5 deste TERMO DE REFERÊNCIA, não foram identificados riscos ambientais significativos, em decorrência do fornecimento dos bens e serviços da solução de UTM/SD-WAN.

A probabilidade de ocorrência dos impactos estudados (geração de resíduos sólidos, poluição sonora e poluição visual) poderá ser facilmente mitigada através de realização de vistorias técnicas durante o período da prestação dos serviços.

Neste sentido, é importante que todos os serviços previstos atendam rigorosamente às normas técnicas vigentes e os padrões adotados pelo TJPA. Assim como, estes serviços deverão ser entregues sem instalações provisórias e com os ambientes livres de entulho ou sujeira, sendo a CONTRATADA responsável por sua limpeza.

Ademais, é desejável que os equipamentos, ferramentas e materiais empregados na execução dos serviços em cena estejam em conformidade com a diretiva RoHS (*Restriction of Hazardous Substances*), relacionada à preservação do meio ambiente, por meio da restrição do uso de metais pesados (mercúrio (Hg), chumbo (Pb), cromo hexavalente (Cr(VI)), cádmio (Cd), bifenil-polibromados (PBBs), éteres difenil-polibromados (PBDEs), etc.) durante a fabricação.

2.12. CONFORMIDADE COM NORMAS TÉCNICAS E LEGAIS (ART. 18, §3º, II, L)

Os procedimentos legais para a renovação contratual pretendida obedecerão, integralmente:

a) À Constituição da República Federativa do Brasil, promulgada em 5 de outubro de 1988;
b) Às disposições contidas na Lei Federal nº 8.666, de 21 de junho de 1993, com as respectivas alterações posteriores;
c) Às disposições contidas na Lei Federal nº 9.784, de 29 de janeiro de 1999, com as respectivas alterações posteriores;
d) À Resolução do CNJ nº 182, de 17 de outubro de 2013;
e) Às disposições contidas na Lei Federal nº 9.472, de 16 de julho de 1997, com as respectivas alterações posteriores.

Quando a conformidade técnica, a contratação em estudo deverá obedecerá às seguintes normas:

a) **ITU-T G.703 (11/2011)** – *Physical/electrical characteristics of hierarchical digital interfaces*;
b) **ANSI/TIA/EIA-568-B.3** – Commercial Building Telecommunications Cabling Standard – Part 3: *Optical Fiber Cabling components standard*;

c) **ANSI/TIA/EIA-568-B.3-1** – *Commercial Building Telecommunications Cabling Standard – Part* 3: *Optical Fiber Cabling components standard – Addendum* 1 – *Additional Transmission Performance Specifications for* 50/125 µm *Optical fiber cables*;

d) **ANSI/TIA/EIA-569-B** – *Commercial Building Standard for Telecommunications Pathways and Spaces*;

e) **RESOLUÇÃO ANATEL nº. 242, de 30/11/2000** – Regulamento para certificação e homologação de produtos para telecomunicações;

2.13. OBRIGAÇÕES CONTRATUAIS (ART. 18, §3º, II, M)

2.13.1. OBRIGAÇÕES DA EMPRESA CONTRATADA:

2.13.1.1. Cumprir fielmente o instrumento contratual, de modo que os serviços sejam realizados com segurança e perfeição, executando-os sobre sua inteira e exclusiva responsabilidade, de acordo com as Especificações Básicas constantes neste Termo de Referência;

2.13.1.2. Fornecer os recursos materiais e humanos necessários à execução dos serviços objeto do contrato, responsabilizando-se por todas as despesas e encargos, de qualquer natureza, exceto quando se tratar de atividades expressamente atribuídas ao TJPA, segundo a lei, o edital ou o contrato;

2.13.1.3. Designar preposto responsável pelo atendimento ao TJPA, devidamente capacitado e com poderes para decidir e solucionar questões pertinentes ao objeto do contrato;

2.13.1.4. Manter atualizados os dados bancários para os pagamentos e os endereços, telefones e e-mail para contato;

2.13.1.5. Solicitar, em tempo hábil, todas as informações de que necessitar para o cumprimento das suas obrigações contratuais, exceto aquelas que são de fornecimento obrigatório pelo TJPA, nos termos do contrato.

2.13.1.6. Prestar os esclarecimentos solicitados pelo TJPA, no prazo máximo de 05 (cinco) dias quanto à execução dos serviços;

2.13.1.7. Acatar integralmente as exigências do TJPA quanto à execução dos serviços, inclusive providenciando a imediata correção das deficiências apontadas;

2.13.1.8. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento deste contrato;

2.13.1.9. Remeter as correspondências destinadas ao TJPA e decorrentes da execução deste contrato à atenção da Secretaria de Informática – SECINFO, mais especificamente ao gestor do Contrato, citando o número do contrato a que se referem;

2.13.1.10. Manter, durante toda a execução dos serviços, as condições de habilitação e qualificação exigidas na contratação, informando ao TJPA a superveniência de eventual ato ou fato que modifique aquelas condições;

2.13.1.11. Efetuar o pagamento de multas, indenizações ou despesas impostas por órgãos fiscalizadores da atividade da CONTRATADA, bem como suportar o ônus decorrente de sua repercussão sobre o objeto deste contrato;

2.13.1.12. Efetuar o pagamento de seguros, impostos, taxas e serviços, encargos sociais e trabalhistas, indenizações por acidente de trabalho e quaisquer despesas decorrentes de sua condição de empregadora, referente aos serviços, inclusive licença em repartições públicas, registros, publicação e autenticação do contrato e dos documentos a ele relativos, se necessário;

2.13.1.13. Fiscalizar o cumprimento do objeto do contrato, cabendo-lhe integralmente os ônus daí decorrentes, necessariamente já incluídos no preço contratado, independentemente da fiscalização exercida pelo TJPA;

2.13.1.14. Assegurar ao TJPA o direito de propriedade intelectual dos produtos desenvolvidos, inclusive sobre as eventuais adequações e atualizações que vierem a ser realizadas, logo após o recebimento de cada parcela, de forma permanente, permitindo ao TJPA distribuir, alterar e utilizar estes sem limitações;

2.13.1.15. Assegurar ao TJPA os direitos autorais da solução do projeto, de suas especificações técnicas, da documentação produzida e congêneres, e de todos os demais produtos gerados na execução do contrato, inclusive aqueles produzidos por terceiros subcontratados, ficando proibida a sua utilização sem que exista autorização expressa do TJPA, sob pena de rescisão contratual e multa;;

2.13.1.16. Comprovar a origem de bens importados e a quitação dos tributos de importação a eles referentes, que deve ser apresentada no momento da entrega, sob pena de rescisão contratual e multa;

2.13.1.17. São de responsabilidade da CONTRATADA eventuais transtornos ou prejuízos causados ao TJPA, provocados por imprudência, imperícia, negligência, atrasos ou irregularidades cometidas na execução dos serviços contratados;

2.13.1.18. O TJPA fica autorizado a descontar o valor correspondente aos danos sofridos da garantia do Contrato ou dos pagamentos devidos à CONTRATADA.

2.13.2. OBRIGAÇÕES DO TJPA:

2.13.2.1. Fornecer à CONTRATADA as informações e os esclarecimentos necessários a execução dos serviços objeto do contrato;

2.13.2.2. Indicar, até o 5º dia útil da vigência do contrato, o nome dos servidores responsáveis pela gestão e fiscalização do contrato e pelo recebimento dos serviços executados;

2.13.2.3. Efetuar os pagamentos devidos na forma prevista neste contrato.

3. ESPECIFICAÇÃO TÉCNICA DETALHADA DO OBJETO (ART. 18, §3º, III)

3.1. QUANTITATIVO DE SERVIÇOS (QUADRO RESUMO)

Tabela 1 - Quadro resumo de quantitativos de serviços.

#	DESCRIÇÃO	QTD.
1.	Firewall Multifuncional Tipo 1 com suporte, garantia e licenciamento por 60 meses	58
2.	Firewall Multifuncional Tipo 1 com suporte, garantia e licenciamento por 60 meses	4
3.	Treinamento Oficial (Voucher para 5 pessoas)	2

3.2. ESPECIFICAÇÃO TÉCNICA DETALHADA DOS SERVIÇOS

As especificações detalhadas dos produtos e serviços a serem entregues constam do **ANEXO B – ESPECIFICAÇÃO TÈCNICA DOS PRODUTOS E SERVIÇOS** deste Termo de Referência.

3.3. PAPÉIS DOS PRINCIPAIS ATORES ENVOLVIDOS (ART. 18, § 3º, III, A, 1)

A Equipe de Gestão da Contratação, responsável pela gestão e pela fiscalização da execução contratual, consoante às atribuições regulamentares, é atualmente formada por pelos atores abaixo relacionados, especialmente designados pelo TJPA, de acordo com o estabelecido no Art. 67 da Lei Federal nº 8.666/1993, e no Art. 2º, XII da Resolução nº. 182/2013/CNJ:

a) **GESTOR DO CONTRATO:** Gestor máximo da área técnica (Secretaria de Informática), **Sr. DIEGO BAPTISTA LEITÃO**, Secretário de Informática, matrícula 123030;

b) **FISCAL TÉCNICO:** servidor representante da Área de Tecnologia da Informação e Comunicação (TIC), especialmente designado pelo TJPA, para acompanhamento e fiscalização contratual quanto aos aspectos técnicos da solução. **Sr. DENISON LEANDRO SERRÂO SOARES**, Analista Judiciário, Chefe do Serviço de Infraestrutura de Redes – SIR/CST/SECINFO, matrícula 162311;

c) **FISCAL ADMINISTRATIVO:** servidor representante da Área Administrativa, especialmente designado pela respectiva autoridade competente, para acompanhar e fiscalizar o contrato quanto aos aspectos administrativos da execução, especialmente os referentes ao acompanhamento das obrigações contratuais, à aderência às normas e diretrizes, à eventual aplicação de sanções, etc.

Pela CONTRATADA, deverá ser indicado um **RESPONSÁVEL TÉCNICO**, encarregado de gerenciar integralmente as atividades da equipe técnica alocada para a execução dos serviços complementares (manutenções corretivas e preventivas, configurações de roteamento e de priorização de tráfego, emissão de relatórios técnicos, etc.).

Para fins de contrato, a empresa contratada deverá designar seu "**PREPOSTO**", ao qual serão transmitidas as instruções, orientações e normas para execução das atividades.

Incumbe ao **PREPOSTO** e ao **RESPONSÁVEL TÉCNICO**:

a) Coordenar, orientar e supervisionar toda a equipe técnica da CONTRATADA alocada para o cumprimento das obrigações contratuais, cabendo-lhe, ainda, a delegação e distribuição das tarefas entre as equipes, garantindo a qualidade dos serviços prestados e o cumprimento dos níveis de serviços estabelecidos;

b) Responder prontamente a todos os questionamentos e solicitações do TJPA, informando-o das eventuais necessidades de intervenções, inclusive, se necessário, aquelas que devem ser realizadas através de terceiros;

c) Propor ao TJPA mudanças nas rotinas e procedimentos técnicos, quando julgar pertinente, visando a otimização dos custos, a racionalização e melhoria dos processos;

d) Participar, quando solicitado pelo TJPA, de reuniões relativas às atividades sob sua gestão, fornecendo informações e relatórios, apresentando sugestões e propondo soluções que julgue pertinentes e necessárias;

e) Acompanhar e avaliar os resultados globais das atividades sob sua gestão, fornecendo subsídios e informações à Secretaria de Informática do TJPA, visando o tratamento das prioridades e o planejamento global;

f) Ser o ponto de contato entre o TJPA e a CONTRATADA, no que se refere às atividades executadas, posicionando os funcionários da Secretaria de Informática do TJPA quanto ao andamento dos serviços e cumprimento das metas estabelecidas.

3.4. DINÂMICA DE EXECUÇÃO DO OBJETO (ART. 18, § 3º, III, A, 2)

3.4.1. CONDIÇÕES DE ENTREGA DOS SERVIÇOS

A CONTRATADA deverá executar todos os serviços correlatos à entrega, instalação e ativação da solução na Secretaria de Informática, localizada na Tv. Rui Barbosa, esquina com a Av. Nazaré, e também no Data Center do TJPA, localizado na Rod. Augusto Montenegro, no horário entre 08:00 e 14:00, de segunda a sexta-feira, ou em outros horários conforme a estrita necessidade técnico de eventual intromissão na infraestrutura do Data Center do TJPA que possa comprometer o bom funcionamento dos serviços, ocasião em que os dias e horário serão formal, prévia e exclusivamente acordados com o responsável do TJPA pela coordenação da implantação.

O serviço de treinamento será executado nas instalações da CONTRATADA, mas caso seja possível, e em comum acordo, o treinamento poderá ser executado em instalações próprias do TJPA, desde que sejam adequadas às exigências técnicas da CONTRATADA e estejam disponíveis. De outro modo, todos os custos e responsabilidades para viabilizar a execução do serviço de treinamento ficarão a cargo da CONTRATADA.

Os equipamentos fornecidos pela CONTRATADA ficarão sob guarda do TJPA, que deverá se responsabilizar pela integridade dos mesmos.

Os materiais a serem utilizados na instalação deverão ser de qualidade e propriedades físicas que melhor atendam às condições técnica recomendadas pelo fabricante do equipamento e de acordo com os melhores princípios, práticas de engenharia e normas técnicas da ABNT.

O detalhamento do Plano de Implantação deverá conter, no mínimo, a descrição dos itens a seguir:

a) Cronograma detalhado ao nível de atividades a serem desenvolvidas, identificando o marco de conclusão destas atividades durante o processo de implantação;

b) Plano de Testes – com cronograma distinto e pormenorizado – a ser utilizado como roteiro para a aceitação dos serviços definidos neste Termo de Referência;

c) Descritivo detalhado de todas as configurações e as conexões físicas e lógicas.

O Plano de Testes consiste num documento onde deverão estar descritos todos os procedimentos a serem realizados pelo TJPA ou seu preposto, com a finalidade de verificar as funcionalidades dos serviços contratados e as suas consequentes aceitações. Estes procedimentos serão realizados no momento da aceitação dos serviços pelo TJPA ou seu preposto, após a instalação e configuração dos serviços pela CONTRATADA.

O TJPA será responsável em cada edificação pela infraestrutura interna das salas onde ficarão alguns dos equipamentos da solução de UTM/SD-WAN destinados as unidades judiciárias no interior, tal como especificado a seguir: energia elétrica, climatização, unidades de fornecimento ininterrupto de energia (nobreak), cabeamento para conexão à rede interna de dados e aos equipamentos das operadoras, bem como switches de acesso, além dos armários de telecomunicações (racks). Adicionalmente, o TJPA será responsável pela disponibilização do espaço físico em rack-padronizado da Sala Segura do seu Data Center e pelas infraestruturas elétrica e de conectividade Ethernet para fornecer as devidas quantidades de portas e conectividade aos respectivos elementos centrais, objetivando a melhor interoperabilidade do equipamento a ser implantado.

3.4.2. TRANSPORTE, MANUSEIO E ARMAZENAGEM

Os custos relativos ao transporte, embalagem e manuseio, dos materiais e ferramentas empregados na execução dos serviços, desde a sua origem até o local de entrega, ocorrerão exclusivamente às expensas e riscos da CONTRATADA, com previsão de seguro em caso de eventual sinistro.

Todas as providências necessárias e despesas decorrentes da carga, manuseio, proteção e descarga dos equipamentos no local de destino final, bem como o agenciamento de firmas transportadoras e a contratação dos habituais seguros de transporte, serão de responsabilidade da CONTRATADA.

Também serão de responsabilidade da CONTRATADA quaisquer danos provocados a terceiros pelos veículos ou pelas peças, equipamentos e materiais que por estes estejam sendo transportadas, respondendo a mesma por todas as implicações legais.

Deverão ser comunicados ao TJPA, imediatamente, as dificuldades e os acidentes eventualmente ocorridos no transporte, que resultem em atrasos na execução dos serviços. A CONTRATADA, em caso de dano causado à CONTRATANTE, indenizará o valor do equipamento pela Nota Fiscal apresentada.

3.4.3. LOGÍSTICA DE IMPLANTAÇÃO DA REDE

Ao optar pela contratação do serviço de treinamento, a empresa CONTRATADA concorda que este deverá ser finalizado previamente ao início do serviço de implantação da solução.

Conforme acordo prévio com o CONTRATANTE, a CONTRATADA poderá, antecipadamente ao início dos serviços de instalação e configuração, vistoriar a Sala Segura do Data Center do TJPA e validar a infraestrutura física.

Nenhuma ativação poderá ser executada sem a prévia anuência do TJPA e deverá ser iniciada somente quando os requisitos técnicos mínimos exigidos pelo fabricante do equipamento forem atendidos.

Entretanto, nos casos de funcionamento anormal da solução, seja por defeito, seja por falhas de configuração, caberá à CONTRATADA todo o processo de planejamento, instalação, configuração e testes dos equipamentos que serão interligados à infraestrutura de TIC do TJPA, devendo ser feito por profissionais devidamente qualificados e certificados pelo fabricante da solução ofertada.

A CONTRATADA deverá preparar, instalar e configurar os equipamentos nos endereços a serem informados pela CONTRATANTE quando da contratação. A execução destes serviços será, sempre que possível, acompanhada por um profissional integrante do Grupo de Arquitetura Tecnológica do TJPA e eventualmente por algum profissional da Equipe Técnica de Operação adequada.

3.4.4. PRAZOS DE EXECUÇÃO DOS SERVIÇOS

Todos os prazos constantes da contratação serão contabilizados em dias corridos e a sua contagem excluirá os dias de início e de vencimento.

A CONTRATADA deverá entregar equipes de trabalho suficientes, bem como adequada gestão logística para suprimento de materiais, equipamentos e serviços necessários ao cumprimento do objeto do contrato.

A CONTRATANTE poderá determinar à execução dos serviços em horários alheios ao comercial, em feriados ou finais de semana, sem qualquer ônus extra ao TJPA, em caso de atrasos no cronograma ou quando explicitamente solicitado pela CONTRATADA, com vistas a execução do objeto nos prazos especificados.

Caso aconteça algum fato superveniente não motivado pela CONTRATADA, o fato deve ser informado à CONTRATANTE, mediante ofício protocolado na sede da CONTRATANTE. Os atrasos ocasionados por motivo de força

maior ou caso fortuito, desde que justificados em até 02 (dois) dias úteis antes do término do prazo de entrega, e aceitos pela CONTRATANTE, não serão considerados como inadimplemento contratual.

Abaixo quadro ilustrativo dos eventos e prazos:

Tabela 2 – Cronograma de execução do contrato, referente ao fornecimento dos equipamentos de UTM/SD-WAN e dos serviços de instalação e configuração.

REF	ETAPA	PRAZO	PRODUTO
D1	Assinatura do Contrato	----------	Contrato Assinado
D2	Entrega dos Equipamentos	No máximo D1 + 60 (sessenta) dias corridos	Entrega de todo o objeto e notas fiscais de hardware
D3	Ativação dos Equipamentos	No máximo D2 + 30 (trinta) dias corridos	• Treinamento realizado (Se adquirido no mesmo contrato); • Ativação e Conferência dos equipamentos; • Equipamentos instalados, conectados, configurados, disponíveis para uso e • Documentação da instalação entregue; • Entrega das notas fiscais de Software e Garantia; • Validação de acesso e acionamento do Suporte Técnico; • Início da Vigência da Garantia dos equipamentos; • Termo de Ativação assinado.
D4	Conclusão da instalação de todos equipamentos	No máximo D3 + 60 (sessenta) dias corridos	• Conferência final da solução de TI contratada; • Entrega das notas fiscais do Serviço de Instalação; • Termo de Recebimento Definitivo assinado.

O prazo de entrega de todos os equipamentos nas dependências do TJPA é de 60 (sessenta) dias. Em conjunto com a entrega dos equipamentos deverão ser entregues todas as notas fiscais de hardware.

Caso haja solicitação de treinamento pelo TJPA junto com a solução de UTM/SD-WAN, somente será iniciada a configuração do equipamento após o treinamento ser realizado.

A etapa de conferência e ativação dos equipamentos (etapa D3) engloba a implantação efetiva dos equipamentos em produção. Ao final da etapa D3, a vigência da garantia dos equipamentos terá início, de forma que os equipamentos, prontos para receberem os dados de produção, já possuam essa cobertura contratual.

Após a entrega, instalação, ativação dos equipamentos e licenças e a entrega da documentação, a equipe técnica da CONTRATANTE fará a conferência final da solução de TI contratada, através da vistoria das instalações físicas, caso necessário, e via console de gerenciamento dos equipamentos, que deverá ser entregue junto com a solução, visando verificar se ainda restam pendências contratuais a serem cumpridas.

O aceite da solução, para efeito de emissão do Termo de Recebimento Definitivo (TRD), será dado após entrega, conferência, instalação, configuração, incluídas a documentação exigida e acesso ao suporte técnico. Todos os elementos que compõem o objeto deste edital deverão estar disponíveis para que seja emitido o TRD.

O cronograma para treinamento segue abaixo:

Tabela 3 – Cronograma de execução do contrato, referente ao fornecimento do serviço de treinamento.

REF	ETAPA	PRAZO	PRODUTO
T1	Assinatura do Contrato	----------	Contrato Assinado
T2	Entrega dos Equipamentos	No máximo 10 (dez) dias corridos após a assinatura do contrato	Solicitação da CONTRATADA informando os tópicos do treinamento e sugestão de datas
T3	Início de treinamento	No máximo T2 + 45 (quarenta e cinco) dias corridos	Material e instrutor
T4	Entrega de certificados e da nota fiscal	No máximo 15 (quinze) dias corridos após o termino do treinamento	Certificados de participação do treinamento

O aceite da execução dos treinamentos é vinculado à aprovação na avaliação realizada pelos participantes.

Caso a CONTRATADA não seja aprovada na avaliação, esta deverá ser notificada sobre a necessidade de execução de novo treinamento.

3.5. INSTRUMENTOS FORMAIS DE PRESTAÇÃO DO SERVIÇO (ART. 18, § 3º, III, A, 3)

As comunicações formais imprescindivelmente ocorrerão por intermédio de e-mails, especialmente no que tange à formalização de pedidos, prazos e intercâmbio de documentação, sem prejuízo da utilização de recursos telefônicos quando da prestação do serviço de suporte ou quando couber a agilização do contato para a consecução de atividade específica, ficando estas discricionariamente a cargo da CONTRATANTE.

3.6. ACOMPANHAMENTO DA GARANTIA E DOS NÍVEIS DE SERVIÇO (ART. 18, § 3º, III, A, 4)

3.6.1. GARANTIA DE EXECUÇÃO DO CONTRATO

A empresa contratada tem o prazo de 10 (dez) dias, podendo ser prorrogado por mais 10 (dez) dias, a critério do TJPA, contados da data de assinatura do contrato, para apresentar garantia no valor de 5% (cinco por cento) do valor global do instrumento contratual, em uma das seguintes modalidades:

A garantia, qualquer que seja a modalidade escolhida, visa assegurar o pagamento de:

a) Prejuízos advindos do não cumprimento do objeto do contrato;
b) Prejuízos diretos causados ao TJPA, decorrentes de culpa ou dolo durante a execução do contrato;
c) Multas moratórias e punitivas aplicadas pelo TJPA à CONTRATADA

Caso a CONTRATADA opte pela modalidade seguro-garantia, esta somente será aceita se contemplar todos os incisos indicados no Parágrafo Primeiro desta Cláusula, observada a legislação que rege a matéria.

A inobservância das condições de garantia sujeita a CONTRATADA às sanções previstas na seção referente às Sanções administrativas do contrato.

O garantidor não é parte para figurar em processo administrativo instaurado pelo TJPA com o objetivo de apurar prejuízos e/ou aplicar sanções à CONTRATADA.

A garantia somente é liberada ou restituída mediante solicitação da CONTRATADA, desde que integralmente cumpridas as obrigações assumidas no contrato.

Se o valor da garantia for utilizado em pagamento de qualquer obrigação, inclusive multas contratuais, a CONTRATADA fica obrigada a fazer a reposição, no prazo máximo de 15 (quinze) dias a contar da data de recebimento de comunicação do TJPA.

A alteração no valor do contrato, por qualquer motivo, implica a atualização do valor da garantia, no percentual estabelecido na Clausula Trigésima Primeira, obrigando-se a CONTRATADA a complementá-la, se necessário.

A garantia é considerada extinta:

a) Após o término da vigência do contrato ou do prazo adicional estabelecido no instrumento convocatório, que pode ser estendido em caso da ocorrência de sinistro;
b) Com a devolução da apólice, carta fiança ou autorização para o levantamento de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração do TJPA, mediante termo circunstanciado, de que a CONTRATADA cumpriu todas as cláusulas do contrato.

O TJPA executará a garantia na forma prevista na legislação que rege a matéria.

3.6.2. CONDIÇÕES GERAIS DE GARANTIA, SUPORTE E ASSISTÊNCIA TÉCNICA

A CONTRATADA deverá fornecer garantia e assistência técnica 24x7, com vigência de, no mínimo, 60 (sessenta) meses. Durante o prazo de garantia, deverá ser prestado serviço de assistência técnica presencial por meio de manutenção corretiva e preventiva com fornecimento de peças novas e originais, sem ônus adicional para o TJPA.

A CONTRATADA deverá, necessariamente, contratar garantia do FABRICANTE para todos os equipamentos fornecidos, com vigência mínima igual aos prazos mencionados, e apresentar documentação que comprove esta contratação.

A garantia e assistência técnica devem englobar todos os equipamentos, seus componentes e softwares.

Tanto a garantia quanto a assistência técnica terão suas vigências contadas a partir da data de emissão do Termo de Ativação dos equipamentos, não se limitando ao término da vigência contratual.

O serviço da garantia e assistência técnica deverá ser prestado, remotamente quando possível e pessoalmente, quando necessário, nos locais de instalação dos equipamentos então adquiridos.

O serviço da garantia e assistência técnica para o hardware e software da solução de UTM/SD-WAN devem contempla, durante sua vigência, sem ônus adicional para o TJPA, os seguintes requisitos:

a) Prestação de assistência técnica on-site nos endereços do TJPA, por meio de fornecimento e instalação de peças novas e originais em substituição a peças defeituosas;
b) Por peças originais, entendem-se peças fornecidas pelo FABRICANTE do equipamento;
c) As peças defeituosas devem necessariamente ser substituídas por peças novas com características iguais ou superiores e que assegurem a total compatibilidade com o ambiente do TJPA, sem perda de funcionalidades;

d) Direito a instalação de todas as atualizações, upgrades e correções de software, devendo-se, para tanto, disponibilizar acesso para download por meio do site do FABRICANTE;

e) Manutenção preventiva, executada de acordo com a conveniência do TJPA e destinada a reduzir a probabilidade de falha ou a degradação do funcionamento da solução;

f) A manutenção preventiva inclui a atualização de firmware dos equipamentos pela CONTRATADA e software de gerenciamento, no mínimo, 2 (duas) vezes ao ano, se o TJPA assim o solicitar;

g) Manutenção corretiva, que inclui procedimentos e reparos destinados a recolocar a solução em seu perfeito estado de uso;

h) Atendimento a chamados técnicos;

i) Acesso à base de conhecimento do FABRICANTE em sítio disponível via internet.

As demais falhas causadas por hardware ou software deverão ser solucionadas ou contornadas em um prazo máximo de 15 (quinze) dias úteis após o início do atendimento.

A assistência técnica e a garantia, bem como as ferramentas e equipamentos necessários à execução desses serviços, serão de responsabilidade da CONTRATADA, sem custos adicionais ao TJPA.

Quando houver necessidade de entrega e substituição de peças, a data e o horário devem ser previamente agendados com o TJPA.

Deve ser fornecido acesso a serviço de atendimento a clientes para abertura e acompanhamento de chamados por meio de telefone 0800 (chamada gratuita) ou sítio acessível via Internet, disponível 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

Caso seja feito por meio de telefone 0800, deve ser fornecido um único número de telefone para abertura de chamados de todos os equipamentos contratados.

Caso seja feito por meio de sítio acessível via internet, deve ser fornecido um único endereço para abertura de chamados de todos os equipamentos contratados.

No momento do início da vigência do serviço de suporte ao menos um mecanismo de comunicação (telefone/e-mail/chat/sítio) com a CONTRATADA) deverá existir a ser testado, de forma a validar a disponibilidade do corpo técnico desta para fins de abertura de chamados/consultas, sendo este teste requisito para a assinatura do Termo de Ativação e, portanto, requisito imprescindível para o pagamento da Garantia.

A CONTRATADA terá até 7 (sete) dias úteis, a partir do início da prestação do serviço de suporte, para encaminhar todas as informações necessárias (usuários, sítios, canais de comunicação) para que ao menos um técnico do TJPA possa realizar todas as consultas e bases de conhecimentos detalhados neste objeto.

O TJPA terá direito de criação de no mínimo 10 (dez) usuários vinculados ao contrato de suporte, para acesso a base de conhecimento/abertura de chamados e consultas sem ônus adicional. Cada solicitação de criação de usuário e sua vinculação ao contrato de suporte para acesso aos recursos do FABRICANTE deverá ser atendida em até 7(sete) dias corridos.

Todas as solicitações serão registradas pelo TJPA e pela CONTRATADA objetivando o acompanhamento e controle da execução do Contrato.

Devem ser observadas as seguintes restrições quanto ao acesso remoto aos equipamentos do TJPA:

a) Cabe à CONTRATADA informar antecipadamente ao TJPA qualquer necessidade de acesso remoto. O acesso será controlado pelo TJPA, restringindo-se ao tempo necessário para resolução do problema;
b) Todas as intervenções realizadas remotamente são de responsabilidade da CONTRATADA, cabendo a ela responder por qualquer danos porventura decorrentes dessas intervenções.

Quando da solicitação da manutenção, via contato pessoal, mensagens ou telefone, o TJPA fornecerá à CONTRATADA, para fins de abertura de chamado técnico, a seguintes informações:

a) Código de fabricação e número de série do equipamento para o qual for solicitada a manutenção;
b) Local onde a assistência técnica deverá ser prestada;
c) Anormalidade observada;
d) Nome do responsável pela solicitação do serviço e número do telefone para contato.

Quando for necessário atendimento on-site, a CONTRATADA deverá apresentar, via e-mail, relatório de visita contendo: data, hora do chamado, início e término do atendimento, nome do técnico responsável, identificação do problema, as providências adotadas e as informações pertinentes..

A CONTRATADA deverá possuir representação em Brasília, com pelo menos uma das alternativas abaixo, para prestar os serviços descritos nestas especificações:

a) Escritório/filial do FABRICANTE com Centro de Assistência Técnica (CAT);
b) Empresa terceirizada/parceira do FABRICANTE que exerça a função de Centro de Assistência Técnica (CAT).
c) A CONTRATADA deverá, durante a vigência do serviço, substituir so Centros de Assistência Técnica (CAT) por outro CAT, sempre que for necessário para manter a representação no local de prestação do serviço.

3.6.3. NÍVEIS DE SERVIÇO (EXECUÇÃO E MANUTENÇÃO)

Todos os serviços descritos nestas especificações devem estar disponíveis 24 (vinte e quatro) horas por dia e 7 (sete) dias por semana, em horário integral.

O início do atendimento para abertura de chamados não poderá ultrapassar os prazos estabelecidos no quadro abaixo, de acordo com a tabela abaixo e contados a partir da solicitação feita pelo TJPA:

Tabela 4 – Acordo de Níveis de Serviços para o atendimento de chamados

Severidade	Descrição da Severidade	Tempo de Atendimento
A (Emergencial)	Indisponibilidade total, funcionamento parcial ou intermitente	6 Horas (Capital e região Metropolitana) 8 Horas (Demais regiões do Estado)
B (Grave)	Não prejudicam significativamente o funcionamento dos sistemas/serviços do equipamento, afetando apenas áreas específicas	8 Horas (Capital e região Metropolitana) 12 Horas (Demais regiões do Estado)

C (Pedido de Informação)	Solicitação de informações sobre o funcionamento dos equipamentos, não gerando indisponibilidade ou interrupção	24 Horas (Capital, regiões metropolitanas e demais regiões do Estado).

Por início de atendimento entende-se o contato com técnico responsável pelo acompanhamento do chamado.

3.7. ACOMPANHAMENTO DA EXECUÇÃO DO CONTRATO (ART. 18, § 3º, III, A, 5)

3.7.1. CANAIS DE COMUNICAÇÃO

A CONTRATADA deverá fornecer previamente os contatos de e-mail e telefone de seu(s) preposto(s). Estes serão os principais canais de comunicação a serem utilizados durante a execução do contrato, devendo as partes optar pelo uso preferencial de e-mails, para geração de registros documentais.

No entanto, toda e qualquer documentação produzida durante a vigência contratual (a saber: ordens de serviço, boletins de medição, termos de recebimento, ofícios, etc.) deverá assinada pelas partes, e as respectivas vias físicas encaminhadas por um serviço de postagem (Correios, transportadoras, etc.).

3.7.2. REUNIÕES

A CONTRATADA, juntamente com a CONTRATANTE, deverá promover reuniões periódicas de acordo com as demandas em andamento, no intuito de avaliar e zelar pela qualidade de atendimento e execução de serviços. Estas reuniões deverão ocorrer nas dependências da CONTRATANTE, nos endereços previamente informados.

3.7.3. FISCALIZAÇÃO DOS SERVIÇOS

Os serviços deverão ser rigorosamente executados em conformidade com esta ESPECIFICAÇÃO TÉCNICA, a LEI Nº 8.666 de 21 de junho de 1993 (Licitações e Contratos Administrativos), as Normas Técnicas da ABNT, e ainda, códigos, normas, leis e regulamentos dos órgãos públicos federais, estaduais ou municipais e das empresas concessionárias de serviços públicos que estejam em vigor e sejam referentes aos tipos de serviços então descritos.

A fiscalização e o recebimento dos serviços serão realizados por representantes da Secretaria de Informática e da Secretaria de Administração, devidamente designados para este fim.

Em caso de dúvidas quanto à interpretação de eventual documentação fornecida pela CONTRATANTE, e nos casos onde existam divergências nas dimensões dos serviços, a CONTRATADA deverá entrar em contato com a Gestão e/ou com a Fiscalização, previamente ao início dos serviços. Salvo em casos extraordinários, a CONTRATADA não poderá alegar eventuais dúvidas de escopo de serviços como escusa para o não cumprimento dos prazos estabelecidos na SEÇÃO 3.4.4 – PRAZOS DE EXECUÇÃO DOS SERVIÇOS.

Durante a execução dos serviços, a CONTRATADA deverá acatar todas as instruções e ordens da FISCALIZAÇÃO, ressalvadas as possíveis alterações de preços e prazos. Qualquer modificação que se fizer necessária, durante a execução dos serviços, deverá ser previamente autorizada pela FISCALIZAÇÃO.

A FISCALIZAÇÃO poderá determinar a substituição de equipamentos, materiais e serviços considerados fora de padrão, mal executados ou com qualidade aquém da especificada, cabendo à CONTRATADA providenciar a substituição destes no prazo máximo de 15 (quinze) dias e sem ônus adicional a CONTRATANTE.

Nenhuma ação da FISCALIZAÇÃO, seja de inspeção, auditoria, aceitação de uma não conformidade ou dispensa de uma inspeção prevista, isenta a CONTRATADA de suas responsabilidades.

3.8. CONDIÇÕES DE RECEBIMENTO (ART. 18, § 3º, III, A, 6)

Sem prejuízo do especificado neste Termo de Referência, deverá ser emitido o Termo de Recebimento Definitivo (TRD) tão logo a solução for efetivamente entregue e posta em funcionamento.

.

A entrega das documentações abaixo descritas são componentes necessários para a assinatura do Termo de Recebimento Definitivo:

a) Caso a CONTRATADA não seja o próprio FABRICANTE do equipamento, ela deverá obrigatoriamente:

- Contratar garantia do FABRICANTE para todos os equipamentos fornecidos, nos prazos mínimos iguais aos descritos no item 3.4.4 e apresentar documentação que comprove esta contratação;
- Enviar junto com a declaração de assistência técnica da FABRICANTE procuração pública ou particular com firma reconhecida, contrato social ou estatuto, que o signatário tem o poder para assinar tal compromisso ou responder pelo FABRICANTE.

b) Caso a CONTRATADA seja o próprio FABRICANTE, devidamente comprovado, não se faz necessária a apresentação de Declaração de Assistência Técnica do FABRICANTE.

c) Caso o treinamento seja realizado, deverão ser entregues:

- Cópia do certificado para operação do hardware/software, fornecido pelo FABRICANTE do(s) instrutor(es) do treinamento;
- Certificados de conclusão de curso para os participantes

3.9. CONDIÇÕES DE PAGAMENTO (ART. 18, § 3º, III, A, 7)

O TJPA efetuará o pagamento mensal à empresa contratada, por meio de boleto bancário com código de barras, em até 30 (trinta) dias contados da data de apresentação da nota fiscal ou fatura discriminativa, acompanhada da correspondente nota de empenho, com o respectivo ateste de efetiva prestação dos serviços, pelos agentes de gestão e fiscalização contratual.

Se, à época do pagamento, a CONTRATADA não demonstrar que se encontra em situação de regularidade fiscal, incluída a regularidade relativa à Seguridade Social e ao Fundo de Garantia por Tempo de Serviço (FGTS), e em situação de regularidade perante a Justiça do Trabalho, pelo descumprimento dos termos pactuados e das obrigações então estabelecidas, poderão ser aplicadas as penalidades previstas em cláusula própria.

O descumprimento pela CONTRATADA do estabelecido no parágrafo anterior não lhe gera direito a alteração de preços ou compensação de qualquer natureza.

O TJPA poderá deduzir, do montante a ser pago, os valores correspondentes a multas, ressarcimentos ou indenizações devidas pela CONTRATADA, nos termos do instrumento contratual.

No caso de atraso no pagamento, desde que a CONTRATADA não tenha concorrido de alguma forma para tanto, serão devidos pelo TJPA encargos monetários à taxa nominal de 6% a.a. (seis por cento ao ano), capitalizados diariamente em regime de juros simples.

O valor dos encargos será calculado pela fórmula: EM = I x N x VP, onde EM = pagamento; I= índice de compensação financeira = 0,00016438; e VP = valor da prestação em atraso.

3.10. TRANSFERÊNCIA DE CONHECIMENTO (ART. 18, § 3º, III, A, 8)

Como se trata de uma solução nova que será implantada na infraestrutura tecnológica do Tribunal, faz-se necessária a contratação de treinamento que tenha como escopo a instrução de procedimentos de instalação, configuração e operação da solução, bem como dos conhecimentos em gerenciamento e análise de problemas (troubleshooting), sendo que este treinamento deve ser ministrado previamente a ativação da solução, com o objetivo de prevenir a subutilização ou mesmo a utilização de forma errônea dos equipamentos que compõem a solução.

Adicionalmente, durante toda a implantação da solução, os técnicos da CONTRATADA deverão demonstrar à Equipe Técnica de Acompanhamento da CONTRATANTE os procedimentos de instalação e configuração dos equipamentos e os procedimentos de operação dos componentes da solução. Todo o processo de instalação e configuração deverá ser documentado pela CONTRATADA sob a forma de relatório ou roteiro, de modo que a Equipe Técnica do TJPA possa absorver o conhecimento e aplica-lo quando for necessário.

3.11. DIREITOS DE PROPRIEDADE INTELECTUAL E AUTORAL (ART. 18, § 3º, III, A, 9)

Concluída a execução dos serviços e comprovada a qualidade e a quantidade do objeto, bem como sua conformidade com todas as condições exigidas em contrato, será emitido o TERMO DE RECEBIMENTO DEFINITIVO da solução. Neste momento, ocorrerá a transferência de propriedade da solução (incluindo-se todos os equipamentos e softwares) para o TJPA.

Quanto à documentação produzida (projetos, relatórios, manuais, etc), os direitos de propriedade autoral sobre os projeto, planos, desenhos, diagramas e esboços produzidos durante a vigência contratual pertencerão à empresa contratada e, respeitadas as relações contratuais expressas entre o autor e outros interessados, ao profissional que os elaborar.

Vale ressaltar que a empresa contratada se limita a projetar a implantação da solução de UTM/SD-WAN idealizada pelo TJPA e constante nos projetos preliminares apresentadas antes da emissão de toda e qualquer ordem de fornecimento de serviço. Em resumo, as atividades compreendem a análise e a validação dos desenhos produzidos, bem como a estimativa dos quantitativos de materiais e serviços necessários para sua execução. Tal condição não apenas limita o direito autoral, mas também permite ao TJPA a manipulação e a modificação da referida documentação, respeitando-se a titularidade na autoria.

Eventuais softwares, necessários ao funcionamento da solução contratada, são próprios dos fabricantes e deverão ser fornecidos em conjunto com os equipamentos correspondentes. Os direitos de propriedade intelectual sobre estes produtos pertencem à empresa fabricante da solução, tal como dispõe o art. 2ª, § 2º e § 3º da Lei Federal 9609/98 que versa sobre a propriedade intelectual dos programas de computador.

3.12. QUALIFICAÇÃO TÉCNICA (ART. 18, § 3º, III, A, 10)

Sem prejuízo do especificado neste Termo de Referência, toda a documentação relativa à qualificação técnica dos representantes da CONTRATADA deverá ser apresentada e analisada quando da assinatura do contrato.

Ainda assim, o TJPA reserva-se ao direito de, a qualquer momento e a seu exclusivo critério, exigir o reenvio de documentação recente e atualizada, inclusive quanto ao registro ou inscrição da empresa na entidade profissional competente e quanto a qualificação profissional doas agentes envolvidos na execução dos serviços.

A não apresentação da documentação exigida caracterizará a falta e habilidades e competências mínimas para a execução do objeto contratual, dando a entender que pode representar risco ao processo e que não possui capacidade ou apoio do fabricante em sua proposição.

3.13. SANÇÕES ADMNISTRATIVAS (ART. 18, § 3º, III, A, 11)

A empresa contratada ficará impedida de licitar e contratar com o Tribunal de Justiça do Estado do Pará – TJPA, pelo prazo de 05 (cinco) anos, e será descredenciada no SICAF, se for o caso, sem prejuízo das multas previstas no contrato emergencial e das demais cominações referidas no Capítula IV da Lei nº. 8.666/93, no que couber, garantindo o direito à prévia defesa, se:

a) Deixar de entregar a documentação exigida no instrumento contratual;
b) Convocada dentro do prazo de validade de sua proposta, não assinar o contrato;
c) Apresentar documento falso ou fizer declaração falsa;
d) Ensejar o retardamento da execução do objeto do contrato emergencial;
e) Não mantiver a proposta, injustificadamente;
f) Falhar ou fraudar na execução do contrato emergencial;
g) Comportar-se de modo inidôneo;
h) Cometer fraude fiscal.

Pela inexecução total ou parcial do objeto contratual, a Administração do Tribunal de Justiça do Estado do Pará poderá aplicar a CONTRATADA as seguintes sanções, garantindo sempre o direito à prévia e ampla defesa:

a) Advertência, definindo-se prazo razoável para o adimplemento da obrigação;
b) Multa
   - Multa moratória de 5% (cinco por cento) sobre o valor do Contrato, pela recusa da CONTRATADA em assinar contrato e pela não apresentação da documentação exigida no Edital para sua celebração, nos prazos e condições estabelecidas, caracterizando o descumprimento total da obrigação assumida, com base no art. 81 da Lei 8.666/93, independentemente das demais sanções cabíveis;
   - Multa moratória de 0,33% (zero vírgula trinta e três por cento) sobre o valor do item ou conjunto de itens, por dia de atraso, no caso da CONTRATADA não entregar e/ou não instalar os equipamentos no prazo estipulado no item 3.4.4, até o limite máximo de 30 (trinta) dias.
   - Multa moratória de 5% (cinco por cento) sobre o valor do Contrato, pela inexecução parcial, total ou execução insatisfatória do contrato, aplicada em dobro na sua reincidência, ou pela interrupção da execução do contrato sem prévia autorização da CONTRATANTE, independentemente das demais sanções cabíveis;
   - Multa moratória de 1% (cinco por cento) sobre o valor do Contrato, pela recusa em corrigir qualquer objeto rejeitado ou com defeito, caracterizando-se a recusa caso a correção não se efetive nos 10 (dez) dias que se seguirem à data de comunicação formal da rejeição ou defeito, independentemente das demais sanções cabíveis;
   - Multa moratória de 1% (cinco por cento) sobre o valor do Contrato, pelo não cumprimento dos prazos estipulados nos Acordos de Níveis de Serviço (ANS), de acordo com o item 3.4.4,

sem justificativa prévia aceita pela CONTRATANTE, independentemente das demais sanções cabíveis;

- Multa compensatória de 10% (dez por cento) sobre o valor do Contrato, sendo deste valor deduzido o(s) valor(es) referente(s) às multa(s) moratória(s), no caso de rescisão do Contrato por ato unilateral da administração, motivado por culpa da CONTRATADA, garantida a defesa prévia e o contraditório, independentemente das demais sanções cabíveis.

c) Suspensão temporária de participação em licitação e impedimento de contratar com a Administração, por prazo não superior a 02 (dois) anos.

d) Declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição, conforme disposto no inciso IV do Art. 87 da Lei 8666/93. Esta declaração será emitida pela autoridade máxima do órgão CONTRATANTE.

As multas previstas neste Termo de Referência poderão ser aplicadas, cumulativamente ou não com as demais sanções administrativas previstas na legislação aplicável e vigente.

O atraso ou a suspensão injustificada na execução do objeto a ser contratado, por período superior a 30 (trinta) dias, poderá ensejar a rescisão do contrato emergencial.

As multas aplicadas serão descontadas do valor da garantia prestada. Se for insuficiente, além de perder a garantia, responderá a CONTRATADA pela sua diferença, que será descontada dos pagamentos eventualmente devidos pelo TJPA. Se preferir, poderá a CONTRATADA recolher as multas no prazo de 05 (cinco) dias úteis a contar da comunicação oficial.

Na ausência/insuficiência de garantia e de créditos para desconto das multas, e se estas não foram recolhidas no prazo estipulado anteriormente, as multas aplicadas serão cobradas judicialmente.

Em sendo a garantia utilizada para o pagamento de multas, compromete-se a empresa CONTRATADA a complementar ou apresentar nova garantia no prazo de 05 (cinco) dias úteis.

Da aplicação das previstas inicialmente caberá recurso, no prazo de 05 (cinco) dias úteis, contados da notificação oficial, que será dirigido à autoridade superior, por intermédio da que praticou o ato, a qual poderá reconsiderar a sua decisão ou fazê-lo subir devidamente informado.

As penalidades serão obrigatoriamente registradas no SICAF e, no caso de impedimento de licitar, por descumprimento parcial ou total do contrato, a CONTRATADA deverá ser descredenciada por igual período, ou seja, por prazo não superior a 5 (cinco) anos, conforme atr. 7º da Lei nº 10.520, de 17 de julho de 2002, sem prejuízo das multas previstas no instrumento convocatório e das demais combinações legais.

4. REQUISITOS TÉCNICOS A SEREM ATENDIDOS (ART. 18, § 3º, IV)

Deverão ser atendidos todos os requisitos constantes deste Termo de Referência, incluindo os constantes do seu ANEXO B – ESPECIFICAÇÕES TÉCNICA DOS PRODUTOS E SERVIÇOS.

5. RESPONSÁVEIS PELO TERMO DE REFERÊNCIA

EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO

DIEGO BAPTISTA LEITÃO	THIAGO DO ROSÁRIO DE CASTRO	CARMEM AMORIM BARBALHO
INTEGRANTE DEMANDANTE	INTEGRANTE TÉCNICO	INTEGRANTE ADMINISTRATIVO
MAT.: 123030	MAT.: 174394	MAT.: 122297

VALIDAÇÃO DO TERMO DE REFERÊNCIA

DIEGO BAPTISTA LEITÃO
SECRETÁRIO DE INFORMÁTICA

ANEXO A – LISTA DAS UNIDADES DO TJPA

#	MUNICÍPIO	UNIDADE	ENDEREÇO
1	ABAETETUBA	Fórum Juiz Hugo Oscar Figueira de Mendonça	AV. D. PEDRO II, 1177, BAIRRO: AVIAÇÃO - CEP: 68440-000
2	ACARÁ	Fórum Prof. Dr. Lourenço do Vale Paiva	RUA DEODORO DA FONSECA, 1930, BAIRRO: CENTRO - CEP: 68690-000
3	ALENQUER	Fórum Des. Raimundo Nogueira Faria	TV. SANTO ANTÔNIO, S/N, BAIRRO: CENTRO - CEP: 68200-000
4	ALMEIRIM	Fórum Des. Ignácio C. Guilhon D'Oliveira	RODOVIA ALMEIRIM / PANAICA, 668, BAIRRO: CENTRO - CEP: 68230-000
5	ALTAMIRA	Fórum Des. José Amazonas Pantoja	AV. BRIGADEIRO EDUARDO GOMES, 1651, BAIRRO: SÃO SEBASTIÃO - CEP: 68372-020
6	ALTAMIRA	Vara Agrária de Altamira	Rua Otaviano Santos, 2298 - Bairro: Centro. CEP: 68.371-288.
7	ANAJÁS	Fórum Dr. Walton Cezar Brudzinsk	AV. BARÃO DO RIO BRANCO, 19, BAIRRO: CENTRO - CEP: 68810-000
8	BAGRE	Fórum do Termo Judiciário de Bagre	AV. PRESIDENTE VARGAS, 93, BAIRRO: CENTRO - CEP: 68475-000
9	BONITO	Fórum Pretora Izabel Corrêa	AV. MARECHAL HERMES, 498, BAIRRO: CENTRO - CEP: 68645-000
10	BRAGANÇA	Fórum Des. Augusto Rangel de Borborema	AV. NAZEAZENO FERREIRA, S/N, BAIRRO: CENTRO - CEP: 68600-000
11	BREVES	Fórum Dr. Pedro dos Santos Torres	AV. RIO BRANCO, 432, BAIRRO: CENTRO - CEP: 68800-000
12	CAMETÁ	Fórum Des. Manoel de Cacella Alves	RUA TRILHA DA JUVENTUDE, S/N, BAIRRO: CENTRO - CEP: 68400-000
13	CAPANEMA	Fórum Des. Santo Estanislau Pessoa de Vasconcelos	AV. BARÃO DE CAPANEMA, 1011, BAIRRO: CENTRO - CEP: 68.700-970
14	CAPITÃO POÇO	Fórum Des. Aluízio da Silva Leal	AV. 29 DE DEZEMBRO, 1746, BAIRRO: CENTRO - CEP: 68650-000
15	CHAVES	Fórum da Comarca de Chaves	AV. INDEPENDÊNCIA, 07, BAIRRO: CENTRO - CEP: 68880-970
16	COLARES	Fórum do Termo Judiciário de Colares	RUA DR. JUSTO CHERMONT, S/N, BAIRRO: CENTRO - CEP: 68785-000
17	FARO	Fórum Juiz Gaspar Vicente da Costa	RUA DR. DIONÍSIO BENTES, S/N, BAIRRO: CENTRO - CEP: 68280-000

18	GURUPÁ	Fórum Juiz Álvaro Magalhães Costa	AV. SÃO BENEDITO, 240, BAIRRO: CENTRO - CEP: 68300-000
19	ITAITUBA	Fórum Des. Walter Bezerra Falcão	TRAV. PAES DE CARVALHO, S/N, BAIRRO: COMERCIO - CEP: 68180-000
20	ITUPIRANGA	Fórum Des. Osvaldo de Brito Farias	RUA SÃO SALVADOR, S/N, BAIRRO: CENTRO - CEP: 68580-000
21	JACAREACANGA	Fórum Dr. Luis Ercílio do Carmo Faria	TV. ESTANISLAU BRILHANTE, S/N, BAIRRO: BELA VISTA - CEP: 68095-000
22	MARABÁ	Fórum Juiz José Elias Monteiro Lopes	RUA. TRANSAMAZÔNICA, S/N, BAIRRO: AMAPÁ - CEP: 68508-970
23	MARAPANIM	Fórum Juiz Mariano Antunes de Souza	RUA DINIZ BOTELHO, 1722, BAIRRO: CENTRO - CEP: 68760-000
24	MOCAJUBA	Fórum Des. Moacyr Guimarães Moraes	TV.. 7 DE SETEMBRO, S/N, BAIRRO: CENTRO - CEP: 68420-000
25	MONTE DOURADO	Vara Distrital de Monte Dourado	Rua H, 158, Bairro: Staff - CEP: 68.240-000
26	MOSQUEIRO	Juizado Especial de Mosqueiro	Rua 15 de Novembro, 23, BAIRRO: VILA - CEP: 66970-100
27	NOVO PROGRESSO	Fórum Des. Hamilton Ferreira de Souza	RUA DO CACHIMBO, 381, BAIRRO: JARDIM PLANALTO - CEP: 68193-000
28	NOVO REPARTIMENTO	Fórum Des. Hélio de Paiva Mello	AV. CUPUAÇU, S/N, BAIRRO: CENTRO - CEP: 68473-000
29	ÓBIDOS	Fórum Juiz Abdias dos Santos Arruda	RUA MARCOS RODRIGUES DE SOUZA, S/N, BAIRRO: CENTRO - CEP: 68250-000
30	ORIXIMINÁ	FÓRUM JUIZ ANTÔNIO LAUREANO DINIZ	TV. CARLOS MARIA TEIXEIRA, 754, BAIRRO: CENTRO - CEP: 68270-000
31	PARAGOMINAS	Fórum Dr. Célio de Rezende Miranta	RUA ILHÉUS, S/N, BAIRRO: INDUSTRIAL - CEP: 68625-970
32	PARAUAPEBAS	FÓRUM JUIZ CÉLIO RODRIGUES CAL	RUA C, QUADRA ESPECIAL, BAIRRO: CIDADE NOVA - CEP: 68515-000
33	PARAUAPEBAS	Centro Judiciário de Solução de Conflitos e Cidadania - CEJUSC	Rua E, 505, Bairro: Cidade Nova - CEP: 68515-000.
34	PRAINHA	Fórum Pretor Michel de Mello e Silva	RUA BARÃO DO RIO BRANCO, S/N, BAIRRO: CENTRO - CEP: 68130-000
35	REDENÇÃO	FÓRUM DES. RAUL DA COSTA BRAGA	RUA PEDRO COELHO DE CAMARGO, ESQUINA COM A AV. MANOEL VICENTE PEREIRA, SETOR OESTE, QUADRA-22, BAIRRO: PARQUE DOS BURITIS - CEP: 68552-735

36	SALINÓPOLIS	Fórum Pretor José Ribamar de Moura	AV. JOÃO PESSOA, 1084, BAIRRO: AMAPÁ - CEP: 68721-000
37	SANTANA DO ARAGUAIA	Fórum Des. Antônio Koury	AV. GILBERTO CARVELLI, S/N, BAIRRO CENTRO - CEP: 68560-000
38	SANTARÉM	Arquivo Geral de Santarém	TV. PROFESSOR JOSÉ AGOSTINHO, 259, BAIRRO: PRAINHA - CEP: 68.005-460.
39	SANTARÉM	Fórum Des. Ernesto Adolfo de V. Chaves	AV. MENDONÇA FURTADO, S/N - CEP: 68005-100
40	SANTARÉM	Juizado Especial – FIT (Santarém)	Travessa Silvino Pinto, 604 - CEP: 68005-310
41	SANTARÉM	Juizado Especial – UFOPA (Santarém)	Av. Marechal Rondon, S/N, Bairro: Liberdade - CEP: 68040-070
42	SANTARÉM	Juizado Especial – ULBRA(Santarém)	Av. Moaçara, n. 1787, esquina com Av. Sérgio Henn - CEP: 68025-000
43	SÃO DOMINGOS DO CAPIM	Fórum Des. Maurício Cordovil Pinto	RUA MAGALHÃES BARATA, 630 - CEP: 68635-000
44	SÃO FÉLIX DO XINGU	Fórum Juiz Arthur Carvalho Cruz	AV. GOIÁS,S/N, BAIRRO: CENTRO - CEP: 68380-970
45	SÃO GERALDO DO ARAGUAIA	Fórum Juiz Miguel Antunes Carneiro	AV. PRESIDENTE VARGAS, 323, BAIRRO: CENTRO - CEP: 68570-000
46	TERRA SANTA	Fórum Pretora Maria Leite de Brito	TRAV. SANTA TEREZINHA, S/N, BAIRRO: CENTRO - CEP: 68285-000
47	TOME-AÇÚ	Fórum Dra. Nezilda de Melo Bentes	AV. 03 PODERES, 800, BAIRRO: CENTRO - CEP: 68680-000
48	TUCUMÃ	Fórum Des. João Gualberto Alves de Campos	RUA MANOEL MARIA BARROS COSTA, S/N, BAIRRO: CENTRO - CEP: 68385-000
49	TUCURUÍ	Fórum Juiz Lúcio Amorim do Amaral	RUA 31 DE MARÇO, S/N, BAIRRO: SANTA IZABEL - CEP: 68456-110
50	ULIANÓPOLIS	Fórum Des. Nelson Silvestre Rodrigues Amorim	AV. DO CONTORNO, 278, BAIRRO: CAMINHO DAS ÁRVORES - CEP: 68632-000
51	URUARÁ	Fórum Des. Silvio Hall de Moura	RUA MARQUES DE TAMANDARÉ, S/N, BAIRRO: FLUMINENSE - CEP: 68140-000
52	VISEU	Fórum Juiz Francisco Severiano Duarte	RUA MAJOR OLÍMPIO, S/N, BAIRRO: CENTRO - CEP: 68620-000

ANEXO B – ESPECIFICAÇÃO TÉCNICA DOS PRODUTOS E SERVIÇOS

2. ESPECIFICAÇÕES

2.1.Requisitos gerais comuns a todos os Firewalls multifuncionais dos lotes 1,2,3,4 e 5

2.1.1. Todos os equipamentos *firewall* e a solução de gerência integrada devem ser do mesmo fabricante, inclusive os sistemas operacionais executados por esses equipamentos, observado, o disposto no item 2.1.10.

2.1.2. Todos os equipamentos e seus componentes deverão ser novos, sem uso, e ent regues em perfeito estado de funcionamento, sem marcas, amassados, arranhões ou outros problemas físicos, acondicionados em suas embalagens originais e a companhados de todos os acessórios, cabos, conectores, *kits* de fixação, trilhos, fibras óticas (incluindo sua fusão, se necessário), *patchcords*, *transceivers*, etc, necessários às suas instalações e operação em rack de 19" padrão EIA-310. No caso dos lotes 1 e 2, firewall multifuncionais de 100 e 250 Mbps, poderá ser fornecido os insumos como bandejas para colocação dos mesmos em racks.

2.1.3. Não serão aceitos equipamentos em modo *End of Support* durante a vigência da garantia **e** que **estejam** em modo *End of Life* **no ato** da assinatura da ata de registro de preços, não deixando de atender ao item 2.1.6 durante toda a vigência da garantia.

2.1.3.1. A exigência acima encontra fundamento na necessidade que a Administração Pública tem de resguardar seus interesses, no sentido de estabelecer exigências mínimas objetivando evitar que ocorra aquisição de equipamentos que tenham seu ciclo de vida descontinuado em um curto prazo, ou para os quais não haja mais suporte técnico e atualizações antes do fim do período de garantia, que é de 60 (sessenta) meses.

2.1.3.2. No ato da assinatura do contrato, caso o equipamento registrado em ata não atenda o disposto no item 2.1.3., poderá ser aceito equipamento de capacidade técnica igual ou superior, da mesma série ou linha ou família, desde que atenda a todos os requisitos técnicos disposto no presente edital.

2.1.4. O fabricante deverá atualizar *firmwares e softwares* da solução para novas versões durante toda a vigência da garantia.

2.1.5. Todas as funcionalidades adquiridas de *hardware e software* devem operar conforme disposto neste Termo de Referência durante oprazo de garantia dos equipamentos, ou seja, o fornecedor deve garantir a atualização completa das funcionalidades no prazo referido, não sendo permitida a cobrança de quaisquer valores adicionais pelo uso dos *hardwares e softwares* para esse período. As funcionalidades deverão permanecer ativas, mesmo que nã o sejam atualizadas após o fim do prazo da garantia.

2.1.5.1. Após o prazo da garantia, os equipamentos deverão permanecer com todas as funcionalidades operacionais, com as atualizações imediatamente anteriores a data final da garantia dos equipamentos.

2.1.5.2. Somente a funcionalidade de filtro de conteúdo web poderá ser desativada ao final do prazo de garantia do equipamento, em razão de sua natureza técnica de acesso on-line as suas bases de dados.

2.1.5.3. A garantia referida no item 2.1.5 terá início com a emissão do termo de recebimento definitivo da solução a ser gerado pela CONTRATANTE conforme disposto no item 12.4.

2.1.6. As licenças de atualização de *software* (*firmware* ou *drivers*) e licenças de atualização de assinaturas deverão ser forne cidas pelo prazo mínimo de 60 (sessenta) meses, a contar da data do recebimento definitivo dos produtos, sem ônus adiciona l para as atualizações e seu uso.

2.1.7. Todos os equipamentos devem funcionar com alimentação nominal de 100~120V AC e 210~230VAC e frequência de 50 ou 60 Hz, ou*auto-ranging*. Deverá vir acompanhado de cabo de alimentação com, no mínimo, 1,80m (6 pés), com plug tripolar 2P+Tno padrão ABNT NBR 14136.

2.1.8. O equipamento deve possuir 1 (uma) porta de console para configuração e gerenciamento por interface de linha de comando (CLI).

2.1.8.1. Deve ser fornecido pelo menos 1 (um) cabo conversor Serial para USB, compatível com a porta de console do equipamento.

2.1.9. O equipamento deve ser fornecido com todas as suas portas de comunicação, interfaces e afins habilitadas, operacionais e sem custos adicionais, mesmo que para futuras utilizações do órgão ou entidade CONTRATANTE.

2.1.9.1. A CONTRATADA deve entregar a quantidade de *transceivers* equivalente ao **dobro** da quantidade mínima de portas exigidas em cada lote conforme os itens 3.15.1.4, 3.22.1.4 e 3.29.1.4.

2.1.9.2. Em caso de defeito ou mau funcionamento dos *transceivers*, estes devem estar cobertos pela garantia da solução.

2.1.10. O equipamento deve ser fornecido em *hardware* dedicado tipo *appliance* ou chassi, com sistema operacional otimizado, do mesmo fabricante, para o uso como *firewall* corporativo multifuncional.

2.1.10.1. Os equipamentos dos lotes 1, 2, 3 e 4 da solução ofertada, não deve rão exceder, individualmente, 4 Unidades de Rack, sendo “caixas” úni cas, sem empilhamentos.

2.1.10.2. O equipamento do lote 5 da solução ofertada, pode ser baseado em *appliance* ou chassi, deverá ter atestada, pelo fabricante, a compatibilidade entre os módulos e o chassi e deverá suportar agregação de enlaces multi-chassi (MC-LAG), s egundo padrão IEEE 802.1ax.

2.1.11. Deve possuir fonte(s) de energia atendendo aos itens 3.1.1.3, 3.8.1.3, 3.15.1.3, 3.22.1.3 e 3.29.1.3.

2.1.12. Deve suportar topologias de *cluster* redundante de alta disponibilidade (*failover*) no mínimo aos pares, nos modos ativo-ativo e ativo-passivo, com sincronização, em tempo real, de configuração e de estados das sessões. No caso de falha de um dos equipamentos do *cluster*, não deverá haver perda das configurações e nem das sessões já estabelecidas e a transição entre os equipame ntos deverá acontecer de forma transparente para o usuário.

2.1.13. Deve suportar a implementação tanto em modo transparente (camada 2) quanto em modo *gateway* (camada 3).

2.1.14. Possuir filtragem de pacote por endereço IP de origem e destino, por apli cação (independentemente da porta ou protocolo utilizados pela aplicação), po r sub-rede e por períodos do dia, permitindo a aplicação de regras por horários e por dias da semana.

2.1.15. Permitir criação de serviços por porta ou conjunto de portas para, no mínimo, os protocolos T CP, UDP, ICMP e IP.

2.1.16. Suportar *tags* de VLAN;

2.1.17. Permitir a criação de no mínimo 25 VLANs padrão 802.1q para os firewalls especificados nos lotes 1, no mínimo 50 VLANs padrão 802.1q para os firewalls do lote 2 e no mínimo 500 VLANs padrão 802.1q para os firewalls especificados nos lotes 3, 4 e 5.

2.1.18. Ser capaz de aceitar comandos de *scripts* acionados por sistemas externos como, por exemplo, correlacionadores de eventos;

2.1.19. Suportar o bloqueio de tráfego em função da localização geográfica dos IPs de origem e de destino;

2.1.20. Suportar agregação de *links*, segundo padrão IEEE 802.3ad, nos equipamentos firewall descritos nos lotes 3, 4 e 5.

2.1.21. Possuir ferramenta de diagnóstico do tipo *tcpdump*.

2.1.21.1. Suportar e efetuar a captura de pacotes no formato PCAP.

2.1.21.2. Suportar e efetuar o download dos arquivos PCAP

2.1.22. Não deve possuir restrições de licenciamento em relação às características, requisitos e funcionalidades presentes no subitem 2.1, inclusive em relação ao número de ou tipo de clientes, usuários, máquinas e endereços IP.

2.1.23. Deve suportar, no próprio firewall, autenticação de usuários locais e integração com serviços de autenticação de diretório LDAP, Microsoft Active Directory e Radius, sendo que:

2.1.23.1. Não deverão existir limitações de licenciamento quanto ao número de usuários, a não ser o limite operacional do equipamento, respeitado o quantitativo mínimo especificado em cada lote;

2.1.23.2. Deve registrar a identificação do usuário em todos os eventos associados gerados pelo equipamento, tais como (mas não restrito a) eventos de autenticação, registros de acesso ou bloqueio e eventos associados a ameaças;

2.1.23.3. Deve prover identificação de forma transparente aos usuários autentica dos por *single sign-on*, no mínimo, por meio dos serviços Microsoft Active Directory e RADIUS;

2.1.23.4. Deve prover portal ou pop-up de login para identificação dos usuários dos demais serviços de LDAP nã o listados no item anterior;

2.1.23.5. Deve permitir a criação de regras de acesso/bloqueio baseadas em usuários ou grupo de usuários do LDAP e do Microsoft Active Directory;

2.1.23.6. Não será permitida a utilização de agentes instalados nos equipamentos dos usuários;

2.1.23.7. Possuir métodos de autenticação de usuários para aplicações executadas sobre os protocolos TCP, tais como (mas não restritos a) a plicações HTTP, HTTPS e FTP;

2.1.24. Suportar *Network Address Translation* (NAT 1-1, NAT 1-N, NAT N-1) de acordo com a RFC 3022, nos modos estático e dinâmico;

2.1.25. Deve suportar no mínimo NAT 64.

2.1.26. Possuir a funcionalidade de fazer tradução de endereços dinâmicos um-para-N, PAT (*Port Address Translation*);

2.1.27. Suportar nativamente IPv6;

2.1.27.1. Suportar, no mínimo, os protocolos de roteamento dinâmico OSPF v3 e BGP, bem como as funcionalidades de roteamento estático e roteamento *policy-based*

2.1.28. Possuir funcionalidades de DHCP *client*, *server* e *relay*;

2.1.29. Possuir proteção e suporte a protocolos de Real Time, contemplando no mínimo: Real Time Transport Protocol (RTP), H323 e SIP sobre os protocolos IPV4 ou IPV6.

2.1.30. Possuir tecnologia de *firewall stateful*;

2.1.31. Permitir a realização de *backup* e *restore* das regras, configurações e políticas, e a transferência desse *backup* para armazenamento em servidores externos;

2.1.32. Possuir funcionalidade de detecção e bloqueio de, no mínimo, os seguintes tipos de ataques: *IP Spoofing*, *SYN Flood*, *UDP Flood, Port Scanning*, *ICMP Flood, ICMP sweep, Ataques de Força Bruta ataques Man-in-the-Middle e variações de reflexão;*

2.1.33. Suportar sincronização de horário por NTP;

2.1.34. Possuir funcionalidade de geração de relatórios e exportação de logs;

2.1.35. Suportar no mínimo 250 regras ou políticas de firewall para os equipamentos do lote 1 e 1.000 regras ou políticas de firewall para os equipamentos dos lotes 2,3,4 e 5.

2.1.36. Permitir a abertura de novas portas por fluxo de dados para serviços que requerem portas d inâmicas;

2.1.37. Possuir mecanismo de *anti-spoofing*;

2.1.38. Possuir funcionalidade de exceção em SSL Inspection para sites e aplicações bancár ias, não decriptando o tráfego dessas sessões.

2.1.39. Possuir inspeção profunda de pacotes para tráfego criptografado (no mínimo em tráfego VPNe HTTPS);

2.1.40. Possuir, no mínimo, suporte a SNMP v2 e v3;

2.1.41. Deve possuir MIB própria contemplando, no mínimo, indicadores de estado do *hardware* e de performance do equipamento;

2.1.42. Deve identificar os países de origem e destino de todas as sessões estabelecidas através do equipamento, exceto para sessões no âmbito da rede interna (não roteadas).

2.1.43. Deve permitir a criação de políticas de segurança baseadas em geolocalização, permitindo o bloqueio de tráfego com origem ou destino a determinado país ou grupo de países.

2.1.44. Deve possibilitar a visualização dos países de origem e destino nos logs de eventos, de ace ssos e ameaças.

2.1.45. Deve prover interface de gerência local do firewall ou do cluster (virtual ou físico) do qual o firewall faz parte, por meio de interface gráfica (GUI) e linha de comando – (CLI) ou via SSH. Especificamente a interf ace gráfica (GUI) deve atender as funcionalidades gerenciais previstas nos subitens 2.1.45.1 ao 2.1.45.14.

2.1.45.1. Deve possuir a capacidade de definir administradores com diferentes perfis de acesso. Os perfis de acesso devem ser, no mínimo, de leitura/escrita e somente leitura.

2.1.45.2. Deve permitir a delegação de funções de administração.

2.1.45.3. Deve registrar em log as ações dos usuários administradores.

2.1.45.4. Deve suportar a identificação e utilização de usuários nas políticas de segurança.

2.1.45.5. Deve suportar agrupamento lógico de objetos (" *object grouping*") para criação de regras.

2.1.45.6. Deve possibilitar o gerenciamento (incluindo a criação, alteração, monitoramento e exclusão) de objetos de rede. Deverá ainda permitir detectar se e onde, na base de regras, está sendo utilizado determinado objeto de rede. Os tipos de objetos deverão permitir especificar de forma distinta grupos e objetos de rede e serviços, diferenciando-os e agrupando-os conforme suas características ou descrição de maneira a permitir o reaproveitamento dos mesmos em diferentes políticas.

2.1.45.7. Deve contabilizar a utilização ("hit counts") ou o volume de dados trafegados correspondente a cada regra de filtragem individualmente.

2.1.45.8. Deve possibilitar a especificação de política por tempo, ou seja, pe rmitir a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora).

2.1.45.9. Deve suportar a geração de alertas automáticos via *email*, SNMP e Syslog.

2.1.45.10. Deve permitir a exportação de logs via SCP ou FTP.

2.1.45.11. Deve informar a utilização dos recursos de CPU, memória, armazenamento interno e atividade de rede dos equipamentos gerenciados.

2.1.45.12. Deve informar o número de sessões simultâneas e de novas sessões por segundo dos equipamentos gerenciados.

2.1.45.13. Deve possuir visualização mínima sumarizada de: aplicações, ame aças, URLs, endereços de origem, endereços de destino, levando-se em conta o quantitativo de sessões, de consumo de banda e categorização.

2.1.45.14. Deverá suportar gerência remota (via rede local ou WAN) ou por meio da gerência centraliz da, sendo que:

2.1.45.14.1. A comunicação entre a estação ou sistema de gerência e o firewall ou cluster loca l deverá ser criptografada e autenticada;

2.1.46. Deve permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (*inbound/outbound*) através da classificação dos pacotes (*shaping*);

2.1.47. Deve possuir gerenciamento gráfico centralizado das funcionalidades de *QoS/Traffic Shaping* integrado tanto com a gerência local do equipamento, quanto com a gerência centralizada da solução*;*

2.1.48. Deve suportar a criação de políticas de controle de uso de largura de banda, limitando ou expandido individualmente, baseadas em: porta ou protocolo, endereço IP de origem ou destino, grupo de usuários do Microsoft *Active Directory e* LDAP e aplicações (por exemplo, *Youtube* e *WhatsApp*).

2.1.49. As funcionalidades de VPN não podem possuir qualquer restrição de li cenciamento, inclusive em relação ao número de clientes, aos *softwares* instalados nos clientes, IPs e máquinas, limitado apenas à capacidade de*throughput* do equipamento para VPN.

2.1.50. Deve permitir a arquitetura de VPN *hub and spoke* IPSec, tanto para topologias site-to-site ("Full Meshed" e "Estrela") como para *client-to-site* (*remote access*);

2.1.51. Deve permitir a criação de túneis VPN SSL/TLS;

2.1.52. Deve permitir a criação de túneis VPN IPSec;

2.1.53. A funcionalidade de VPN prevista no item anterior poderá ser atendida por meio de dispositivo *standalone*, caso o *appliance* do *firewall* não possua tal funcionalidade, sem prejuízo do gerenciamento centralizado da solução previsto nos itens 2.1.69 e 2.2;

2.1.54. Deve permitir que o usuário realize a conexão VPN por meio de cliente instalado no sistema operacional do seu equipamento ou por meio de interface *Web* do tipo portal.

2.1.54.1. Caso seja por meio de cliente instalado, deverá estar disponível, no mínimo, para os sistemas operacionais Windows (Vista, 7, 8 e 10). Caso não existam clientes (softwares) dos próprios fabricantes instaláveis para os sistemas operacionais: Linux, Mac OS X, Apple iOS e Google Android, deverá a Licitante fornecer gratuitamente softwares de terceiros que sejam totalmente compatíveis com os sistemas operacionais referidos.

2.1.54.2. O acesso por meio da interface Web deverá ser compatível com, no mínimo, os navegadores Internet Explorer 9 ou superior e Firefox 4.0 ou superior.

2.1.55. Deve suportar a customização da interface *Web* para acesso a VPN pelos administradores do sistema, incluindo quais aplicativos, servidores e sistemas estarão acessíveis via portal;

2.1.56. Suportar algoritmos de criptografia para túneis VPN AES-128 e AES-256;

2.1.57. Suportar os algoritmos para definição de chave de cifração 3DES e AES;

2.1.58. Suportar os algoritmos RSA, *Diffie-Hellman/*RSA;

2.1.59. Suportar Certificado Digital X.509 v3;

2.1.60. Suportar a inclusão (*enrollment*) de autoridades certificadoras;

2.1.61. Permitir alteração dos algoritmos criptográficos das VPNs;

2.1.62. Suportar IKE – *Internet Key Exchange,* fases I e II;

2.1.63. Suportar os protocolos de roteamento RIPv2, OSPFv2 ou OSPFv3 para as funcionalidades de VPN;

2.1.64. Implementar autenticação de usuários utilizando LDAP, Microsoft *Active Directory,* RADIUS e certificados digitais e suportar, no mínimo, autenticação *two-way* com certificado digital e LDAP ou Microsoft Active Directory ou RADIUS.

2.1.65. Suportar certificados emitidos por autoridade certificadora no padrão ICP-Bra sil;

2.1.66. Suportar leitura e verificação de *Certificate Revogation List* (CRL);

2.1.67. Suportar NAT *Transversal Tunneling* (NAT-T);

2.1.68. Possuir gerenciamento gráfico das funcionalidades de VPN e monitoramento de seus eventos de forma integrada tanto com a gerência loca do equipamento ou do cluster quanto com a gerência centralizada da solução.

2.1.69. VPN gateway-a-gateway deverá possuir interoperabilidade com os gateways de VPN pelo menos dos seguintes fabricantes: Cisco, Checkpoint, Juniper, Palo Alto Networks, Fortinet, AKER, BluePEX, PFSense e SonicWall.

2.1.70. Deve permitir a aplicação de políticas de segurança e visibilidade para as aplic ações que circulam dentro dos túneis de SSL.

2.1.71. O equipamento deve ser apropriado para o uso em ambiente tropical com umidade relativa na faixa de 20 a 85% (sem condensação) e temper atura ambiente na faixa de 5 a 40°C.

2.2. Solução de gerência centralizada

2.2.1. Deverá ser fornecida solução de gerência centralizada dos *firewalls*, do mesmo fabricante e independente (externa) em relação aos e quipamentos, sendo que:

2.2.1.1. A solução poderá ser fornecida baseada em "appliance especializado" – equipamento especializado para gerência centralizada, ou "appliance virtual" - solução de *software* executada em máquina virtual que possa ser instalado e executado me ambientes virtuais ou componentes de *software* instaláveis em sistemas operacionais padrão servidor;

2.2.1.2. Quando a solução for baseada em "appliance especializado", ou quando quaisquer outros equipamentos forem fornecidos para compor a solução, deverão:

a) ser compatíveis com rack padrão 19 polegadas;

b) possuir, no mínimo, duas interfaces de rede Gigabit Ethernet;

c) possuir fonte de energia com os mesmos parâmetros definidos no item 2.1.7;e

d) possuir, no mínimo, o espaço de armazenamento solicitado no respectivo item 7 de cada um dos lot es do item 3;

2.2.1.3. Quando a solução for baseada em appliance virtual, deverá ser capaz de ser executada em pelo menos uma das seguintes plataformas virtualizadoras: VMware ESXi, Xen, KVM ou Microsoft Hyper-V, cujo ambiente será fornecido pela CONTRATANTE, não sendo necessário o fornecimento da licença da plataforma virtualizadora. Caso o equipamento ou ambiente virtualizado disponibilizado pela CONTRATANTE seja incompatível com os requisitos mínimos necessários para execução completa da solução baseada em appliance virtual, a ponto de inviabilizar ou prejudicar o seu funcionamento e a fabricante da solução não possua outra alternativa de fornecimento dentre aquelas dispostas nos itens 2.2.1.1, 2.2.1.2 e 2.2.1.4, deverá ser fornecido equipamento com ambiente virtual compatível, observado o disposto no item 2.2.1.2;

2.2.1.4. Quando a solução for baseada em componentes de *software*, deverão ser fornecidas e implantadas, em caráter perpétuo, todas as licenças dos softwares e sistemas operacionais necessários ao funcionamento da solução, em versões para servidor, sendo que a versão fornecida de sistema operacional não poderá entrar em modo *End of Support* nos 60 (sessenta) meses a contar da data de assinatura do contrato.

2.2.2. Deve permitir a gerência centralizada dos equipamentos e contextos virtuais que compõem a solução de alta disponibilidade, devendo ser dimensionada e devidamente licenciada para atender, no mínimo, o número total de equipamentos físicos gerenciados e o número total de contextos virtuais possíveis, compatível com o limite operacional dos equipamentos e clusters gerenciados.

2.2.3 Deve ser licenciada de forma a não limitar número de usuários, objetos, regras de segurança, NAT e endereços IP.

2.2.4. Deve ser licenciada de forma a permitir a captura e filtragem de todos os eventos gerados por todos os equipamentos e contextos virtuais que compõe a solução de alta disponibilidade.

2.2.5. Deve permitir a criação e distribuição de políticas de segurança e de objetos de rede de forma centralizada.

2.2.6. Deve permitir a criação de relatórios customizados.

2.2.7. Deve possibilitar a filtragem dos *logs* do equipamento por, no mínimo: aplicação, endereço IP de origem e destino, país de origem e destino, usuário e horário.

2.2.8. Deve possuir relatórios com informações consolidadas sobre: as mais frequentes fontes de sessões bloqueadas com seus destinos e serviços, os mais frequentes ataques e ameaças de segurança detectadas com suas origens e destinos, os serviços de rede mais utilizados, as aplicações maiores consumidoras de banda de Internet, os usuários que consumem mais banda de Internet, os sítios na Internet mais visitados.

2.2.9. Deve permitir a geração automática e agendada dos relatórios.

2.2.10. Deve ser capaz de automatizar a aplicação das regras, objetos e políticas desejadas em tempo real a todos os equipamentos e contextos virtuais administrados.

2.2.11. Deverá utilizar comunicação segura criptografada entre a solução de gerência e os equipamentos gerenciados.

2.2.12. Deverá manter o histórico de configurações enviadas aos equipamentos e deverá permiti o *rollback* das configurações.

2.2.13. Deve permitir distribuição centralizada de pacotes de atualização.

2.2.14. Deve permitir validar as regras antes, durante ou depois de aplicá-las.

2.2.15. Deve ser capaz de testar a conectividade dos equipamentos gerenciados.

2.2.16. Deve prover funcionalidade de detecção de regras conflitantes ou regras equivalentes.

2.3. Conjunto de funcionalidades IPS/IDS

2.3.1. Possuir tecnologia de detecção e prevenção de ataques e intrusões baseada em assinatura;

2.3.2. Possuir, no mínimo, um conjunto de 2.000 (duas mil) assinaturas de detecção e prevenção de ataques, devendo também detectar ataques baseado s em anomalias;

2.3.3. Decodificar múltiplos formatos de *Unicode*;

2.3.4. Suportar fragmentação e desfragmentação IP;

2.3.5. Detectar protocolos independentemente da porta utilizada, identificando aplicações conhecidas em portas não-padrão;

2.3.6. Detectar e Proteger contra, no mínimo, ataques de RPC (*Remote Procedure Call*), Windows ou NetBios, SMTP (*Simple Message Transfer Protocol*), IMAP (*Internet Message Access Protocol*), *Sendmail* ou POP (*Post Office Protocol*), DNS (*Domain Name System*), FTP, SSH , Telnet, ICMP (*Internet Control Message Protocol*), SIP, SNMP, SSDP ou CHARGEN, RDP (*Remote Desktop Protocol*), DoS (*Denial of Service*) e ataques com assinaturas complexas, tais como ataques *TCP hijacking*.

2.3.7. Possuir proteção contra os ataques como, mas não restringindo-se ao s mesmos : 1) Ataques de *Worm*, *Trojan*, *Backdoors*, *Portscans*, IP *Spoofing*, DoS, *Spywares,* Botnets e malwares em geral; 2) Ataques e utilização de tec nologia P2P; 3) Ataques de estouro de pilha (*buffer overflow*); 5) Tráfego mal formado; 6) Cabeçalhos inválidos de protocolo; 6) Ataques de injeção (SQL *Injection*, LDAP *Injection*) e de *Cross-Site Scripting;* 7) Elevação de privilégio e 8) *Exploits - Web Server, Web Browser ActiveX, JavaScript, Browser Plug-ins/Add-nos*.

2.3.8. Emitir alarmes na console de administração integrada, alertas via correio eletrônico, *syslog* e traps SNMP;

2.3.9. Permitir monitoração do comportamento do equipamento mediante o protocolo SNMP;

2.3.10. Atualizar automaticamente as assinaturas para o sistema de detecção de i ntrusos;

2.3.11. Permitir filtros de anomalias de tráfego estatístico de*flooding*, *scan e source session limits*;

2.3.12. Permitir filtros de anomalias de protocolos, inclusive protocolos de aplicação (ex.: HTTP, SMTP, NTP, NetBIOS, HTTPS, FT P, DNS, SMB, RPC, SSH e Telnet);

2.3.13. Deve resistir a técnicas de evasão ou ataques direcionados ao próprio equipamento, suportando, no mínimo, as técnicas: IP *Packet Fragmentation*, *Stream Segmentation*, RPC *Fragmentation*, URL *Obfuscation*, HTML *Obfuscation*, *Payload Encoding*, FTP *Evasion* e *Layered Evasions*.

2.3.14. Possuir funcionalidade que permita desativar a análise de assinaturas e protocolos;

2.3.15. Possuir funcionalidade que permita desativar a análise de ataques a partir de endereços/faixa IP específicos;

2.3.16. Permitir o funcionamento mínimo do *engine* de IPS mesmo que a comunicação com o *site* do fabricante esteja fora de operação;

2.3.17. Possuir as estratégias de bloqueio e liberação selecionáveis, tanto por conjuntos de asinaturas quanto por cada assinatura;

2.3.18. Suportar a verificação de ataques na camada de aplicação;

2.3.19. Possuir gerenciamento gráfico centralizado das funcionalidades de IPS/IDS e monitoramento de seus eventos de forma integrada com a gerência local e a gerência centralizada da solução.

2.3.20. Reconhecer assinaturas seletivas e filtros de ataque que devem proteger contra ataques de negação de serviços automatizados, *worms* e vulnerabilidades conhecidas.

2.3.21. Caso o IPS/IDS não trate parcialmente ou totalmente DoS, será aceito funcionalidade específica complementar.

2.4. Conjunto de funcionalidades antivírus e *anti-malware*

2.4.1. Possuir módulo de proteção de antivírus, *anti-malware e anti-bot* no mesmo equipamento do *firewall*;

2.4.2. Possuir funcionalidade de varredura contra vírus e *malwares* em tráfego nos seguintes protocolos: HTTPS, HTTP e pelo menos doisdos seguintes: FTP, POP3, IMAP e SMTP;

2.4.3. Deve ser capaz de, se houver algum atraso ou falha na realizaç ão da atualização automática, o equipamento deve ter a capacida de de alertar imediatamente o administrador através de*logs*, *e-mail* ou outros meios de alerta;

2.4.4. Deve possuir serviço de atualização automática e manual de assinaturas com o fabri cante;

2.4.5. Suportar funcionamento mínimo da *engine* de antivírus e *anti-malwares* mesmo que a comunicação com o *site* do fabricante esteja fora de operação;

2.4.6. Possuir gerenciamento gráfico centralizado das funcionalidades de antivírus e *anti-malware* integrado com a gerência local e a gerência centralizada da solução .

2.4.7. Identificação, classificação e bloqueio de malwares, contemplando no mínimo, Trojan, Spywares, Backdoors, Worms e Vírus;

2.5. Conjunto de funcionalidades para tratamento de conteúdo web

2.5.1. Deve possuir funcionalidades de tratamento de conteúdo web, devendo sua base de dados conter, no mínimo, 10 (dez) milhões de *sites* internet *web* já registrados e classificados, distribuídos em, no mínimo, 40 (quarenta) categorias ou subcategorias pré-definidas;

2.5.2. Permitir a criação de categorias personalizadas;

2.5.3. Permitir a categorização e reclassificação de *sites web* por URL;

2.5.4. Suportar filtragem e categorização das URLs;

2.5.5. Possuir integração com serviços de diretório LDAP e Microsoft *Active Directory* para autenticação de usuários;

2.5.6. Permitir a criação de regras de acesso/bloqueio baseadas em usuários ou grupo de usuários do LDAP e do Microsoft *Active Directory;*

2.5.7. Permitir a criação de regras para acesso/bloqueio por endereço IP de origem e s ub-rede de origem;

2.5.8. Permitir a criação de quotas de utilização por horário, ou por categorias, ou por aplica ções;

2.5.9. Deve ser capaz de exibir mensagem de bloqueio customizável pelos Administradores para resposta aos usuários, na tentativa de acessoa recursos proibidos ou restringidos pela política de segurança do órgão;

2.5.10. Permitir o bloqueio de páginas web por meio da construção de filtros específicos com mecanismo de busca textual;

2.5.10.1. O item 2.5.10 pode ser atendido através da criação de aplicações em camada 7 customizadas.

2.5.11. Permitir o bloqueio de URLs cujo campo CN ou DN não contém um domínio válido para o certicadof SSL;

2.5.12. Permitir o bloqueio de páginas web por classificação, tais como páginas de streaming, rádio e tv*online*, P2P, URLs originadas de spam, sites de proxy anônimos, entre outros.

2.5.13. Permitir a criação de listas personalizadas de URLs permitidas – lista br anca e bloqueadas – lista negra;

2.5.14. Possuir categorização de sites governamentais nacionais, mesmo não tendo domínio ".gov" ou".gov.br ."

2.5.15. Categorizar as URLs com taxa de acerto mínima de 80% (oitenta por cento), não sendo cons ideradas neste percentual categorização genérica ou similar.

2.5.16. Suportar e forçar pesquisas seguras em pelo menos dois sistemas de buscas, contempla ndo Google e/ou Bing e/ou Yahoo.

2.6. Conjunto de funcionalidades para controle de aplicações e análise profunda

2.6.1. Possuir módulo de filtro de aplicações e de conteúdo desenvolvido e mantido pelo próprio fabricante, no mesmo equipamento do *firewall*;

2.6.2. Deve ser capaz de identificar as aplicações mesmo que não estejam utilizan do sua porta default.

2.6.3. Deve ser capaz de identificar aplicações encapsuladas dentro de protocolos, como HTT P e HTTPS.

2.6.4. Deve ser capaz de identificar aplicações que utilizam comunicação criptogr afada através de SSL.

2.6.5. Permitir o agrupamento de aplicações em grupos personalizados;

2.6.6. Garantir que as atualizações regulares do produto sejam realizadas de forma tr ansparente, sem paradas perceptíveis dos serviços;

2.6.7. Identificar aplicações e permitir ou bloquear sua utilização, independentemente das portas e protocolos utilizados para conexão (inclusive tráfego criptografado), assim como possuir categorias para classificação das aplicações, bem como das técnicas de evasões utilizadas;

2.6.8. Possuir, no mínimo, proteção para aplicações do tipo P2P, *Instant Messaging*, *Web* e VOIP;

2.6.9. Possuir perfis/políticas de segurança de aplicações pré-definidas/pré-configuradas na solução;

2.6.10. Possuir atualização manual e automática de novas assinaturas;

2.6.11. Permitir a criação de regras de acesso/bloqueio baseadas em usuários ou grupo de usuários do LDAP e do Microsoft *Active Directory;*

2.6.12. Deve ser capaz de identificar e filtrar um mínimo de 1.500 (mil e quinhentas) aplicações, contemplando no mínimo: peer-to-peer, streaming e download de áudio, streaming e download de vídeo, update de software, instant messaging, redes sociais, proxies, anonymizers, acesso e controle remoto, VOIP e email.

2.6.13. Identificação, bloqueio e restrição em profundidade e granularidade de aplicações, contemplando no mínimo: *Bittorrent, Youtube, Livestream, Skype, Viber, WhatsApp, Snapchat, Facebook, Facebook Messenger, Google+, Google Talk, Google Docs, Instagram, Twitter, LinkedIn, Dropbox, Google Drive, One Drive, Logmein, Teamviewer, MS-RDP, VNC, Ultrasurf, TOR e Webex.*

2.7. Treinamento oficial para até 5 pessoas

2.7.1. Deverá ser fornecido Voucher para treinamento oficial do fabricante.

2.7.2. A carga horária do treinamento não poderá ser inferior a 24 horas, sendoadac voucher apto para até 5 pessoas. O treinamento é composto por turmas que podem ser formadas de um ou mais Vouchers de uma entidade CONTRATANTE, ou ainda, ser uma turma compartilhada por mais de uma entidade CONTRATANTE. Nos dois casos cada turma se limita a no máximo 10 pessoas.

2.7.3. Os treinamentos deverão ser realizados no Brasil, em português, na modalidade presencial, em local fornecido pela CONTRATADA.

2.7.3.1. O local de treinamento deverá possuir todas as facilidades para um perfeito desempenho das atividades, incluindo os recursos áudio visual e laboratórios necessários, sem ônus algum para a CONTRATANTE.

2.7.4. Caberá à CONTRATADA prover todos os recursos didáticos necessários à realização do treinamento, incluindo (mas não se restringi ndo a) sala de aula, data show, apostilas, bloco de anotações e caneta para cada treinando.

2.7.5. Os treinamentos deverão ocorrer usando-se turnos diários de até 4 horas cada, podendo ser dois turnos no mesmo dia ou um turno por dia a ser acordado com a CONTRATANTE, com intervalos de, no mínimo, 15 minutos em cada turno e de pelo menos 1 hora entre os turnos que ocorrerem no mesmo dia.

2.7.6. Toda a documentação didática necessária aos cursos de treinamento deverá ser disponibilizada em papel impresso e mídia digital.

2.7.7. Os cursos referentes a equipamentos e *softwares* que façam parte do objeto deverão usar o material oficial de treinamento do respectivo fabricante por meio de qualquer um dos seus respectivos centros autorizados de treinamento.

2.7.8. São produtos esperados de todos os treinamentos:

2.7.8.1. Aulas teóricas e práticas.

2.7.8.2. Material didático contratado e aprovado pela CONTRATANTE.

2.7.8.3. Referências para estudos e pesquisas complementares.

2.7.9. A CONTRATANTE poderá, a seu critério, reproduzir o material didático usado, treinar multiplicadores para repetir o treinamento sem custos adicionais. E tal ação não representa a quebra do direito de propriedade do fabricante ou da empresa C ONTRATADA. Isso porque o material fornecido não será usado para fins comercias, mas apenas para uso interno do órgão ou entidade C ONTRATANTE com o intuito de disseminar o conhecimento da solução entre os seus servidores profissionais técnicos.

2.7.10. Os custos referentes ao deslocamento, hospedagem e alimentação dos treinados serão de responsabilidade da CONTRATANTE.

2.7.11. A ementa do curso deve abranger conteúdos que vão desde configurações básicas até as avançadas dos equipamentos de hardware e de *softwares* que compõem a solução, bem como sua operação.

3. DEFINIÇÃO DOS LOTES E ITENS

3.1. LOTE 1 - Item 1: Firewall multifuncional Tipo1

3.1.1. Requisitos específicos:

3.1.1.1. Atender a todos os requisitos do item 2.1;

3.1.1.2. Possuir, no mínimo, o *throughput* de inspeção de 100 Mbps para todas as funcionalidades dos itens 2.1, 2.2, 2.3, 2.4, 2.5 e 2.6, ativadas simultaneamente e com inspeção integral de todos os pacotes de dados, independentemente de seu tamanho ou direção de fluxo, levando-se em consideração o perfil de tráfego descrito no ANEXO E.

3.1.1.3. O equipamento deve possuir no mínimo 01 (uma) fonte de alimentação, a qual pode ser interna ou externa, com alimentação nominal de 100~120VAC e 210~230VAC e frequência de 50 ou 60 Hz, ou*auto- ranging*. Deverá vir acompanhado de cabo de alimentação com, no mínimo, 1,80m (6 pés), com plug tripolar 2P+T no padrão ABNT NBR 14136.

3.1.1.4. Possuir no mínimo 4 (quatro) portas de 10/100/1000 BASE T.

3.1.1.5. *Throughput* mínimo de 50 Mbps para IPSec VPN.

3.1.1.6. Quantidade mínima de 50.000 sessões simultâneas.

3.1.1.7. Quantidade mínima de 5.000 novas sessões por segundo

3.2. LOTE 1 - Item 2: Conjunto de funcionalidades IPS/IDS

3.2.1. Atender a todos os requisitos do item 2.3.

3.3. LOTE 1 - Item 3: Conjunto de funcionalidades antivírus e *anti-malware*

3.3.1. Atender a todos os requisitos do item 2.4;

3.4. LOTE 1 - Item 4: Conjunto de funcionalidades para tratamento de conteúdo web

3.4.1. Atender a todos os requisitos do item 2.5;

3.5. LOTE 1 - Item 5: Conjunto de funcionalidades para controle de aplicações e análise profunda

3.5.1. Atender a todos os requisitos do item 2.1.39 e do item 2.6;

3.6. LOTE 1 - Item 6: Treinamento oficial para até 5 pessoas

3.6.1. Atender a tudo que foi exposto no item 2.7;

3.7. LOTE 1 – item 7: Solução de gerência centralizada

3.7.1. Requisitos específicos:

3.7.1.1. Atender a todos os requisitos do item 2.2

3.7.1.2. Possuir capacidade mínima de 100 GB para armazenamento de logs e eventos

3.8. LOTE 2 - item 01: Firewall multifuncional tipo 2

3.8.1. Requisitos específicos:

3.8.1.1. Atender a todos os requisitos do item 2.1;

3.8.1.2. Possuir, no mínimo, o *throughput* de 250 Mbps para todas as funcionalidades dos itens 2.1, 2.2, 2.3, 2.4, 2.5 e 2.6, ativadas simultaneamente e com inspeção integral de todos os pacotes de dados, independentemente de seu tamanho ou direção de fluxo, levando-se em consideração o perfil de tráfego descrito no ANEXO E.

3.8.1.3. O equipamento deve possuir no mínimo 01 (uma) fonte de alimentação, que pode ser interna ou externa, com alimentação nominal de 100~120VAC e 210~230VAC e frequência de 50 ou 60 Hz, ou*auto-ranging*. Deverá vir acompanhado de cabo de alimentação com, no mínimo, 1,80m (6 pés), com plug tripolar 2P+T no padrão ABNT NBR 14136.

3.8.1.4. Possuir no mínimo 4 (quatro) portas de 10/100/1000 BASE-T.

3.8.1.5. Quantidade de sessões simultâneas 90.000.

3.8.1.6. Quantidade de novas sessões por segundo 12.000.

3.8.1.7. *Throughput* mínimo de 50 Mbps para IPSec VPN.

3.9. LOTE 2 – item 2: Conjunto de funcionalidades IPS/IDS

3.9.1. Atender a todos os requisitos do item 2.3;

3.10. LOTE 2 - item 3: Conjunto de funcionalidades antivírus e anti-malware

3.10.1. Atender a todos os requisitos do 2.4;

3.11. LOTE 2 – item 4: Conjunto de funcionalidades para tratamento de conteúdo web

3.11.1. Atender a todos os requisitos do item 2.5;

3.12. LOTE 2 – item 5: Conjunto de funcionalidades para controle de aplicações e análise profunda

3.12.1. Atender a todos os requisitos do item 2.1.39 e do item 2.6;

3.13. LOTE 2 - item 6: Treinamento oficial para até 5 pessoas

3.13.1. Atender a tudo o que foi exposto no item 2.7.;

3.14. LOTE 2 – item 7: Solução de gerência centralizada

3.14.1. Requisitos específicos

3.14.1.1. Atender a todos os requisitos do item 2.2;

3.14.1.2. Possuir capacidade mínima de 250 GB para armazenamento de logs e eventos