PODER
JUDICIÁRIO
DE ALAGOAS

TERMO DE REFERÊNCIA

Processo Administrativo nº 2023/2008

Aquisição de solução para proteção do perímetro de rede do TJAL

Maceió, maio de 2023

Diretoria Adjunta de Tecnologia da Informação - DIATI

Histórico de Revisões

Data	Versão	Descrição	Autor
29/04/2022	1.0	Versão inicial do T.R.	Equipe de planejamento
02/05/2022	1.1	Modificação do item 4.6	Equipe de planejamento
24/05/2022	1.2	Mudança nos requisitos do Anexo TR1	Equipe de planejamento
27/05/2022	1.3	- Inserção do item 4.2.8.2.1 - Mudanças no cronograma global de execução	Equipe de planejamento
06/06/2022	1.4	Ajuste no item 4.4	Equipe de planejamento
26/07/2022	1.5	Mudança nos requisitos do Anexo TR1	Equipe de planejamento
10/08/2022	1.6	Mudança nos requisitos do Anexo TR1	Equipe de planejamento
15/08/2022	1.7	Mudança nos requisitos do Anexo TR1	Equipe de planejamento
11/05/2023	1.8	Adequações para adesão à ARP	Equipe de planejamento

SUMÁRIO

1. OBJETO DA CONTRATAÇÃO

1.1 O presente instrumento tem por objeto a aquisição de solução de segurança para o perímetro de rede do TJAL, abrangendo proteção do tipo *Next Generation Firewall* (NGFW) de alta disponibilidade, o que inclui suporte e garantia do fabricante, assinaturas de proteção, suporte técnico em repositório mundial do fabricante, suporte técnico do fabricante local e/ou remoto e serviços de instalação e treinamento.

2. BENS E SERVIÇOS QUE COMPÕEM A SOLUÇÃO

2.1. O objeto desta pretensão está consumado em lote único, subdividido da seguinte forma:

LOTE ÚNICO **Firewall de Próxima Geração (*Next Generation Firewall – NGFW)***			
Descrição: Disponibilizado como solução on-premisse, em cluster, com garantia e suporte técnico, subscrição, instalação, treinamento e consultoria especializada.			
Id.	**Descrição do Bem ou Serviço**	**Unidade**	**Qtde/Duração**
1	Solução de segurança da informação do tipo Next Generation Firewall (NGFW), com garantia, suporte técnico e licença de uso por 48 meses	equipamento	2
2	Serviço de instalação e configuração profissional dos equipamentos	serviço	2
3	Treinamento oficial do fabricante	curso	1
4	Consultoria técnica especializada da solução	UST	200

3. FUNDAMENTAÇÃO DA CONTRATAÇÃO

3.1. CONTEXTUALIZAÇÃO E JUSTIFICATIVA

3.1.1. A prestação jurisdicional na Justiça Alagoana depende diretamente dos serviços de TIC que sustentam os sistemas informatizados da Corte. Para sustentar o funcionamento dos sistemas são necessários vários tipos de redes de comunicação, entre elas a Internet, as redes locais dentro das dependências do TJAL (redes LAN) e as redes privadas que conectam o TJAL a funcionários e parceiros. Toda a segurança dos dados que circulam entre todas as redes de dados do Tribunal, nos seus diferentes níveis de interligações, é promovida pelo equipamento Firewall, tornando este equipamento imprescindível para o negócio do Tribunal.

3.1.2. Visando a garantir melhores condições de segurança da informação, com vistas à integridade dos processos eletrônicos judiciais e administrativos e demais serviços à disposição dos jurisdicionados, faz-se necessário a implantação de soluções que atuem no controle e segurança das informações, nas camadas de rede mais avançadas, em nível de aplicação (camada 7), além do controle de aplicações mais específicas e direcionadas, servidas mediante os protocolos HTTP e HTTPS, relacionados aos portais Web, de modo a minimizar os riscos de exploração de possíveis ameaças e que permitam, por meio de alarmes e controles, uma rápida resposta do Tribunal em caso de incidentes de segurança.

3.1.3. Atualmente o Tribunal de Justiça de Alagoas (TJAL) mantém em seu datacenter 2 (dois) equipamentos de Firewall do tipo Next Generation Firewall (NGFW), modelo Fortigate 500E, que funcionam como um único cluster. Estes equipamentos funcionam em regime de comodato por meio do contrato de prestação de serviço nº 10/2018 e são utilizados para prover restrição de tráfego malicioso ente a Internet e a rede local, além funcionar como um gateway para serviços relevantes do Tribunal, como a Rede Privada Virtual (VPN – Virtual Private Network), por exemplo.

3.1.4. Após alguns estudos, observaram-se as seguintes oportunidades de melhoria em relação a este contrato:

3.1.4.1. O serviço de fornecimento dos firewalls, imerso no contrato 10/2018, é agregado a um serviço de fornecimento de link de internet, ambos providos por uma única empresa. Desmembrando estes objetos potencializará a competição entre empresas interessadas, cada qual especializada no fornecimento de um objeto específico, aumentando as chances de se obter uma melhor relação custo-benefício para a Administração.

3.1.4.2. Buscou-se adquirir os firewalls ao invés de repetir o modelo de contratação atual. Este modelo de contratação, provida como serviço, atualmente carece de maturidade no âmbito da Administração Pública. Em outras palavras, o provimento dos equipamentos – em comodato – conjugado à terceirização da operacionalização destes ainda é infimamente presente em contratos públicos. Desta forma, não é trivial obter parâmetros de preço e desempenho que minimizem os riscos de uma eventual perpetuação deste tipo de serviço. Ademais, a aquisição dos firewalls, atrelado ao treinamento especializado, dará mais autonomia ao *staff* da CONTRATANTE para administrar e operar o produto.

3.1.4.3. O modelo Fortigate 500E, atualmente em operação, está apresentando indícios de subdimensionamento, para determinadas funções, em relação à atual demanda da Corte Alagoana. Na fase de estudos preliminares, uma ampla análise de mercado foi realizada com o objetivo de parear, com a maior precisão possível, as necessidades institucionais e tecnológicas do TJAL com o que o mercado poderia oferecer na área de Segurança da Informação, mais precisamente na área de Firewall de Próxima Geração. Portanto, esta pretensão traduz os anseios da Corte Alagoana de se obter uma solução de Firewall mais robusta, visando o aprimoramento da Segurança da Informação no curto, médio e longo prazo.

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

3.2. ALINHAMENTO AOS INSTRUMENTOS DE PLANEJAMENTO INSTITUCIONAIS

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

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

3.3. ESTIMATIVA DA DEMANDA

3.3.1. A estimativa da demanda está lastreada em uma pesquisa de mercado quando, na oportunidade, foram levantados os atuais requisitos técnicos e tecnológicos da Corte Alagoana e as soluções que as empresas do ramo poderiam oferecer para atender a estes requisitos. Mais detalhes estão expressos no Documento de Estudos Técnicos Preliminares da Contratação, incluso nos autos.

3.4. PARCELAMENTO DA SOLUÇÃO DE TIC

3.4.1. Os serviços associados às soluções de segurança, incluindo instalação e treinamento, possuem alta correlação técnica entre si, de forma que é bastante recomendável que sejam adjudicados a um único fornecedor para que seja mantida a máxima compatibilidade técnica.

3.5. RESULTADOS E BENEFÍCIOS A SEREM ALCANÇADOS

3.5.1. A Segurança da Informação exerce papel preponderante para que este Egrégio Tribunal consiga satisfazer com efetividade sua missão institucional. Espera-se, com esta aquisição, a criação de um ambiente minimamente seguro para a sustentação dos serviços informatizados;

3.5.2. Os principais benefícios decorrentes da contratação vinculam-se à minimização dos riscos de perda de informações e de indisponibilidade no acesso aos sistemas internos e externos, e se mostra compatível e alinhada com a relevância e criticidade dos sistemas judiciais para as atividades desempenhadas pelo Tribunal de Justiça de Alagoas.

3.5.3. Além disso, espera-se com a pretendida contratação:

3.5.3.1. Maior visibilidade do tráfego de rede, possibilitando a detecção e proteção em tempo real contra ameaças;

3.5.3.2. Controle efetivo do tráfego de dados através de regras de segurança;

3.5.3.3. Detecção e prevenção contra ameaças e tentativas de invasão;

3.5.3.4. Monitoramento e rastreabilidade das atividades de rede;

3.5.3.5. Manter o monitoramento abrangente e eficiente sobre acessos à internet e tráfego de dados na rede corporativa de computadores;

3.5.3.6. Garantir que o TJAL esteja aderente às melhores práticas nacionais e internacionais da área de Segurança da Informação e em consonância com as normas vigentes, tais como a LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e o Marco Civil da Internet Lei nº 12.965/2014);

3.5.3.7. Garantir que o TJAL preste serviços de qualidade à sociedade, bem como atenda as próprias necessidades institucionais, com base nos pilares de confiabilidade, integridade e disponibilidade.

3.5.3.8. Promover proteção superior aos serviços disponibilizados de forma online;

3.5.3.9. Promover a melhoria da imagem do Poder Judiciário de Alagoas como provedor de serviços

4. REQUISITOS DO OBJETO

4.1. DAS ESPECIFICAÇÕES TÉCNICAS

4.1.1. A solução deverá ser composta por 2 (dois) equipamentos (appliances) funcionando em cluster, construídos especificamente para exercer a função de Next Generation Firewall, com hardware e software fornecidos pelo mesmo fabricante.

4.1.2. O software deverá ser fornecido em sua versão mais atualizada, relativo à data de sua instalação e configuração, não sendo permitido qualquer tipo de comprovação futura;

4.1.3. A solução deve vir acompanhada de todos os acessórios necessários (cabos, suportes, gavetas, braços, trilhos, etc.) para fixação em bastidor (rack) localizado nas dependências do CONTRATANTE;

4.1.4. A especificação técnica detalhada está presente no ANEXO TR1 – ESPECIFICAÇÃO TÉCNICA DA SOLUÇÃO, deste Termo de Referência.

4.2. DO SERVIÇO DE INSTALAÇÃO PROFISSIONAL E CONFIGURAÇÃO

4.2.1. A instalação dos equipamentos deverá ser realizada no *DataCenter* do CONTRATANTE;

4.2.2. Todo ferramental necessário para execução dos serviços de instalação, configuração inicial, incluindo *softwares*, equipamentos ou ferramentas, bem como eventuais materiais necessários para ligações temporárias, são de inteira responsabilidade da CONTRATADA;

4.2.3. A CONTRATANTE disponibilizará o espaço no *DataCenter*, assim como a infraestrutura elétrica até a posição onde serão instalados os equipamentos;

4.2.4. O equipamento deverá ser instalado na última versão de *firmware* disponível pelo fabricante;

4.2.5. Entende-se por configuração inicial para efeito deste Termo de Referência:

4.2.5.1. Elaboração, em conjunto com a equipe técnica do TJAL, de um Plano de Implantação e Configuração, segundo as melhores práticas do fabricante e considerando as demandas e características dos serviços do CONTRATANTE;

4.2.5.2. Realização da configuração inicial do equipamento ofertado, segundo projeto, e conforme padrão de endereçamento IP a ser fornecido pelo CONTRATANTE;

4.2.5.3. Realização de migração e adequação das regras vigentes no CONTRATANTE, incluindo migração de regras e políticas do cluster de firewalls em operação[1];

4.2.6. O Plano de Implantação e Configuração previsto no item 4.2.5.1, a ser fornecido pela CONTRATADA, deverá conter as seguintes informações, no mínimo:

4.2.6.1. Indicação do(s) técnico(s) da CONTRATADA que deverá(ão) ficar responsável(is) pela coordenação de todos os trabalhos de implantação dos serviços e que deverá(ão) estar presente(s) nas instalações do CONTRATANTE, ou outro endereço designado, para reuniões conjuntas de acompanhamento das atividades de implantação realizadas, com a equipe técnica indicada pelo CONTRATANTE, sempre que requisitado;

4.2.6.2. Cronograma das atividades de Implantação, indicando também as ações que envolvam interrupção dos serviços prestados pelo CONTRATANTE, para execução em janela de implantação fora do horário comercial. As ações serão analisadas pelo gerenciamento de risco e mudança da CONTRATANTE, podendo ser agendadas em horário não comercial de baixo impacto para os usuários.

4.2.7. A instalação e configuração inicial deverão contemplar, no mínimo:

4.2.7.1. Instalação física de todos os equipamentos em local determinado pelo CONTRATANTE;

4.2.7.2. Configuração das funcionalidades Next Generation Firewall, IPS, proteção avançada contra ameaças, QoS, controle de aplicativos e VPN IPSEC;

4.2.7.3. Migração das políticas de segurança existentes;

4.2.7.4. Criação dos usuários administradores;

4.2.7.5. Migração de perfis de usuários da VPN IPSEC;

4.2.7.6. Customização de regras de acesso de acordo com as necessidades do CONTRATANTE;

4.2.7.7. Substituição dos firewalls existentes;

4.2.7.8. Integração com o Active Directory;

4.2.7.9. Realização de backup das configurações;

4.2.7.10. Balanceamento de carga e otimização de uso entre os links de trânsito com a Internet;

4.2.8. A etapa de conclusão da instalação e configuração dos equipamentos deverá contemplar, no mínimo:

4.2.8.1. Testes de Aceite e Funcionamento, simulando todos os cenários possíveis de failover e failback;

4.2.8.2. Operação Assistida de Funcionamento da Solução, que consiste da disponibilização de um técnico residente, certificado pelo fabricante do equipamento, no endereço do CONTRATANTE, devidamente identificado, para sanar quaisquer dúvidas e problemas que ocorrerem na operação da solução, durante o prazo mínimo de 3 (três) dias úteis;

4.2.8.2.1. A operação assistida se iniciará a partir do 1º dia útil subsequente ao término da etapa de instalação e configuração;

4.2.8.3. Repasse de conhecimento das implementações realizadas, no formato “hands-on”, para no mínimo 8 funcionários designados pelo CONTRATANTE, com carga horária mínima de 8 horas;

4.2.8.3.1. O repasse de conhecimento deverá ser comprovado através de uma lista de presença com a assinatura de todos os presentes;

4.2.8.4. Fornecimento da documentação de todo o projeto (AS-BUILT);

1 Fortinet Fortigate 500E

4.2.8.4.1. A documentação deverá ser desenvolvida sob a forma de relatório ou roteiro, de modo que a Equipe Técnica da CONTRATANTE possa absorver o conhecimento e aplicá-lo quando for necessário;

4.2.9. O serviço de instalação e configuração deverá ser realizado por técnico certificado oficialmente pelo fabricante da solução ofertada ou pelo próprio fabricante;

4.3. DO TREINAMENTO OFICIAL DO FABRICANTE

4.3.1. A CONTRATADA deverá fornecer treinamento oficial do fabricante, podendo ocorrer nas dependências do CONTRATANTE ou na modalidade à distância (EAD), a critério da CONTRATADA;

4.3.2. Ocorrendo treinamento nas dependências do CONTRATANTE, a infraestrutura local para o aluno será provida pela CONTRATANTE. A CONTRATADA deverá prover qualquer outro equipamento específico que seja exigido pelo fabricante para o aluno realizar o treinamento. Os laboratórios virtuais deverão ser providos pelo fabricante;

4.3.2.1. A CONTRATADA deverá informar, com antecedência mínima de 03 (três) dias úteis à CONTRATANTE as necessidades de infraestrutura e de acesso aos laboratórios virtuais para realização do treinamento;

4.3.3. O treinamento deverá ser focado na aprendizagem e no desenvolvimento de habilidades práticas necessárias para configurar e gerenciar o ambiente;

4.3.4. O treinamento deverá habilitar o participante a gerenciar a solução e a realizar configurações referentes às funcionalidades especificadas nos requisitos técnicos da solução;

4.3.5. O treinamento deverá ter carga horária de, no mínimo, 40 (quarenta) horas;

4.3.6. Todos os treinamentos deverão ser ministrados na língua portuguesa, por instrutor certificado pelo fabricante, em dias úteis consecutivos, em horário comercial (entre 8h e 18h), com carga máxima de 8h (oito horas) por dia;

4.3.7. Deverão ser fornecidos materiais didáticos e certificados oficiais do fabricante referente à participação, contendo, no mínimo, as seguintes informações: nome do participante, especificação da tecnologia, carga horária e período;

4.3.7.1. Os certificados deverão ser entregues no prazo de 10 (dez) dias corridos contados após o término do treinamento, sem ônus adicional para a CONTRATANTE;

4.3.8. A CONTRATANTE emitirá nota(s) de empenho e ordem de fornecimento para confirmar as reservas, identificando a relação de alunos que participarão.

4.4. DOS REQUISITOS DE GARANTIA E SUPORTE TÉCNICO

4.4.1. A garantia será aquela usualmente fornecida pelo fabricante acrescida dos Níveis Mínimos de Serviço (NMS) e demais condições estabelecidas neste Termo de Referência;

4.4.2. A garantia para todos os equipamentos será de 48 (quarenta e oito) meses;

4.4.3. A garantia terá sua vigência contada a partir da data de conclusão do serviço de instalação e configuração profissional da solução (item 4.2), atestado pela equipe técnica da CONTRATANTE.

4.4.4. Todos os itens deverão possuir suporte ilimitado para abertura de chamados junto ao Fabricante;

4.4.5. O serviço de suporte técnico vinculado à garantia deverá ser prestado de forma ininterrupta no regime 24x7 (vinte e quatro horas durante sete dias por semana), inclusive em feriados e deverá cobrir todo e qualquer defeito e/ou problema apresentado nos equipamentos ou serviços da solução de firewall, peça ou componente, incluindo esclarecimentos técnicos para ajustes, reparos, instalações, configurações e correções necessárias, sem qualquer custo adicional para a CONTRATANTE;

4.4.6. A CONTRATADA deve fornecer o acesso da CONTRATANTE à Central de Suporte Técnico da CONTRATADA para abertura de chamados.

4.4.6.1. A interação entre a CONTRATANTE e a Central de Suporte Técnico da CONTRATADA deve ser possibilitada através de chamada telefônica a custo local ou gratuita de qualquer operadora e

através de sistema web, ambas as formas devem ser disponibilizadas no idioma português do Brasil.

4.4.6.2. No momento da abertura do chamado, deve ser informado à CONTRATANTE o número do chamado, a previsão de atendimento, que será baseada na criticidade do chamado, e o nome do responsável pelo atendimento. Todas estas informações deverão ficar disponíveis no sistema web de chamados para consulta pela CONTRATANTE. O nível de criticidade do chamado deve ser informado pela CONTRATANTE no momento da abertura do chamado e registrado para fins de revisão do tempo de atendimento.

4.4.7. O início de atendimento e da resolução do serviço de garantia será a hora da comunicação feita pelo CONTRATANTE à CONTRATADA, conforme sistema de registro do próprio solicitante;

4.4.8. A manutenção realizada on-site (procedimentos realizados no local de instalação) será sempre efetuada com o acompanhamento de um servidor do quadro do CONTRATANTE;

4.4.8.1. Quando não for possível a execução do serviço, em razão da ausência de servidor para acompanhamento, deve o técnico anotar este fato no relatório junto com o tempo de espera;

4.4.9. O prazo de garantia deverá contemplar:

4.4.9.1. Atualizações para novas versões e releases de software lançadas durante a vigência do contrato;

4.4.9.2. Atualizações periódicas de todas as bases de assinaturas dos componentes;

4.4.9.3. Suporte para a instalação e configuração das novas versões e releases de software lançadas durante a vigência do contrato;

4.4.10. Em caso de defeitos de software que necessitem de desenvolvimento de correções pelo fabricante, o prazo deverá ser acordado com o CONTRATANTE;

4.4.11. Após concluído o suporte técnico, a CONTRATADA comunicará o fato à equipe técnica do CONTRATANTE e solicitará autorização para o fechamento do chamado. Durante o período de conclusão do suporte até a efetiva comunicação ao CONTRATANTE, o chamado permanecerá em espera, de forma a não haver penalização indevida à CONTRATADA. Caso o CONTRATANTE não confirme a solução definitiva do problema, o chamado será reaberto e os prazos de atendimento voltarão a ser considerados, até que seja efetivamente solucionado pela CONTRATADA;

4.4.12. O suporte técnico da CONTRATADA deve disponibilizar para a CONTRATANTE o acesso, por meio da Internet, à base de documentos e conhecimentos mantida pela fabricante da solução, contemplando seus manuais de instalação, utilização e correção de problemas, dicas de utilização, configuração e melhores práticas de uso, fóruns de discussão, boletins técnicos, download de firmwares, fixes e patches, dentre outros;

4.4.13. A CONTRATADA deverá manter em seu quadro de profissionais da equipe técnica, durante toda a vigência do contrato, pelo menos 1 (um) técnico com formação específica e oficial do fabricante para as atividades de instalação, configuração e suporte, envolvendo os equipamentos e programas da solução, a ser comprovada com certificado emitido pelo fabricante, ou empresa credenciada e qualificada para esta finalidade;

4.4.14. O CONTRATANTE encaminhará à CONTRATADA, quando da reunião de alinhamento de expectativas, relação nominal da equipe técnica autorizada a abrir e fechar chamados de suporte técnico;

4.4.15. Todas as solicitações de atendimento serão registradas pelo fiscal do contrato e pela CONTRATADA, para acompanhamento e controle da execução do contrato:

4.4.15.1. A CONTRATADA apresentará um Relatório de Atendimento, enviado por meio de correio eletrônico, contendo datas e horas de chamada, de início e de término do atendimento, descrição da necessidade de atendimento, e as providências adotadas e toda e qualquer informação pertinente ao chamado após o encerramento do mesmo;

4.4.15.2. A equipe técnica do CONTRATANTE informará à CONTRATADA quanto ao recebimento e aceite do Relatório de Atendimento;

4.4.16. Na abertura do chamado a CONTRATADA deverá fornecer o número de protocolo e o horário de abertura e encaminhar mensagem de correio eletrônico com tais informações para os endereços do fiscal do contrato em até meia hora após o registro, procedimento que servirá como evidência em caso de contestação de penalidades. O cálculo para aferição da desconformidade do tempo de resposta considerará o tempo de resposta descrito nos Níveis Mínimos de Serviço;

4.4.17. Quando a solução depender de ações do CONTRATANTE, o tempo de solução do chamado deve ser pausado até a conclusão da parte que não cabe à CONTRATADA, depois continuar de onde havia parado antes da solicitação do outro ator no processo;

4.4.18. Todas as ações provenientes de um chamado deverão ser amplamente comunicadas ao CONTRATANTE. Sendo que o CONTRATANTE deverá ser comunicado no mínimo em dois momentos, no início e no final de cada atendimento;

4.4.19. Toda indisponibilidade causada pela solução contratada poderá gerar multa de acordo com os Níveis Mínimos de Serviços detalhados no item 5.2;

4.4.20. Faculta-se à CONTRATADA substituir temporariamente o equipamento, peça ou componente defeituoso por outros que restabeleçam o serviço aos níveis de serviço acordados, quando então, a partir de seu pleno estado de funcionamento, ficará suspensa a contagem do prazo de solução definitiva;

4.4.20.1. A CONTRATADA deverá realizar a substituição definitiva do referido componente no prazo de 30 (trinta) dias corridos;

4.4.20.2. A substituição definitiva de componentes, caso necessário, deverá ser feita por itens novos e para primeiro uso;

4.4.21. Em havendo necessidade de retirada do equipamento para conserto em laboratório, esta deverá substituir o equipamento defeituoso por outro, igual ou superior, em regime 24x7 (vinte e quatro horas durante sete dias por semana), inclusive em feriados com entrega no próximo dia útil, para chamados abertos até às 14h. Após esse horário, o chamado passa a ser contado a partir do próximo dia;

4.4.22. Em caso de quebra, mau funcionamento, queda de desempenho ou qualquer outro fato causado por defeitos em componentes dos equipamentos, deverá ser realizado a troca dos componentes por novos, do mesmo modelo ou tecnicamente superiores, homologados pelo fabricante. Não serão aceitos componentes recondicionados ou usados anteriormente;

4.4.23. Qualquer substituição de componente, temporária ou definitiva, só será permitida após prévia avaliação técnica e autorização por parte da Equipe Técnica do CONTRATANTE.

4.5. DO LICENCIAMENTO (SUBSCRIÇÃO) DO NGFW

4.5.1. A licença deve permitir que todas as assinaturas, listas e demais métodos de detecção e prevenção de ameaças e de filtros de conteúdo e aplicação empregados pela solução sejam atualizados até suas últimas versões disponíveis.

4.5.2. A licença de uso deverá ter a mesma duração da garantia, contados a partir da aplicação destas nos produtos.

4.5.3. Deverá ser fornecida com licença(s) do(s) software(s) embutido(s) em todos os seus componentes. Após o seu término, a Contratante poderá continuar a utilizar o firewall e a console de gerência, isto é, a solução continuará funcionando mesmo sem contrato de suporte e de subscrição ativos;

4.5.4. Deverá ser licenciado e habilitado para uso ilimitado de usuários e endereços IP;

4.6. DA CONSULTORIA TÉCNICA ESPECIALIZADA

4.6.1. O modelo de contratação do serviço de consultoria para apoio técnico pontual, sob demanda, à critério e conveniência da CONTRATANTE, terá como referência a Unidade de Serviço Técnico (UST);

4.6.2. A UST é definida como unidade do item contratado aferido pelos resultados alcançados. Cada UST será equivalente a **01 (uma) hora** de esforço combinado dos profissionais técnicos e gerenciais (técnicos, analistas, consultores, gerentes de projeto) necessários para realização do serviço demandado pela CONTRATANTE;

4.6.3. Os serviços de consultoria corresponderão, essencialmente, aos recursos humanos técnicos e operacionais da CONTRATADA que sejam necessários para executar atividades técnicas específicas de arquitetura, implementação, gerência de projeto, suporte ou administração da solução contratada, devendo seguir as práticas preconizadas pelo modelo ITIL v3 ou v4 (Information Technology Infrastructure Library), PMBOK do PMI e demais preceitos legais pertinentes aos serviços envolvidos;

4.6.4. Este serviço não demandará alocação exclusiva de profissionais da CONTRATADA. Logo, não haverá caracterização de pessoalidade e subordinação direta na relação entre os profissionais da equipe da CONTRATADA e da CONTRATANTE;

4.6.5. A CONTRATADA deverá considerar em seus custos todas as variáveis para dimensionamento do esforço necessário para execução dos serviços, além das despesas com salários, encargos sociais e trabalhistas, seguros, impostos, taxas e contribuições, transporte, alimentação, despesas administrativas, lucros e demais insumos necessários à execução dos serviços definidos;

4.6.6. Os serviços serão prestados na modalidade *on-site* ou remoto, a depender da complexidade do serviço a ser executado, determinado através de comum acordo entre as partes;

4.6.7. Os serviços deverão ser prestados durante o expediente comercial (8h às 18h);

4.6.8. Os serviços não devem contemplar fornecimento de *software* ou *hardware*;

4.6.9. Os tipos de serviços a serem prestados pela consultoria, bem como os resultados esperados, incluem, mas não se limitam a:

Tipo do serviço	Resultado esperado
Arquitetura da solução	• Definição de arquitetura lógica e física de projeto e declaração de escopo (SoW), garantindo a qualidade durante a implantação e o atendimento de todos os requisitos funcionais e não funcionais; • Definir controles e monitoramento do ambiente, sugerindo métricas, *thresholds* e indicadores de acompanhamento; • Definir *playbooks* para automação e orquestração de respostas a incidentes; • Propor melhorias e apoio no planejamento e avaliação de mudanças; • Aconselhamento em comitês de segurança e governança; • Avaliar vulnerabilidades e propor ajustes e apoio no planejamento e execução de mudanças; • Planejamento de provas de conceito e ensaios para testes de verificação e consistência;
Suporte N2	• Análise e aplicação de *patches*, *fixes* e *updates* corretivos; • Aplicação de testes e realização de ensaios; • Atendimento a incidentes de suporte realizando análises, troubleshooting, diagnósticos; • Monitoração do ambiente; • Atualização das versões de *software*; • Ativação e configuração de novas funcionalidades incorporadas através de novas versões;
Melhoria Contínua	• Customização de ferramentas de gerenciamento, consultas, visões, relatórios; • Criação e manutenção de inventário; • Aplicação de tunning e hardening; • Otimização da plataforma, incluindo análise de conformidade da configuração implementada com as melhores práticas recomendadas pelo fabricante;

4.6.10. Os tipos de serviços do item anterior devem ser executados por profissionais com formação específica e oficial do fabricante, a ser comprovada com certificado válido emitido pelo fabricante;

4.6.11. A dinâmica do serviço de consultoria técnica obedecerá a seguinte sequência:

4.6.11.1. <u>Etapa de qualificação:</u>

4.6.11.1.1. A CONTRATANTE submeterá uma solicitação de estimativa de UST à CONTRATADA, detalhando a atividade pretendida, o resultado esperado, localidade e restrições, se existirem;

4.6.11.1.2. A CONTRATADA informará o macro escopo do serviço e a quantidade de USTs estimada para realização dos serviços, através de uma proposta formal;

4.6.11.1.3. A CONTRATANTE analisará a proposta e, caso concorde, emitirá Ordem de Fornecimento para a CONTRATADA executar os serviços;

4.6.11.2. Etapa de Execução:

4.6.11.2.1. Realizada(s) a(s) consultoria(s), a CONTRATADA deverá submeter para a CONTRATANTE a(s) Ordem(ns) de Fornecimento(s) que teve/tiveram conclusão atestada pela CONTRATANTE. A(s) ordem(ns) de Fornecimento deverá(ão) informar detalhadamente o tipo de serviço executado, o *flag* de prioridade, datas e horários de abertura, início de atendimento e conclusão de cada OS para análise da CONTRATANTE.

4.6.11.3. Etapa de aceite:

4.6.11.3.1. Em até 05 (cinco) dias úteis, a CONTRATANTE emitirá Termo de Aceite. Após emissão do Termo de Aceite, a CONTRATADA será informada do início do processo de liquidação e pagamento do serviço prestado, para que tome as devidas providências no sentido de realizar o envio dos documentos necessários ao pagamento.

4.6.12. Em eventuais requisições de serviços, a CONTRATADA deverá apresentar estimativa de consumo de UST em até 2 dias úteis, contados a partir do primeiro dia útil subsequente à data da requisição.

4.6.13. As atividades da consultoria técnica deverão ser iniciadas após emissão da Ordem de Fornecimento (OF) pela CONTRATANTE, dentro dos seguintes prazos:

4.6.13.1. Em até 5 (cinco) dias úteis após a emissão da O.F., para consultoria on-site;

4.6.13.2. Em até 2 (dois) dias úteis pós a emissão da O.F., para consultoria à distância;

4.6.14. O prazo de conclusão será estimado para cada demanda, individualmente;

4.7. DO LOCAL E PRAZO DE ENTREGA

4.7.1. O prazo para a entrega do objeto será de 60 (sessenta) dias corridos, a contar da assinatura do contrato ou do recebimento da nota de empenho pela Contratada, quando não houver instrumento contratual.

4.7.2. Os bens licitados deverão ser entregues no **Departamento Central de Material e Patrimônio do Poder Judiciário de Alagoas, localizado na Av. Juca Sampaio, nº 1049, CEP: 57040-600, Barro Duro, Maceió-AL. Telefones de contato: (82) 4009-3671 ou (82) 4009-3672**.

4.7.2.1. O horário para entrega dos bens é de 08:00 às 14:00, de segunda à sexta-feira.

4.7.3. Os equipamentos deverão vir acompanhados dos certificados de garantia do fabricante.

4.7.4. Na nota fiscal expedida, os valores e as descrições de todos os itens deverão estar de acordo com os descritos na proposta apresentada na licitação e aceita pela CONTRATANTE.

4.7.5. Na contagem dos prazos previstos neste documento, excluir-se-á o dia de início e incluir-se-á o dia do vencimento. Só se iniciam e vencem os prazos em dias úteis e de expediente do CONTRATANTE.

4.7.6. Serão considerados injustificados os atrasos não comunicados tempestivamente e indevidamente fundamentados. A aceitação da justificativa ficará a critério do Contratante.

4.7.7. Havendo pedido de prorrogação do prazo de entrega, este somente será concedido nas hipóteses previstas no Art. 57, §1°, da Lei nº 8.666/93, em caráter excepcional e sem efeito suspensivo, e deverá ser encaminhado por escrito, com antecedência mínima de 1 (um) dia do seu vencimento, anexando-se documento comprobatório do alegado pela Contratada.

4.7.8. Em casos excepcionais, autorizados pelo Contratante, o documento comprobatório do alegado poderá acompanhar a entrega do produto.

5. NÍVEIS MÍNIMOS DE SERVIÇO (NMS)

5.1.1. Os Níveis Mínimos de Serviço (NMS) visa garantir que o serviço contratado seja prestado pela CONTRATADA em grau mínimo de eficiência e qualidade exigido pela CONTRATANTE;

5.1.2. Os níveis mínimos de serviço serão aferidos mensalmente e eventuais descumprimentos serão comunicados à CONTRATADA;

5.1.3. A CONTRATADA será responsável pelo cumprimento e medição dos índices estabelecidos neste item que serão auditados pela CONTRATANTE durante todo o prazo de vigência do contrato, e que poderão ser revistos, a qualquer tempo, com vistas à melhoria ou ajustes na qualidade dos serviços prestados;

5.1.4. As inoperâncias e/ou indisponibilidades da solução contratada, no todo ou em parte, que não sejam de responsabilidade da CONTRATANTE, bem como insuficiência no alcance dos níveis mínimos de satisfação dos requisitos técnicos, representados por indicadores, deve gerar sanções proporcionais ao tempo e grau de desconformidade;

5.1.5. Deverão ser consideradas as seguintes métricas para os incidentes:

5.1.5.1. **Nível de severidade**: prioridade a ser atribuído a um chamado realizado pelo CONTRATANTE;

5.1.5.2. **Prazo de atendimento:** Tempo decorrido entre a abertura do chamado automático, por iniciativa da CONTRATADA, ou realizado pelo CONTRATANTE e a disponibilização/envio do número do protocolo de atendimento ao CONTRATANTE

5.1.5.3. **Prazo de solução definitiva:** Tempo decorrido entre a data e hora de registro da OS e o efetivo restabelecimento do serviço ao seu pleno estado de funcionamento ou atendimento integral da demanda, isto é, até o momento da comunicação da solução definitiva do problema pela CONTRATADA e aceite pela equipe técnica do CONTRATANTE;

5.1.6. Para fins de aferição dos níveis mínimos de serviço, ao final, o chamado será considerado completamente atendido ou não atendido, não havendo possibilidade de atendimento parcial;

5.2. DOS PRAZOS E PENALIDADES

5.2.1. O limite temporal para atendimento técnico e operacional deverá obedecer à classificação de severidade, o prazo de atendimento e de solução definitiva, conforme tabela abaixo:

CLASSIFICAÇÃO DOS NÍVEIS DE SEVERIDADE DOS CHAMADOS	
NÍVEIS	**DESCRIÇÃO**
1-CRÍTICO	Este Nível de severidade é aplicado em situações de emergência ou problema crítico, caracterizado pela existência de ambiente paralisado, indisponível. Falha que afete operações críticas da CONTRATANTE.
2-URGENTE	Este nível de severidade é aplicado em situações de alto impacto, incluindo os casos de degradação severa de desempenho da solução. Também se aplica a esta severidade casos onde um appliance para de funcionar, ocasionando a perda da alta disponibilidade da solução. Outros exemplos para esta severidade: Perda de redundância, reinicialização de módulos, slots ou portas com defeitos, perda de funcionalidades.
3-MÉDIA	Este nível de severidade é aplicado em situações de baixo impacto ou de problemas que se apresentam de forma intermitente.
3-BAIXA	Este nível de severidade é aplicado em situações de dúvidas técnicas em relação ao uso ou à implementação da solução.

TABELA DE PRAZOS CONFORME SEVERIDADE DO CHAMADO				
	PRAZOS			
	1-CRÍTICO	**2-URGENTE**	**3-MÉDIA**	**4-BAIXA**
Prazo de atendimento	30 min.	60 min.	4 horas, em 8x5	8 horas, em 8x5
Prazo de solução definitiva ou contorno	6 horas	12 horas	24 horas	A combinar
Tolerância mensal de descumprimentos	0	1	2	N/A

(TMD)				
Penalidade	A empresa estará sujeito à sanção de multa, conforme disposições do item 9.2.2 deste T.R.	**Se NIM[2] ≤ TMD:** Pena de Advertência **Se NIM > TMD:** A empresa estará sujeito à sanção de multa, conforme disposições do item 9.2.2 deste T.R.	**Se NIM ≤ TMD** Pena de Advertência **Se NIM > TMD** A empresa estará sujeito à sanção de multa, conforme disposições do item 9.2.2 deste T.R.	Não há

5.2.2. Os atendimentos às solicitações de severidade crítica ou alta deverão ser realizados nas instalações do Contratante (on-site) e não poderão ser interrompidos até o completo restabelecimento dos serviços, salvo em casos excepcionais, autorizados pelo Contratante, mesmo que se estendam por períodos noturnos, sábados, domingos e feriados. Tal situação não implicará em custos adicionais ao Contratante;

5.2.3. Os atendimentos às solicitações de severidade média poderão ser realizados remotamente ou nas instalações do Contratante (on-site), conforme o caso, e não poderão ser interrompidos até o completo restabelecimento dos serviços, salvo em casos excepcionais, autorizados pelo CONTRATANTE, mesmo que se estendam por períodos noturnos, sábados, domingos e feriados. Tal situação não implicará em custos adicionais ao Contratante;

5.2.4. A interrupção do atendimento de uma solicitação, de quaisquer das severidades, por parte da CONTRATADA sem prévia autorização da equipe técnica do CONTRATANTE será caracterizada como um descumprimento mensal para efeitos de aplicação de sanções;

5.2.5. O tempo de indisponibilidade será calculado pela diferença entre a abertura da solicitação e o aceite da correção do problema;

5.2.6. Não será considerada indisponibilidade de equipamentos quando ocorrer uma ou mais das seguintes condições:

5.2.6.1. Quando for caracterizado o uso indevido e/ou mau uso, comprovado por relatório técnico aceito pela Coordenação de Infraestrutura de Redes (DIATI);

5.2.6.2. Quando ocorrer falta de energia elétrica;

5.2.6.3. Quando o CONTRATANTE não disponibilizar o equipamento para a manutenção on-site, devendo o técnico observar no relatório o tempo de espera;

5.2.6.4. Quando o Tribunal não disponibilizar técnico para acompanhamento da manutenção.

5.2.7. A indisponibilidade cessará quando:

5.2.7.1. O equipamento for colocado em funcionamento pela Contratada, após testes de validação, acompanhamento e assinatura do Relatório de Atendimento Técnico pelo CONTRATANTE;

5.2.7.2. O equipamento for substituído por backup igual ou superior, quando necessária a retirada para conserto em laboratório;

5.2.8. Equipamentos substituídos por backup têm um prazo de 45 (quarenta e cinco) dias corridos para serem devolvidos ao TJAL, devidamente reparados;

5.2.9. Quando não houver a possibilidade de conserto do equipamento, este deverá ser substituído por equipamento novo, de características iguais ou superiores às do equipamento em questão;

5.2.10. Se o backup for um equipamento novo, ele poderá ser aceito na substituição, a critério do TJAL;

5.2.11. A substituição só será aceita com relatório detalhado sobre as causas e motivos do mau funcionamento, assim como a indicação do motivo da impossibilidade de conserto.

6. REQUISITOS DE SEGURANÇA DA INFORMAÇÃO

6.1. A CONTRATADA obrigase a tratar como "segredos comerciais e confidenciais", quaisquer informações, dados, processos, fórmulas, códigos, fluxogramas, diagramas lógicos, dispositivos e modelos relativos aos serviços ora

2 NIM - Número de Infrações no Mês

contratados, utilizandoos apenas para as finalidades previstas neste ajuste, não podendo revelá-los ou facilitar a sua revelação a terceiros;

6.2. A CONTRATADA deverá cumprir e atender aos padrões de segurança e controle para acesso e uso das instalações da CONTRATANTE, zelando por sua integridade, preservando o sigilo e a confidencialidade de todos os dados e informações pertinentes aos serviços prestados, de acordo com a legislação vigente que dispõe sobre a categoria dos documentos públicos sigilosos e o acesso a eles;

6.3. Os profissionais disponibilizados pela Contratada para a prestação dos serviços deverão estar identificados com crachá de identificação da mesma, estando sujeitos às normas internas de segurança do Contratante, inclusive àqueles referentes à identificação, trajes, trânsito e permanência em suas dependências.

6.4. A CONTRATADA não deverá acessar ou manipular qualquer informação confiada sem prévia autorização da CONTRATANTE;

6.5. A CONTRATADA deverá firmar um Termo de Confidencialidade, conforme modelo do ANEXO TR3 – TERMO DE CONFIDENCIALIDADE E SIGILO, por ocasião da assinatura do Contrato.

7. RESPONSABILIDADES

7.1. DEVERES E RESPONSABILIDADES DA CONTRATANTE

7.1.1. Nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contrato para acompanhar e fiscalizar a execução dos contratos;

7.1.2. Encaminhar formalmente a demanda por meio de Ordem de Serviço ou de Fornecimento de Bens, de acordo com os critérios estabelecidos no Termo de Referência ou Projeto Básico;

7.1.3. Receber o objeto fornecido pela CONTRATADA que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;

7.1.4. Aplicar à CONTRATADA as sanções administrativas regulamentares e contratuais cabíveis, comunicando ao órgão gerenciador da Ata de Registro de Preços, quando aplicável;

7.1.5. Liquidar o empenho e efetuar o pagamento à CONTRATADA, dentro dos prazos preestabelecidos em contrato;

7.1.6. Comunicar à CONTRATADA todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC;

7.1.7. Definir produtividade ou capacidade mínima de fornecimento da solução de TIC por parte da CONTRATADA, com base em pesquisas de mercado, quando aplicável;

7.1.8. Proporcionar as facilidades indispensáveis à boa execução das obrigações contratuais;

7.1.9. Receber o objeto no prazo e condições estabelecidas no Edital e seus anexos;

7.1.10. Verificar minuciosamente, no prazo fixado, a conformidade dos serviços realizados provisoriamente com as especificações constantes do Edital e da proposta, para fins de aceitação e recebimentos;

7.1.11. Comunicar à CONTRATADA, por escrito, sobre imperfeições, falhas ou irregularidades verificadas no serviço realizado, fixando prazo para que seja substituído, reparado ou corrigido;

7.1.12. Efetuar o pagamento à CONTRATADA no valor correspondente ao serviço, no prazo e forma estabelecidos neste Termo de Referência;

7.1.13. A Administração não responderá por quaisquer compromissos assumidos pela CONTRATADA com terceiros, ainda que vinculados à execução do presente contrato/objeto, bem como por qualquer dano causado a terceiros em decorrência de ato da CONTRATADA, de seus empregados, prepostos ou subordinados;

7.1.14. Assegurar o livre acesso dos empregados da CONTRATADA, no período de expediente do CONTRATANTE, nos dias úteis, desde que devidamente identificados, aos locais em que devam executar suas tarefas, sendo vedada, salvo se por autorização expressa do CONTRATANTE, o trânsito em áreas estranhas às suas atividades;

7.1.15. Prestar todas as informações e esclarecimentos pertinentes ao serviço à CONTRATADA, que venham a ser solicitadas pelos técnicos da CONTRATADA

7.1.16. Ordenar a imediata retirada do local, bem como a substituição, de empregado da CONTRATADA que estiver sem uniforme ou crachá de identificação, que atrapalhar ou dificultar a fiscalização, ou cuja conduta esteja inadequada, a critério da CONTRATANTE.

7.1.17. Anotar em registro próprio e notificar à CONTRATADA, por escrito, a ocorrência de eventuais imperfeições no curso de execução do serviço, fixando prazo para a sua correção.

7.2. DEVERES E RESPONSABILIDADES DA CONTRATADA

7.2.1. Cumprir todas as obrigações constantes no termo de referência e sua proposta, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto;

7.2.2. Relacionar-se com o CONTRATANTE, exclusivamente, por meio do gestor do contrato, e, em sua ausência, por meio dos fiscais requisitantes e técnicos, preferencialmente, por escrito.

7.2.3. A CONTRATADA deverá prestar esclarecimentos ao CONTRATANTE e sujeitar-se às orientações do fiscal do contrato.

7.2.4. Relatar ao CONTRATANTE, no prazo máximo de 48 (quarenta e oito) horas, irregularidades ocorridas que impeçam, alterem ou retardem a execução do contrato/objeto, efetuando o registro da ocorrência com todos os dados e circunstâncias necessárias a seu esclarecimento, sem prejuízo da análise da administração e das sanções previstas.

7.2.5. Manter, durante toda a execução do contrato, em compatibilidade com as obrigações por ele assumidas, todas as condições de habilitação e qualificação exigidas na licitação (Art. 55, XVIII Lei 8.666/93).

7.2.6. A CONTRATADA é responsável pelos danos causados diretamente à Administração ou a terceiros, decorrentes de sua culpa ou dolo na execução do contrato (Art. 70 Lei 8.666/93).

7.2.7. A CONTRATADA é responsável pelos encargos trabalhista, previdenciário, fiscal e comercial, pelos seguros de acidente e quaisquer outros encargos resultantes da prestação do serviço, sendo que não existirá para a CONTRATANTE qualquer solidariedade quanto ao cumprimento dessas obrigações.

7.2.8. A CONTRATADA deve responsabilizar-se por quaisquer acidentes de trabalho sofridos pelos seus empregados quando em serviço.

7.2.9. A CONTRATADA deve observar rigorosamente as normas regulamentadoras de segurança do trabalho.

7.2.10. A CONTRATADA obriga-se a manter, nas dependências do CONTRATANTE, os funcionários identificados e uniformizados de maneira condizente com o serviço, observando ainda as normas internas e de segurança.

7.2.11. Indicar formalmente preposto apto a representá-lo junto à contratante, que deverá responder pela fiel execução do contrato;

7.2.12. Deve disponibilizar e manter atualizados conta de e-mail, endereço e telefones comerciais e do preposto responsável pelo contrato para fins de comunicação formal entre as partes.

7.2.13. Resguardar que seus funcionários cumpram as normas internas do CONTRATANTE e impedir que os que cometerem faltas a partir da classificação de natureza grave continuem na prestação dos serviços.

7.2.14. Assumir todas as responsabilidades e tomar as medidas necessárias para o atendimento dos prestadores de serviço acidentados ou com mal súbito.

7.2.15. É vedado à CONTRATADA caucionar ou utilizar o contrato para quaisquer operações financeiras.

7.2.16. É vedado à CONTRATADA utilizar o nome do CONTRATANTE, ou sua qualidade de CONTRATADA, em quaisquer atividades de divulgação empresarial, como, por exemplo, em cartões de visita, anúncios e impressos.

7.2.17. É vedado à CONTRATADA reproduzir, divulgar ou utilizar, em benefício próprio ou de terceiros, quaisquer informações de que tenha tomado ciência em razão da execução dos serviços sem o consentimento prévio e por escrito do CONTRATANTE.

7.2.18. Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual;

7.2.19. Reparar quaisquer danos diretamente causados à contratante ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou

reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução dos serviços pela CONTRATANTE;

7.2.20. Propiciar todos os meios necessários à fiscalização do contrato pela contratante, cujo representante terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, sempre que considerar a medida necessária;

7.2.21. Quando especificada, manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da solução de TIC;

7.2.22. Quando especificado, manter a produtividade ou a capacidade mínima de fornecimento da solução de TIC durante a execução do contrato; e

7.2.23. Ceder os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, os modelos de dados e as bases de dados à Administração;

8. MODELO DE EXECUÇÃO DO CONTRATO

8.1. PRINCIPAIS AUTORES ENVOLVIDOS NA CONTRATAÇÃO[3]

8.1.1. **Gestor**: é o servidor responsável pela coordenação das atividades relacionadas à fiscalização técnica, administrativa, setorial e pelo público usuário, bem como pelos atos preparatórios à instrução processual e pelo encaminhamento da documentação pertinente ao setor competente para formalização dos procedimentos relativos a prorrogação, alteração, reequilíbrio, pagamento, eventual aplicação de sanções, extinção dos contratos, dentre outros;

8.1.2. **Fiscal Técnico do Contrato**: Servidor responsável pelo acompanhamento com o objetivo de avaliar a execução do objeto nos moldes contratados e, se for o caso, aferir se a quantidade, qualidade, tempo e modo da prestação dos serviços estão compatíveis com os indicadores de níveis mínimos de desempenho estipulados no ato convocatório, para efeito de pagamento conforme o resultado;

8.1.3. **Preposto/representante**: É o empregado da CONTRATADA incumbido de representá-la junto ao Tribunal de Justiça de Alagoas, onde o contrato é executado. Cabe ao preposto:

8.1.3.1. gerenciar a execução do contrato,

8.1.3.2. receber orientações e documentos pertinentes;

8.1.3.3. prestar as informações que se fizerem necessárias; e

8.1.3.4. providenciar a regularização de pendências.

8.2. REUNIÃO DE ALINHAMENTO DE EXPECTATIVAS

8.2.1. Deverá ser realizada uma reunião presencial de alinhamento com o objetivo de identificar as expectativas, levantar informações, nivelar os entendimentos acerca das condições estabelecidas no Contrato e esclarecer possíveis dúvidas acerca do objeto;

8.2.2. Deverão participar dessa reunião, no mínimo, o Gestor do Contrato do CONTRATANTE e o Interlocutor da CONTRATADA;

8.2.3. A reunião realizar-se-á na DIATI (Diretoria Adjunta de Tecnologia da Informação), ou por videoconferência, em até 10 (dez) dias após a assinatura do Contrato de Prestação de Serviço, conforme agendamento efetuado pelo Gestor do Contrato;

8.2.4. Nessa reunião, a CONTRATADA deverá apresentar oficialmente seu interlocutor (preposto).

8.3. CRONOGRAMA GLOBAL DE EXECUÇÃO

8.3.1. A tabela a seguir contém com os principais marcos e eventos que ocorrerão durante a execução do Contrato:

Etapa	DESCRIÇÃO	RESPONSÁVEL	QUANDO OCORRE

3 Definições dadas pelo Ato Normativo TJAL 48/2019

MARCO: RECEBIMENTO E ACEITE DO OBJETO			
1	Assinatura do Contrato	TJAL e CONTRATADA	Após a homologação do certame
2	Reunião de alinhamento de expectativas	TJAL e CONTRATADA	Em até 10 (dez) dias úteis após a Etapa 1
3	Emissão da ordem de fornecimento dos bens/serviços	TJAL	Em até 10 (dez) dias úteis após a Etapa 2
4	Prazo para entrega total dos equipamentos, licenciamentos e softwares, objeto da ordem de fornecimento de bens	CONTRATADA	Em até 60 (sessenta) dias corridos após a Etapa 3
5	Aceite provisório dos equipamentos e softwares	TJAL	Mediante Termo de Aceite Provisório, após o recebimento do objeto, para posterior verificação de sua conformidade com as especificações do edital e proposta comercial
6	Aceite definitivo dos equipamentos e softwares	TJAL	Em até 10 (dez) dias úteis após a Etapa 5, mediante Termo de Aceite Definitivo.
MARCO: INSTALAÇÃO PROFISSIONAL E CONFIGURAÇÃO			
7	Entrega do Plano de Implantação e Configuração	CONTRATADA	Em até 10 dias úteis após Etapa 3
8	Aprovação do Plano de Implantação e Configuração	TJAL	Em até 5 dias úteis após Etapa 7
9	Finalização da instalação e configuração profissional	CONTRATADA	Em até 10 dias corridos após a Etapa 6
10	Operação assistida	CONTRATADA	Início no 1º dia útil após etapa 9
11	Aceite provisório da instalação e configuração profissional	TJAL	Mediante entrega do documento de AS-Built para posterior verificação de sua conformidade com as obrigações do edital
12	Aceite definitivo da instalação e configuração profissional	TJAL	Em até 10 (dez) dias úteis, após a validação do serviço contratado, realização de testes de conformidade, repasse de conhecimento (hands-on) e aprovação do AS-BUILT fornecido pela CONTRATADA
MARCO: TREINAMENTO DA SOLUÇÃO			
13	Execução do serviço de treinamento oficial da fabricante	TJAL / CONTRATADA	Em até 15 dias corridos após a etapa de instalação profissional e configuração
MARCO: GARANTIA, LICENCIAMENTO E SUPORTE TÉCNICO			
14	Início da vigência da garantia, licenciamento e suporte técnico dos produtos	CONTRATANTE	Após o cumprimento da Etapa 9

8.4. MECANISMOS FORMAIS DE COMUNICAÇÃO

8.4.1. O mecanismo de comunicação terá como ponto focal o Fiscal Administrativo e Técnico por parte do CONTRATANTE e o PREPOSTO indicado pela CONTRATADA, utilizando ferramentas digitais de comunicação (Voz, e-mail ou Instant Messenger), reuniões presenciais realizadas no endereço de prestação de serviço ou através de videoconferência (sempre que solicitado pelo CONTRATANTE) e comunicação escrita formal por carta.

8.4.2. Sempre que exigir-se, a comunicação entre o representante do CONTRATANTE e o preposto da FORNECEDORA deverá ser formal, considerando-se como documentos formais, além de documentos do tipo ofício, as comunicações por correio eletrônico.

8.4.3. O representante da CONTRATANTE e o preposto responderão sobre todas as questões sobre o contrato a ser firmado, procurando solucionar todos os problemas que defrontarem, dentro dos limites legais e dentro da razoabilidade.

8.4.4. O acionamento do Serviço de Garantia e Suporte Técnico será através da abertura de chamados junto a **Central de Atendimento** da CONTRATADA realizada pelos especialistas do CONTRATANTE indicados pela Fiscalização Técnica.

9. MODELO DE GESTÃO DO CONTRATO

9.1. CRITÉRIOS DE ACEITAÇÃO

9.1.1. Em conformidade com os artigos 73 a 76 da Lei n.º 8.666/93, o objeto deste Termo de Referência será aceito:

9.1.1.1. Provisoriamente, mediante recibo, em, no máximo, 5 (cinco) dias depois de efetuada a entrega do objeto, para efeito de posterior verificação de sua conformidade;

9.1.1.2. Definitivamente, mediante Termo de Recebimento Definitivo, em até 10 (quinze) dias úteis.

9.1.2. A Administração emitirá a nota de empenho especificando o produto pretendido e a quantidade, entregando-a ao contratado.

9.1.3. Por ocasião da entrega do objeto, será requerido o fornecimento da documentação de suporte técnico e o certificado de garantia, contendo as informações necessárias para abertura dos chamados por telefone e por correio eletrônico (códigos de acesso, números de telefone, endereços de correio eletrônico, códigos de identificação do cliente, etc.).

9.1.4. Após o recebimento provisório, a fiscalização avaliará as características do objeto, identificando eventuais problemas. Estando em conformidade, será efetuado o recebimento definitivo.

9.1.5. Se, após o aceite provisório, constatar-se que o objeto foi entregue em desacordo com este TR ou com a proposta, com incorreção, ou incompleto, serão interrompidos os prazos de recebimento e suspenso o pagamento, após a notificação por escrito à CONTRATADA e até que seja sanada a situação.

9.1.6. Os objetos entregues em desacordo com o especificado neste termo de referência, no instrumento convocatório, no contrato ou com defeito serão rejeitados parcial ou totalmente, conforme o caso, e a CONTRATADA será obrigada a substituí-los dentro do prazo contratual, sob pena de se considerar atraso na entrega.

9.1.7. A CONTRATADA ficará obrigada a trocar, a suas expensas, o material que vier a ser recusado.

9.1.8. A CONTRATADA deverá retirar o material recusado no momento da entrega do material correto. O CONTRATANTE não se responsabilizará por qualquer dano ou prejuízo que venha a ocorrer após esse prazo.

9.1.9. A Administração poderá dar a destinação que julgar conveniente ao material abandonado em suas dependências.

9.1.10. Independentemente da aceitação, a CONTRATADA garantirá a qualidade de cada unidade do produto fornecido pelo prazo estabelecido nas especificações, obrigando-se a reparar aquela que apresentar defeito no prazo estabelecido pelo CONTRATANTE.

9.1.11. Os produtos deverão ser novos e devidamente acondicionados em suas embalagens originais, de forma a permitir completa segurança dos produtos.

9.1.12. Os produtos serão inteiramente recusados pelo CONTRATANTE nas seguintes condições:

9.1.12.1. caso tenham sido entregues com as especificações diferentes das contidas no edital, seus anexos ou da proposta;

9.1.12.2. caso apresentem problemas de acondicionamento: embalagens violadas, vazamentos, objetos quebrados, etc.

9.1.13. No caso de recusa de algum produto, o licitante vencedor terá prazo de 10 (dez) dias úteis para providenciar a sua substituição, contados da comunicação escrita feita pelo Gestor.

9.1.14. O aceite/aprovação do(s) material(is) pelo órgão licitante não exclui a responsabilidade civil do(s) fornecedor(es) por vícios de quantidade ou qualidade do(s) material(is) ou disparidades com as especificações estabelecidas no Edital, verificadas, posteriormente, garantindo-se ao órgão licitante as faculdades previstas no art. 18 da Lei 8.078/90 (Código de Defesa do Consumidor).

9.2. SANÇÕES ADMINISTRATIVAS E PROCEDIMENTOS PARA RETENÇÃO OU GLOSA NO PAGAMENTO

9.2.1. À contratada e ao licitante, conforme o caso, poderão ser aplicadas as sanções administrativas previstas nos arts. 86 e 87, incisos I a IV, da Lei nº 8.666, de 1993, art. 7º da Lei nº 10.520, de 17 de julho de 2002, nos Decretos Estaduais nº 68.119, de 31 de outubro de 2019, e nº 68.118, de 31 de outubro de 2019 de:

9.2.1.1. advertência;

9.2.1.2. multa;

9.2.1.3. suspensão temporária de participação em licitação e impedimento de contratar com a Administração, por prazo não superior a 2 (dois) anos;

9.2.1.4. declaração de inidoneidade para licitar ou contratar com a Administração Pública enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a contratada ressarcir a Administração pelos prejuízos resultantes e após decorrido o prazo da sanção aplicada com base no inciso anterior; e

9.2.1.5. impedimento de licitar e contratar com a Administração Pública e descredenciamento sistema de cadastramento de fornecedores do Estado de Alagoas, pelo prazo de até 5 (cinco) anos, sem prejuízo das multas previstas em edital e no contrato e das demais cominações legais.

9.2.2. A sanção de multa tem natureza pecuniária, cabível nos seguintes percentuais e hipóteses:

9.2.2.1. 0,20% (zero vírgula vinte por cento) por dia de atraso na celebração do contrato ou da ata de registro de preços, sobre o valor de adjudicação, até o limite de 30 (trinta) dias, após o que configurará não celebração do contrato ou da ata de registro de preços;

9.2.2.2. 6% (seis por cento) pela não celebração do contrato ou da ata de registro de preços, sobre o valor de Adjudicação;

9.2.2.3. 0,50% (zero vírgula cinquenta por cento) por dia de retardamento na execução do fornecimento ou serviço, sobre o valor do contrato ou da parcela inadimplida, até o limite de 30 (trinta) dias, após o que configurará inexecução do fornecimento ou serviço, sem prejuízo da possibilidade de rescisão unilateral da avença;

9.2.2.4. 15% (quinze por cento) pela inexecução total ou parcial do fornecimento ou serviço, sobre o valor total do contrato ou da parcela inadimplida;

9.2.2.5. 10% (dez por cento) pela falha na execução do contrato ou da ata de registro de preços, exceto quanto ao retardamento na execução ou à inexecução total ou parcial do fornecimento ou serviço, sobre o valor total do contrato ou da ata de registro de preços; e

9.2.2.6. 20% (vinte por cento) pela fraude na licitação ou na execução do contrato ou da ata de registro de preços, comportamento inidôneo ou cometimento de fraude fiscal, sobre o valor total do contrato ou da ata de registro de preços.

9.2.3. A multa pode ser aplicada isolada ou cumulativamente com outras sanções, sem prejuízo de perdas e danos cabíveis;

9.2.4. A multa será descontada da garantia prestada pelo imputado;

9.2.4.1. Se não houver garantia prestada ou a multa for de valor superior a essa, responderá o imputado pela diferença, que será descontada dos pagamentos eventualmente devidos pelo Tribunal de Justiça de Alagoas ou ainda, quando for o caso, cobrada judicialmente;

9.2.5. O CONTRATADO sujeitar-se-á ao impedimento de licitar e contratar com o Estado de Alagoas nas seguintes hipóteses e prazos:

9.2.5.1. até 90 (noventa) dias, quando deixar de entregar, no prazo estabelecido no Edital, documentação exigida para o certame, ou não mantiver a proposta;

9.2.5.2. até 12 (doze) meses, quando não celebrar o contrato ou a ata de registro de preços;

9.2.5.3. até 24 (vinte e quatro) meses, quando ensejar o retardamento ou falhar na execução do contrato ou da ata de registro de preços; e

9.2.5.4. de 24 (vinte e quatro) a 60 (sessenta) meses, quando apresentar documentação falsa exigida para o certame, fraudar a licitação ou na execução do contrato, comportar-se de modo inidôneo ou cometer fraude fiscal.

9.2.6. A sanção de descredenciamento nos sistemas cadastrais de fornecedores do Estado de Alagoas é acessória da aplicação da sanção de impedimento de licitar e contratar com o Estado de Alagoas, constituindo restrição que deve ostentar a mesma amplitude e perdurar pelo mesmo prazo desta;

9.2.7. As retenções ou glosas no pagamento se darão na forma e nas condições estipuladas nos Níveis Mínimos de Serviço.

9.3. DO PAGAMENTO

9.3.1. O pagamento dos itens componentes do lote será efetuado uma única vez, exceto aqueles que sejam prestados sob demanda, que serão pagos após a execução dos serviços discriminados na Ordem de Fornecimento;

9.3.2. As notas fiscais deverão consignar, concomitantemente ao período considerado, os descontos proporcionais relativos ao desempenho da CONTRATADA no que diz respeito ao atendimento dos Níveis Mínimos de Serviço estabelecidos no edital e contrato, e serão acompanhadas das respectivas memórias de cálculo dos descontos lançados.

9.3.3. Os pagamentos serão efetuados, em moeda corrente nacional, em até 10 (dez) dias úteis após o recebimento definitivo, mediante apresentação da seguinte documentação:

9.3.3.1. Nota fiscal/fatura discriminativa, em via única, devidamente atestada pelo GESTOR DO CONTRATO;

9.3.3.2. CND – Certidão Negativa de Débitos para com a Previdência Social;

9.3.3.3. CRF – Certificado de Regularidade de FGTS, expedido pela Caixa Econômica Federal;

9.3.3.4. Certidão Conjunta Negativa de Débitos Relativos a Tributos Federais, expedida pela Receita Federal do Brasil;

9.3.3.5. Certidão negativa de débitos trabalhistas, emitido pelo TST – Tribunal Superior do Trabalho;

9.3.3.6. Prova de regularidade para com a Fazenda Estadual ou Municipal do domicílio ou sede da licitante;

9.3.4. Considera-se para efeito de pagamento o dia da entrega da O.B. na unidade bancária;

9.3.5. Não será admitida a emissão de faturas com vencimentos diversos correspondentes ao mesmo mês;

9.3.6. A apresentação de nota fiscal/fatura com incorreções ou desacompanhada da documentação requerida implicará na sua devolução à Empresa Contratada para regularização, devendo o prazo de pagamento ser contado a partir da data de sua reapresentação;

9.3.7. Poderá ser deduzida do valor da Nota Fiscal de Serviços/Fatura, multa imposta pelo Tribunal de Justiça, se for o caso.

9.3.8. Nos casos de eventuais atrasos de pagamento, desde que a Contratada não tenha concorrido de alguma forma para tanto, fica convencionado que a taxa de compensação financeira devida pelo Contratante, entre a data de pagamento prevista para o pagamento e o efetivo adimplemento da parcela, será aquela resultante da aplicação da seguinte fórmula:

$$EM = I * N * VP$$

Onde:

EM = Encargos moratórios;

N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;

VP = Valor da parcela a ser paga;

I = índice de atualização financeira = 0,00016438, assim apurado:

I=TX I = (6/100) /365 I = 0,00016438

TX = Percentual da taxa anual = 6%

10. ADEQUAÇÃO ORÇAMENTÁRIA E CRONOGRAMA FÍSICO-FINANCEIRO

10.1. Os recursos necessários ao atendimento das despesas correrão à conta dos recursos orçamentários e serão designados pelo Fundo Especial de Modernização do Poder Judiciário - FUNJURIS.

11. DA VIGÊNCIA DO CONTRATO

11.1. A vigência do contrato terá a mesma duração da garantia do produto.

12. DA SUBCONTRATAÇÃO

12.1. Não será admitida a subcontratação do objeto licitado;

13. DOS CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

13.1. REGIME, TIPO E MODALIDADE DA LICITAÇÃO

13.1.1. De acordo com o Art. 4º do Decreto nº 5.450/2005, esta licitação deve ser realizada na modalidade de Pregão, preferencialmente na sua forma eletrônica, com julgamento pelo critério de menor preço por valor global.

13.1.2. A fundamentação pauta-se na premissa que a contratação de serviços baseia-se em padrões de desempenho e qualidade claramente definidos no Termo de Referência, havendo diversos fornecedores capazes de prestá-los. Caracterizando-se como “serviço comum” conforme Art. 9º, §2º do Decreto 7.174/2010.

13.2. DA PROPOSTA TÉCNICA

13.2.1. A licitante deverá apresentar proposta técnica, contendo a descrição detalhada do objeto ofertado, devendo estar de acordo com as quantidades, especificações técnicas e condições estabelecidas;

13.2.2. Deverá apresentar na proposta a indicação detalhada do equipamento ofertado, citando a marca, modelo, tipo e fabricante;

13.2.3. Deverá ser fornecida pela licitante uma tabela com o número das páginas de sua proposta na qual contenha a comprovação do atendimento dos requisitos exigidos;

13.2.4. A tabela de comprovação técnica é parte obrigatória da proposta comercial e deve ser apresentada conforme modelo abaixo. É necessária a especificação de TODOS os requisitos contidos no anexo de especificações técnicas (ANEXO TR1 – ESPECIFICAÇÃO TÉCNICA DA SOLUÇÃO) deste Termo de Referência e a apresentação da documentação comprobatória com indicação da página. Salienta-se que todos os itens da tabela devem ser devidamente preenchidos.

Nº Requisito no TR	Descrição da característica ou funcionalidade exigida	Documento do fabricante (nome)	Página(s)	Atende ao Requisito (sim/não)
.....	.....	.....	.....	.....

13.2.5. Além da indicação da página da documentação fornecida na qual se encontra a comprovação de cada funcionalidade ou característica técnica exigida para cada item, a correspondente comprovação deverá ser grifada, destacada com marca texto ou o parágrafo ou expressão que comprova o atendimento do item deverá ser copiado e transferido para a planilha;

13.2.6. Serão considerados documentos oficiais para comprovação técnica: catálogos, folders, prospectos e manuais;

13.2.7. Para os documentos do fabricante, é mandatória a comprovação que se trata de documento oficial fornecido pelo fabricante ao mercado, sendo comprovação suficiente desse requisito o link para o acesso ao documento no site do fabricante;

13.2.8. Havendo divergência entra as características técnicas descritas na proposta da licitante e as disponibilizadas pelo fabricante, prevalecerão os informes do fabricante, salvo os casos específicos em que o licitante esclareça os motivos da divergência e que sejam aceitos pelo CONTRATANTE;

13.2.9. Os documentos técnicos fornecidos que não apresentarem numeração de página deverão ser numerados manualmente de forma visível pela licitante, no canto inferior direito;

13.2.10. A CONTRATADA deverá arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, devendo complementá-los, caso o previsto inicialmente não seja satisfatório para o atendimento do objeto da licitação, exceto quando ocorrer algum dos eventos arrolados nos incisos do §1º do art. 57 da Lei nº 8.666/1993;

13.3. DOS CRITÉRIOS DE QUALIFICAÇÃO TÉCNICA PARA HABILITAÇÃO

13.3.1. A licitante deve comprovar por meio de atestado(s) e/ou declaração(ões) que é revenda autorizada e está apta a comercializar, instalar, configurar e dar suporte aos equipamentos e sistemas objetos desta licitação.

13.3.2. A empresa deverá comprovar aptidão para o desempenho de atividade pertinente e compatível em características, quantidades e prazos com o objeto desta licitação, por meio da apresentação de atestado ou declaração de capacidade técnica, em nome da licitante, em documento timbrado, emitido por entidade da Administração Federal, Estadual ou Municipal, direta ou indireta e/ou empresa privada, que comprove que a empresa licitante tenha executado ou esteja executando serviços de características técnicas semelhantes ao objeto desta aquisição, nos termos da Lei;

13.3.2.1. Os atestados deverão ser acompanhados dos respectivos contratos;

13.3.2.2. No caso de atestados emitidos por empresa da iniciativa privada, não serão considerados aqueles emitidos por empresas pertencentes ao mesmo grupo empresarial da empresa proponente. Serão considerados como pertencentes ao mesmo grupo empresarial da empresa proponente, empresas controladas ou controladoras da empresa proponente, ou que tenha pelo menos uma mesma pessoa física ou jurídica que seja sócio da empresa emitente e da empresa proponente;

13.3.3. A comprovação deverá englobar, pelo menos, os seguintes serviços:

13.3.3.1. Fornecimento de solução de segurança da informação, composta de pelo menos um *cluster* de equipamento do tipo *NGFW*;

13.3.3.2. prestação de serviço de suporte técnico para a solução de segurança;

13.3.3.3. Disponibilização de licenças e de atualização de assinatura;

13.3.3.4. Garantia.

13.3.4. Os atestados e/ou declarações poderão ser objetos de diligência por parte do pregoeiro ou da equipe técnica, com vistas a dirimir as dúvidas em relação ao tipo de serviço prestado, podendo a CONTRATANTE requerer cópia de outros documentos que possam comprovar, inequivocamente, que os equipamentos e serviços apresentados nos atestados e/ou declarações foram fornecidos e prestados.

13.3.5. Declaração direcionada ao certame, expedida pelo PROPONENTE, de que disponibilizará, para controle da execução dos serviços de suporte técnico e consultoria especializada, profissional(is) com formação específica e oficial do fabricante para os equipamentos objetos desta licitação, comprovado por certificado válido, emitido pelo fabricante.

13.3.6. A comprovação da disponibilidade do(s) profissional(is) para controle e execução dos serviços em discussão será feita com a apresentação de cópia da carteira de trabalho (CTPS) em que conste o licitante como contratante, do contrato social do licitante em que conste o profissional como sócio, do contrato de trabalho ou, ainda, de declaração de contratação futura do profissional detentor do certificado de qualificação apresentado, desde que acompanhada de declaração de anuência do profissional;

13.3.7. Declaração exigida neste item deverá conter o nome e CPF do(s) profissional(is) que acompanhará(ão) a execução dos serviços que trata o objeto desta licitação;

13.3.8. O(s) profissional(is) indicado(s) pelo licitante para fins de comprovação da capacitação técnico-profissional deverão participar da execução dos serviços de suporte técnico objeto da licitação, admitindo-se a substituição por profissional(is) de experiência equivalente ou superior, desde que previamente comunicado à CONTRATANTE, que poderá solicitar a comprovação dos requisitos de qualificação técnica.

14. DA VISTORIA FACULTATIVA

14.1. A licitante poderá vistoriar o local onde serão executados os serviços on-site, incluídos no objeto deste termo de referência, em companhia de um servidor do TJAL, para inteirar-se das condições das instalações e do grau de dificuldade existentes;

14.2. O horário para visita será realizado das 08 às 14 horas, o qual deverá ser agendado, com antecedência mínima de 24 (vinte quatro) horas;

14.3. A vistoria técnica ocorrerá até a data final para o recebimento das propostas;

14.4. Um Termo de Vistoria Facultativa será emitido após a conclusão da visita;

14.5. A licitante que optar por não realizar vistoria não poderá alegar desconhecimento das condições de execução dos serviços para desobrigar-se do contrato.

15. DA GARANTIA CONTRATUAL

15.1. Para assegurar o integral cumprimento de todas as obrigações contratuais assumidas, inclusive indenização a terceiros e multas eventualmente aplicadas, a CONTRATADA apresentará garantia de 5% (cinco) por cento do valor total do contrato em uma das modalidades estabelecidas no art. 56 da Lei n° 8.666/1993, no prazo de até 10 (dez) dias úteis após a data da sua assinatura, prorrogáveis por igual período, a critério do CONTRATANTE;

15.2. A inobservância do prazo fixado para apresentação da garantia acarretará a aplicação de multa de 0,07% (sete centésimos por cento) do valor do Contrato por dia de atraso, até o limite de 2% (dois por cento);

15.3. O atraso superior a 25 (vinte e cinco) dias autoriza a Administração a promover a rescisão do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõem os incisos I e II do art. 78 da Lei nº 8.666, de 1993;

15.4. A garantia, qualquer que seja a modalidade escolhida, assegurará o pagamento de:

15.4.1. Prejuízos advindos do não cumprimento do objeto do contrato;

15.4.2. Prejuízos diretos causados à Administração decorrentes de culpa ou dolo durante a execução do contrato;

15.4.3. Multas moratórias e punitivas aplicadas pela Administração à contratada; e

15.4.4. Obrigações trabalhistas e previdenciárias de qualquer natureza, não adimplidas pela contratada, quando couber.

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

15.6. A garantia deverá vigorar durante todo o período de vigência contratual, mantendo-se válida até 03 (três) meses após o término deste Contrato, devendo ser renovada a cada prorrogação;

15.7. Havendo opção pela modalidade caução em dinheiro, o valor deverá ser depositado em conta-caução em uma conta a ser designada pelo CONTRATANTE;

15.8. A garantia ficará sob a responsabilidade e à ordem do CONTRATANTE;

15.9. A garantia será considerada extinta:

15.9.1. Com a devolução da apólice, carta fiança ou autorização para o levantamento de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração da Administração, mediante termo circunstanciado, de que a contratada cumpriu todas as cláusulas do contrato; e

15.9.2. Após o prazo estabelecido no subitem 15.6, que poderá ser estendido em caso de ocorrência de sinistro.

15.10. O CONTRATANTE executará a garantia na forma prevista na legislação que rege a matéria;

15.11. Havendo repactuação de preços, acréscimo ou supressão de serviços, a garantia será acrescida ou devolvida, guardada a proporção de 5% (cinco por cento) sobre o valor resultante da alteração, conforme o art. 56 §4º, da Lei 8.666/1993;

15.12. Se o valor da garantia for utilizado em pagamento de qualquer obrigação, inclusive indenização a terceiros, a CONTRATADA obriga-se a fazer a respectiva reposição no prazo de 05 (cinco) dias, contados da data em que for notificada, pelo CONTRATANTE.

Integrante Demandante	Integrante Técnico	Integrante Administrativo
JOSE BAPTISTA DOS SANTOS NETO:91232 Assinado de forma digital por JOSE BAPTISTA DOS SANTOS NETO:91232 Dados: 2023.05.11 14:30:42 -03'00'	Assinado digitalmente por Christiano Rossini Martins Costa:93077 ND: C=BR, O=ICP-Brasil, OU=Autoridade Certificadora da Justica - AC-JUS, OU=Cert-JUS Institucional - A3, OU=08447641000109, OU=Presencial, OU=Tribunal de Justica de Alagoas-TJAL, OU=Servidor, CN=Christiano Rossini Martins Costa:93077 Razão: Eu revisei este documento Localização: Data: 2023.05.11 14:24:27-03'00'	ALINE GAMA PINHEIRO DE MELO:926027 Assinado de forma digital por ALINE GAMA PINHEIRO DE MELO:926027 Dados: 2023.05.11 15:37:42 -03'00'
Jose Baptista dos Santos Neto Diretor da DIATI	Christiano Rossini Martins Costa DIATI	Aline Gama Pinheiro de Melo DGC

PODER JUDICIÁRIO DE ALAGOAS

ANEXO TR1 – ESPECIFICAÇÃO TÉCNICA DA SOLUÇÃO

REQUISITOS ESPECÍFICOS	
ID	Descrição
RE002	Suportar no mínimo 2 milhões de conexões simultâneas;
RE003	Suportar no mínimo 200 mil novas conexões por segundo;
RE004	Throughput de no mínimo 12 Gbps de VPN IPSec;
RE006	Throughput de, no mínimo, 7 Gbps com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação, IPS, Antivírus e Antispyware. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito;
RE007	Deve possuir, pelo menos, 12 interfaces 1GE com conectores RJ-45;
RE008	Deve possuir, pelo menos, 4 interfaces 10GE SFP+;
RE009	Deve possuir, pelo menos, 4 interfaces 25GE SFP28;
RE010	Deve possuir, pelo menos, 2 interfaces 40GE QSFP+;
RE011	Deve possui armazenamento interno, no minimo, de 240GB em SSD;
RE012	Deve possuir fonte redundate “Hot Swappable”;
RE013	Estar licenciado, sem custo adicional, 10 sistemas virtuais lógicos (Contextos) por appliance;

REQUISITOS LEGAIS	
ID	Descrição
RE014	Os equipamentos devem obrigatoriamente estar em conformidade com o artigo 55 da Resolução 715 de 23 de outubro de 2019, emitida pela ANATEL;
RE015	Deve possuir certificação de conformidade sustentável de acordo com os padrões EPA (Enviromental Protection Agency) ou similar, tais como, EnergyStar, RoHS (Restriction on Harzadous Substances), WEEE (Waste Electrical and Eletronic Equipament) ou EMI Certifications FCC part 15, CE, EN55022, EN55024.

REQUISITOS GERAIS	
ID	Descrição
RE016	A solução deve consistir em plataforma de proteção de rede baseada em appliance com funcionalidades de Next Generation Firewall (NGFW), não se admitindo equipamentos servidores e sistema operacional de uso genérico;
RE018	Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;
RE019	As funcionalidades de proteção de rede que compõe a plataforma de segurança podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação;
RE020	A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;
RE021	O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;
RE022	O gerenciamento da solução deve suportar a interface de administração via web no próprio dispositivo de proteção de rede;
RE023	Os dispositivos de proteção de rede devem possuir suporte a 4094 VLAN Tags 802.1q;
RE024	Os dispositivos de proteção de rede devem possuir suporte a agregação de links 802.3ad e LACP;
RE025	Os dispositivos de proteção de rede devem possuir suporte a policy-based routing ou policy-based forwarding;
RE026	Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM);
RE027	Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay;
RE028	Os dispositivos de proteção de rede devem possuir suporte a DHCP Server;
RE029	Os dispositivos de proteção de rede devem suportar sFlow ou similar;
RE030	Os dispositivos de proteção de rede devem possuir suporte a Jumbo Frames;
RE031	Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;
RE032	Deve suportar NAT dinâmico (Many-to-1);

RE033	Deve suportar NAT dinâmico (Many-to-Many);
RE034	Deve suportar NAT estático (1-to-1);
RE035	Deve suportar NAT estático (Many-to-Many);
RE036	Deve suportar NAT estático bidirecional 1-to-1;
RE037	Deve suportar Tradução de porta (PAT);
RE038	Deve suportar NAT de Origem, NAT de Destino e os dois simultaneamente;
RE039	Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;
RE040	Deve suportar NAT64;
RE041	Deve implementar o protocolo ECMP;
RE042	Deve implementar balanceamento de link por hash do IP de origem;
RE043	Deve implementar balanceamento de link por hash do IP de origem e destino;
RE044	Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links ou definir o tamanho real do link de download/upload. Deve suportar o balanceamento de, no mínimo, três links;
RE046	Deve permitir monitorar via SNMP falhas de hardware, uso de recursos por número elevado de sessões, conexões por segundo, número de túneis estabelecidos na VPN, CPU, memória, status do cluster, ataques e estatísticas de uso das interfaces de rede;
RE047	Deverá suportar o envio de logs para sistemas de monitoração externos, simultaneamente;
RE048	Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;
RE049	O Firewall em questão deverá possuir proteção anti-spoofing, evitando assim o redirecionamento de tráfego de dados ou utilização de um falso endereço IP
RE051	Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
RE052	Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);
RE053	Suportar OSPF graceful restart;
RE054	Os dispositivos de proteção devem ter a capacidade de operar de forma simultânea em uma única instância de firewall, mediante o uso de suas interfaces físicas nos seguintes modos: Modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3);
RE055	Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
RE056	Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade do tráfego;
RE057	Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;
RE058	Deve suportar Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;
RE059	Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo em modo transparente.
RE060	A configuração em alta disponibilidade deve sincronizar a. sessões; b. configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede; c. Associações de Segurança das VPNs; d. tabelas FIB
RE061	O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link;
RE062	Deve possuir suporte a criação de sistemas virtuais no mesmo appliance;
RE064	Deve permitir a criação de administradores independentes, para cada um dos sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados por equipes distintas;
RE065	O gerenciamento da solução deve suportar acesso via SSH e interface WEB (HTTPS), incluindo, mas não limitado, a exportação da configuração dos sistemas virtuais (contextos) por ambas interfaces;
RE066	Deverá suportar controle, inspeção e descriptografia de SSL para tráfego de entrada (Inbound) e Saída (Outbound), sendo que deve suportar o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolamento das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos).

CONTROLE POR POLÍTICA DE FIREWALL	
ID	Descrição
RE067	Deverá suportar controles por zona de segurança

RE068	Deverá suportar controles de políticas: a. por porta e protocolo; b. por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações; c. por usuários, grupos de usuários, IPs, redes e zonas de segurança d. por código de País (Por exemplo: BR, USA, UK, RUS);
RE069	Deverá suportar controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e Saída (Outbound);
RE070	Deverá suportar offload de certificado em inspeção de conexões SSL de entrada (Inbound);
RE071	Deve descriptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.2 e superior;
RE072	Deverá suportar controle de inspeção e descriptografia de SSH por política;
RE073	Deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada;
RE074	Deve suportar configurações de Traffic shaping QoS baseado em Políticas (Prioridade, Garantia e Máximo);
RE075	Deve suportar QoS baseado em políticas para marcação de pacotes (diffserv marking), inclusive por aplicações;
RE076	Suporte a objetos e regras IPV6;
RE077	Suporte a objetos e regras multicast;
RE078	Deve suportar no mínimo três tipos de resposta nas políticas de firewall: Drop sem notificação do bloqueio ao usuário, drop com notificação do bloqueio ao usuário, Drop com opção de envio de ICMP Unreachable para máquina de origem do tráfego, TCP- Reset para o client, TCP-Reset para o server ou para os dois lados da conexão;
RE079	Deve suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;

CONTROLE DE APLICAÇÕES	
ID	Descrição
RE080	Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocol;
RE081	Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;
RE082	Reconhecer pelo menos 1800 aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;
RE083	Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;
RE084	Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;
RE085	Deve detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a Bittorrent e aplicações VOIP que utilizam criptografia proprietária;
RE086	Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor;
RE087	Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
RE088	Identificar o uso de táticas evasivas via comunicações criptografadas;
RE089	Atualizar a base de assinaturas de aplicações automaticamente;
RE090	Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos;

RE091	Deve ser possível adicionar controle de aplicações em múltiplas regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;
RE092	Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;
RE093	Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;
RE094	Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante;
RE095	A criação de assinaturas personalizadas deve permitir o uso de expressões regulares, contexto (sessões ou transações), usando posição no payload dos pacotes TCP e UDP e usando decoders de pelo menos os seguintes protocolos: HTTP, FTP, NBSS, DCE RPC, SMTP, Telnet, SSH, MS-SQL, IMAP, DNS, LDAP, RTSP e SSL;
RE096	O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
RE097	Deve alertar o usuário quando uma aplicação for bloqueada;
RE098	Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos;
RE099	Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;
RE100	Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Hangouts chat e bloquear a chamada de vídeo;
RE101	Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos;
RE102	Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: a. Tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc); b. Nível de risco da aplicação; c. Categoria da aplicação;

PREVENÇÃO DE AMEAÇAS	
ID	Descrição
RE103	Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;
RE104	Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);
RE105	As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante;
RE106	Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;
RE107	Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear, bloquear IP do atacante por um intervalo de tempo e enviar tcp-reset;
RE108	As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;
RE109	Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;
RE110	Deve permitir o uso de exceções por IP de origem ou de destino nas regras e assinatura ;
RE111	Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes politicas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;
RE112	Deve permitir o bloqueio de vulnerabilidades;
RE113	Deve permitir o bloqueio de exploits conhecidos;
RE114	Deve incluir proteção contra ataques de negação de serviços;
RE115	Deverá possuir os seguintes mecanismos de inspeção de IPS:

	a. Análise de padrões de estado de conexões; b. Análise de decodificação de protocolo; c. Análise para detecção de anomalias de protocolo; d. IP Defragmentation; e. Remontagem de pacotes de TCP; f. Bloqueio de pacotes mal formados;
RE116	Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;
RE117	Detectar e bloquear a origem de portscans;
RE118	Bloquear ataques efetuados por worms conhecidos;
RE119	Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;
RE120	Possuir assinaturas para bloqueio de ataques de buffer overflow;
RE121	Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;
RE122	Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS ou anti-spyware, permitindo a criação de exceções com granularidade nas configurações;
RE123	Deverá permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
RE124	Suportar bloqueio de arquivos por tipo;
RE125	Identificar e bloquear comunicação com botnets;
RE126	Registrar no console de monitoração as seguintes informações sobre ameaças identificadas: O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
RE127	Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação;
RE128	Deve permitir que na captura de pacotes por assinaturas de IPS seja definido o número de pacotes a serem capturados ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos;
RE129	Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;
RE130	Os eventos devem identificar o país de onde partiu a ameaça;
RE131	Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;
RE132	Deve possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;
RE133	Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança;
RE134	Deve possuir a capacidade de identificar ataques de ransomwares e Advanced Persistent Threat (APT) ou Zero-Day
RE135	Deve possuir a capacidade de emular um ambiente operacional isolado e seguro (Sandbox), na nuvem do fabricante, independente do volume mensal, para execução e observação de código malicioso, sem a utilização de assinaturas, com base na atividade, como, por exemplo, operações de arquivo, alterações de registro e sistema etc.
RE136	A solução deve fornecer a capacidade de emular ataques em diferentes sistemas operacionais e aplicativos;
RE137	Toda a análise e bloqueio de malwares e/ou códigos maliciosos deve ocorrer em tempo real e o bloqueio deve ser imediato. Não serão aceitas soluções que apenas detectam o malware e/ou códigos maliciosos;
RE138	A solução deve emular e eliminar malwares conhecidos em anexos de e-mail e documentos baixados na web;
RE139	Deve permitir exportar o resultado das análises de malwares de zero-day em PDF ou CSV, a partir da própria interface de gerência;

FILTRO DE URL	
ID	Descrição
RE140	Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou

	período (dia, mês, ano, dia da semana e hora);
RE141	Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;
RE142	Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local, em modo de proxy transparente e explícito;
RE143	Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
RE144	Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs;
RE145	Possuir pelo menos 60 categorias de URLs;
RE146	Deve possuir a função de exclusão de URLs do bloqueio, por categoria;
RE147	Permitir a customização de página de bloqueio;
RE148	Permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão Continuar para permitir o usuário continuar acessando o site);

IDENTIFICAÇÃO DE USUÁRIOS	
ID	Descrição
RE149	Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, E-directory e base de dados local;
RE150	Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários;
RE152	Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários ou qualquer tipo de restrição de uso como, mas não limitado à utilização de sistemas virtuais, segmentos de rede, etc;
RE153	Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários;
RE154	Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em Usuários e Grupos de usuários;
RE155	Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);
RE156	Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;
RE157	Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;
RE158	Permitir integração com tokens para autenticação dos usuários, incluindo, mas não limitado a acesso à internet e gerenciamento da solução;
RE160	Deve possuir capacidade de autenticar usuários para administração do Equipamento, através de base de dados: a. Local; b. Integrada a servidor TACACS+ ou RADIUS; c. Integrada a servidor Ldap ou RADIUS;

QoS e Traffic Shaping	
ID	Descrição
RE161	Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como youtube, ustream, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio

	como de vídeo streaming;
RE162	Suportar a criação de políticas de QoS e Traffic Shaping por: a. endereço de origem b. endereço de destino c. usuário e grupo d. aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus; e. porta
RE163	O QoS deve possibilitar a definição de tráfego com banda garantida;
RE164	O QoS deve possibilitar a definição de tráfego com banda máxima;
RE165	O QoS deve possibilitar a definição de fila de prioridade;
RE166	Suportar priorização em tempo real de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype;
RE167	Suportar marcação de pacotes Diffserv, inclusive por aplicação;
RE169	Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping;
RE170	Deve suportar QOS (traffic-shapping), em interfaces agregadas ou redundantes.

FILTRO DE DADOS	
ID	Descrição
RE171	Permitir a criação de filtros para arquivos e dados pré-definidos;
RE172	Os arquivos devem ser identificados por extensão e tipo;
RE173	Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP, etc);
RE174	Suportar a identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
RE176	Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular;

GEOLOCALIZAÇÃO	
ID	Descrição
RE177	Deve suportar a criação de políticas por geolocalização, permitindo o trafego de determinado País/Países sejam bloqueados;
RE178	Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;
RE179	Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas;

VPN	
ID	Descrição
RE180	Suportar VPN Site-to-Site e Cliente-To-Site;
RE181	Suportar IPSec VPN;
RE182	Suportar SSL VPN;
RE183	A VPN IPSEc deve suportar: a. 3DES; b. Autenticação MD5 e SHA-1; c. Diffie-Hellman Group 1, Group 2, Group 5, Group 14 e Group 15-21; d. Algoritmo Internet Key Exchange (IKEv1 e v2); e. AES 128, 192 e 256 (Advanced Encryption Standard); f. Autenticação via certificado IKE PKI
RE184	Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;
RE186	Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de troubleshooting;
RE187	A VPN SSL deve suportar o usuário realizar a conexão por meio de cliente instalado no sistema

	operacional do equipamento ou por meio de interface WEB;
RE188	A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;
RE189	Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;
RE190	Atribuição de DNS nos clientes remotos de VPN;
RE191	Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;
RE192	Deve suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local;
RE193	Deve suportar leitura e verificação de CRL (certificate revocation list);
RE194	Deve permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;
RE195	Deve permitir que a conexão com a VPN seja estabelecida das seguintes formas: Antes do usuário autenticar na estação; Após autenticação do usuário na estação; Sob demanda do usuário;
RE196	Deverá manter uma conexão segura com o portal durante a sessão;
RE197	O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 7 (32 e 64 bits), Windows 8 (32 e 64 bits), Windows 10 (32 e 64 bits) e Mac OS X (v10.14 ou superior).

CARACTERÍSTICAS DE SD-WAN	
ID	Descrição
RE198	Deve possuir capacidade de agregar e balancear, no mínimo, 4 circuitos de dados utilizando uma interface dedicada para cada circuito;
RE199	A solução SD-WAN deve ser viabilizada com recursos de segurança integrados de: Firewall, VPN, Antivírus, IPS e Filtro de Segurança Web;
RE200	A solução SD-WAN deve suportar micro-segmentação de tráfego onde seja possível aplicar políticas de IPS e Antivírus entre segmentos de LAN;
RE201	A solução SD-WAN deve suportar NAT em contexto de saída (Nat Outbound) para um pool de IPs públicos;
RE203	Solução deve ser capaz de prover Zero Touch provisioning;
RE204	A solução de Zero Touch provisioning deve ser capaz de suportar endereçamentos estáticos e dinâmicos, e que seja suportado múltiplos links WAN
RE205	A solução de Zero Touch deve ser escalável, suportando, no mínimo, todos os dispositivos da solução em uma mesma comunidade VPN neste context;
RE207	Reconhecimento em camada 7 totalmente segregado da camada 4;
RE208	Deve, de forma alternativa, contar com um banco de Dados interno, onde seja possível atrelar uma aplicação à um determinado IP/ range de IPs de destino;
RE209	O reconhecimento de aplicações deve ser atualizado de forma dinâmica e totalmente transparente para o dispositivo
RE210	O reconhecimento de aplicações deve ser realizado independentemente de porta e protocolo, inspecionando o payload de pacote de dados;
RE211	Ainda sobre o reconhecimento de Aplicações, a solução deve fornecer o reconhecimento default em camada 7, de pelo menos 2000 aplicações largamente utilizadas em contextos de SaaS, Aplicações na Nuvem, Aplicações Multimídia (Vimeo, YouTube, Facebook, etc);
RE212	A solução deve considerar os seguintes itens: a. 802.1Q; b. BFD ou BGP;
RE213	A solução de SD-WAN deve suportar Roteamento dinâmico BGP;
RE214	A solução de SD-WAN deve suportar Roteamento dinâmico BGP com suporte a IPv4 e, quando requisitado, possuir suporte a IPv6 mesmo que seja necessário substituição do equipamento, com o ônus da CONTRATADA;
RE215	A solução deve ser capaz de refletir, de forma manual ou automatizada, suas políticas de SD-WAN em condições onde a largura de banda é modificada;

RE216	A solução deve ser capaz de medir o Status de Saúde do Link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss, onde seja possível configurar um valor de threshold para cada um deles ou um limite de kbyte como fator de decisão nas regras de SD-WAN;
RE217	A solução deve ser capaz de medir o Status de Saúde com Suporte a múltiplos servidores;
RE218	A solução deve permitir modificar configuração de tempo de checagem em segundos para cada um dos links;
RE220	A solução deve permitir a configuração de regras onde o Failback (retorno à condição inicial) apenas ocorra dentro de um espaço de tempo de X segundos, configurável pelo administrador do sistema, ou que o sistema possua snapshot de regras para retorno rápido das configurações;
RE221	A solução deve permitir a configuração de políticas de QoS em camada 7, associadas percentualmente à largura de banda da Interface SD-WAN;
RE222	A solução deve permitir a configuração de políticas de QoS em valores onde o máximo corresponda à totalidade de largura de banda disponível no equipamento
RE223	A solução deve permitir a consulta via SNMPv2/v3 referente aos seguintes dados: a. Estado atual dos links SD-WAN; b. Latência; c. Jitter; d. Packet Loss; e. Pacotes enviados / Pacotes Recebidos; f. Link Bandwitdh;
RE224	A solução deve possibilitar a distribuição de Peso em cada um dos links que compõe o SD-WAN, a critério do administrador, de forma em que o algoritmo de balanceamento utilizado possa ser baseado em: a. Número de Sessões; b. Volume de Tráfego; c. IP de Origem e Destino; d. Transbordo de Link (Spillover).
RE226	Solução deve ser capaz de suportar uma arquitetura de transporte Multicast IPv4 e IPv6 através de tuneis VPN IPSEC construídos em ADVPN ou possuir suporte a orquestrador de VPN para esta função;
RE228	Disparar ações automáticas de: Envio de traps SNMPv2/v3, Alertas por Email e Envio de Log ao Servidor Syslog quando em situações de: a. HA Failover; b. Túnel IPSec Up/Down; c. Interface UP/Down; d. Appliance em estado inoperante;
RE230	A Alta Disponibilidade provida pela solução de SD-WAN deverá suportar Balanceamento Ativo – Ativo, Ativo – Passivo, Distribuído Geograficamente;
RE231	A solução SD-Wan deve oferecer Troubleshooting em console de linha de comando ou gráfica, onde seja possível: a. Executar Packet sniffer do tráfego interessante, filtrando por: IP e Porta; b. Realizar debug detalhado das fases de negociação VPN;
RE233	A solução SDWAN deve suportar marcação de pacotes DSCP nas definições e regras para tráfego SDWAN;
RE234	Os appliances devem ser capazes de inspecionar (Descriptografar) tráfego SSL e permitir aplicar regras dentro dos túneis das aplicações.

ANEXO TR2 – MODELO DE TERMO DE VISTORIA

TERMO DE VISTORIA

Declaro, para fins de participação na licitação em epígrafe, que vistoriei minuciosamente o ambiente técnico do CONTRATANTE e que tomei conhecimento de todas as informações necessárias à execução do contrato e proclamo estar ciente da complexidade dos serviços, bem como dos termos e condições descritos no respectivo edital e seus anexos.

Maceió-AL,____/____/_____.

_____

CARIMBO E ASSINATURA OU ASSINATURA DIGITAL DO RESPONSÁVEL/REPRESENTANTE DA EMPRESA

Nome legível: _____

CPF: _____

_____

CARIMBO E ASSINATURA OU ASSINATURA DIGITAL DO REPRESENTANTE DO CONTRATANTE

TERMO DE CONFIDENCIALIDADE E SIGILO

A empresa **[RAZÃO/DENOMINAÇÃO SOCIAL]**, pessoa jurídica com sede em **[ENDEREÇO]**, inscrita no CNPJ/MF com o n.º **[N.º DE INSCRIÇÃO NO CNPJ/MF]**, neste ato representada na forma de seus atos constitutivos, doravante denominada simplesmente EMPRESA RECEPTORA, por tomar conhecimento de informações sobre o ambiente computacional do Tribunal de Justiça do Estado de Alagoas – TJAL, aceita as regras, condições e obrigações constantes do presente Termo.

1. O objetivo deste Termo de Confidencialidade e Sigilo é prover a necessária e adequada proteção às informações restritas de propriedade exclusiva do TJAL reveladas à EMPRESA RECEPTORA em função da prestação dos serviços objeto do contrato **[Nº DO CONTRATO]**.

2. A expressão "informação restrita" abrangerá toda informação escrita, oral ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: técnicas, projetos, especificações, desenhos, cópias, diagramas, fórmulas, modelos, amostras, fluxogramas, croquis, fotografias, plantas, programas de computador, discos, disquetes, pen drives, fitas, contratos, planos de negócios, processos, projetos, conceitos de produto, especificações, amostras de ideia, clientes, nomes de revendedores e/ou distribuidores, preços e custos, definições e informações mercadológicas, invenções e ideias, outras informações técnicas, financeiras ou comerciais, entre outros.

3. A EMPRESA RECEPTORA compromete-se a não reproduzir nem dar conhecimento a terceiros, sem a anuência formal e expressa do TJAL, das informações restritas reveladas.

4. A EMPRESA RECEPTORA compromete-se a não utilizar, bem como a não permitir que seus diretores, consultores, prestadores de serviços, empregados e/ou prepostos utilizem, de forma diversa da prevista no contrato de prestação de serviços ao TJAL, as informações restritas reveladas.

5. A EMPRESA RECEPTORA deverá cuidar para que as informações reveladas fiquem limitadas ao conhecimento dos diretores, consultores, prestadores de serviços, empregados e/ou prepostos que estejam diretamente envolvidos nas discussões, análises, reuniões e demais atividades relativas à prestação de serviços ao TJAL, devendo cientificá-los da existência deste Termo e da natureza confidencial das informações restritas reveladas.

6. A EMPRESA RECEPTORA possuirá ou firmará acordos por escrito com seus diretores, consultores, prestadores de serviços, empregados e/ou prepostos cujos termos sejam suficientes a garantir o cumprimento de todas as disposições do presente Termo.

7. A EMPRESA RECEPTORA obriga-se a informar imediatamente ao TJAL qualquer violação das regras de sigilo estabelecidas neste Termo que tenha tomado conhecimento ou ocorrido por sua ação ou omissão, independentemente da existência de dolo.

8. A quebra do sigilo das informações restritas reveladas, devidamente comprovada, sem autorização expressa do TJAL, possibilitará a imediata rescisão de qualquer contrato firmado entre o TJAL e a EMPRESA

RECEPTORA sem qualquer ônus para o TJAL. Nesse caso, a EMPRESA RECEPTORA, estará sujeita, por ação ou omissão, além das multas definidas no Termo de Referência, ao pagamento ou recomposição de todas as perdas e danos sofridos pelo TJAL, inclusive os de ordem moral, bem como as de responsabilidades civil e criminal respectivas, as quais serão apuradas em regular processo judicial ou administrativo.

9. O presente Termo tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de acesso às informações restritas do TJAL. E, por aceitar todas as condições e as obrigações constantes do presente Termo, a EMPRESA RECEPTORA assina o presente termo através de seus representantes legais.

Maceió, _____ de _____ de 20___ .

[NOME DA EMPRESA RECEPTORA]

_____ _____

Nome:

Nome:

ANEXO TR4 – PLANILHA DE COMPOSIÇÃO DE PREÇOS

LOTE ÚNICO **Firewall de Próxima Geração (*Next Generation Firewall – NGFW)***					
Id.	**Descrição do Bem ou Serviço**	**Unidade**	**Qtde/Duração**	**Preço unitário**	**Preço global**
1	Solução de segurança da informação do tipo Next Generation Firewall (NGFW), com garantia, suporte técnico e licença de uso por 60 meses	equipamento	2	R$ _____,__	R$ _____,__
2	Serviço de instalação e configuração profissional dos equipamentos	serviço	2	R$ _____,__	R$ _____,__
3	Treinamento oficial do fabricante	curso	1	R$ _____,__	R$ _____,__
4	Consultoria técnica especializada da solução	UST	200	R$ _____,__	R$ _____,__
VALOR TOTAL DA PROPOSTA					**R$ _____,__**