Termo de Referência Nº 8/2020 - PJPI/TJPI/PRESIDENCIA/STIC/GOVTIC/ACSTIC

TERMO DE REFERÊNCIA

REGISTRO DE PREÇOS PARA AQUISIÇÃO DE SOLUÇÃO DE SEGURANÇA DA INFORMAÇÃO

1. FUNDAMENTO LEGAL

1.1. Legislação Federal/Nacional: Lei nº 10.520/2002, Decretos nº 3.555/2000, nº 5.450/2005, nº 7.892/2013 e suas alterações; Lei Complementar nº 123/2006 e subsidiariamente, Lei nº 8.666/93 e Lei nº 8.078/1990 e outras normas aplicáveis ao objeto deste certame.

1.2. Legislação do Estado do Piauí: Decreto nº 11.319/04 (Regulamento do SRP do Governo do Estado do Piauí), Resolução TJ/PI nº 19/2007, Portaria nº 168/2011/TJPI e outras normas aplicáveis ao objeto deste certame e, ainda, pelo estabelecido no instrumento convocatório que permear o referido certame.

1.3. A licitante deverá se credenciar no sítio www.comprasgovernamentais.gov.br, sistema “Pregão Eletrônico”, para participar da Licitação.

1.4. Objetivou-se atender também a resolução 182 do CNJ para efeito de auditoria futura pelo Conselho Nacional de Justiça - CNJ.

2. OBJETO (art. 18, §3, I)

2.1. O objeto deste Termo de Referência é a aquisição, através do Sistema de Registro de Preços, de **Solução de firewall de próxima geração** (NGFW), para ser fornecido de forma única ou parcelado, conforme solicitações, durante a validade da Ata de Registro de Preços, para atender todas as unidades integrantes do Tribunal de Justiça do Estado do Piauí, incluindo a Corregedoria Geral de Justiça e a EJUD, de acordo com as especificações, condições e quantidades estimadas, descritas neste Termo de Referência e seus Anexos.

2.2. Havendo divergências entre as especificações dos itens constante do Termo de Referência e as do sistema de pregão eletrônico prevalecerão aquelas.

3. FUNDAMENTAÇÃO DA CONTRATAÇÃO

3.1. Motivação da contratação (art. 18, §3, II, a)

Os serviços tecnológicos providos pelo TJPI, assim como em outros Tribunais pátrios, são acessados diariamente pelo mais diverso público: advogados, servidores, magistrados, promotores, procuradores, cidadãos são apenas alguns exemplos.

Nesse sentido, trafegam nos sistemas e bancos de dados institucionais dados de altíssima criticidade e importância não só para as partes litigantes em processos, mas para o Estado do Piauí como um tudo haja visto que todos os litígios envolvendo órgãos e entidades da Administração Pública Estadual, bem como dos Municípios sitos neste Estado, são decididos pelos juízos vinculados a este Tribunal.

Assim, prover segurança dos dados sob a custódia do TJPI não é tarefa trivial. Pelo contrário, os sistemas informatizados deste Tribunal sofrem ataques diários de indivíduos mal intencionados que buscam acesso aos dados que aqui trafegam.

Nessa toada, **mostra-se necessária a aquisição de solução de proteção de rede moderna, segura e aderente às principais tecnologias existentes no mercado com o fito de garantir a segurança dos dados e sistemas institucionais que suportam as atividades do TJPI**.

Frise-se, em tempo, que a atual solução de firewall existente possui mais de 05 (cinco) anos de uso e que, portanto, encontra-se bastante desatualizada bem como é carente das tecnologias de detecção e prevenção de intrusão (IDS e IPS), dentre outras tecnologias de seguranças modernas.

Dessarte, a aquisição de um firewall de próxima geração (*Next Generation Firewall* – NGFW, no original) **visa resguardar o sigilo e segurança dos dados, bem como prover alta disponibilidade e usabilidade da informação proveniente dos negócios geridos pelo TJPI**.

3.2. Objetivos a serem alcançados (art. 18, §3, II, b)

O objetivo desta Contratação é adquirir de uma solução de segurança capaz de detectar e bloquear ameaças avançadas e que funcione como uma camada extra de segurança para suprir as lacunas de controle que outras ferramentas de segurança não estão aptas a detectar.

3.3. Benefícios diretos e indiretos (art. 18, §3, II, c)

Com a contratação da solução de Firewall de Próxima Geração pretende-se alcançar os seguintes benefícios:

- Garantir a alta disponibilidade, desempenho e confiabilidade dos serviços prestados pelo TJPI;
- Aumentar a qualidade dos serviços prestados pelo TJPI;
- Permitir a administração centralizada das políticas de segurança da informação;
- Minimizar as ameaças ao ambiente computacional do TJPI;
- Permitir o controle de acesso dos usuários dos serviços de rede providos, evitando trafego de aplicativos e conteúdo impróprios;
- Garantir a segurança interna dos dados contra intrusos;
- Aumentar a segurança contra ameaças de vírus oriundos da internet;
- Garantir a confiabilidade, integralidade e disponibilidade das informações;
- Aumentar a visibilidade do tráfego de rede, possibilitando a proatividade na detecção de incidentes;
- Inspecionar acessos criptografados TLS;
- Proteger o TJPI contra ameaças desconhecidas (*Zero-Day*);

- Permitir o controle da utilização dos recursos de rede, sendo possível a aplicação de filtros e bloqueios conforme perfil de usuários, controlando de forma granular a utilização dos recursos;
- Proteger do ambiente de rede, atendendo às exigências do TJPI e do Marco Civil da Internet (Lei N° 12.965/14);
- Diminui a taxa de sucesso dos incidentes de segurança ocasionados por malwares novos e/ou desconhecidos;
- Evitar a propagação de pragas digitais que prejudiquem as atividades do TJPI;
- Aumentar a proteção ao patrimônio digital do TJPI.

3.4. Alinhamento estratégico (art. 18, §3, II, d)

PDTI 2019-2020

Ação	Projeto
Segurança da informação	Implantação de Solução de Segurança "Firewall", com suporte e garantia.

PETIC

Perspectiva	Ação estratégica
Recursos	Melhorar a infraestrutura de hardware e software
Processos Internos	Aprimorar a gestão de segurança da informação

3.5. Referência aos estudos preliminares (art. 18, §3, II, e)

Este Termo de Referência foi elaborada considerando o Documento de Oficialização da Demanda (DOD) encaminhado pela ACSTIC e os Estudos Preliminares constantes do Processo SEI nº 19.0.000107113-3.

3.6. Relação entre a demanda prevista e a contratada (art. 18, §3, II, f)

Para atender a demanda atual do TJPI, resta necessário a aquisição unitária de cada um dos seguintes itens:

1. Cluster de Firewall com licença de Filtro URL e identificação de aplicações, licenças de proteção contra ameaças conhecidas e desconhecidas (Zero-Day) e suporte/garantia 24x7 on site de 3 (três) anos;
2. Software de gerenciamento centralizado para cluster de NGFW com garantia de 3 (três) anos;
3. Treinamento para operação de cluster de NGFW para 06 (seis) pessoas.

Ocorre que a STIC, na qualidade de principal provedora dos serviços de TIC do Poder Judiciário Estadual, não pode se distanciar do planejamento estratégico deste. Assim, levando em consideração que está prevista a instalação de um novo Palácio da Justiça para o ano de 2020, opta-se pela aquisição via **ata de registro de preços** com o seguinte quantitativo:

Lote Único		
Item	**Nome**	**Quantidade**
1	Cluster de Firewall com licença de Filtro URL e identificação de aplicações, licenças de proteção contra ameaças conhecidas e desconhecidas (Zero-Day) e suporte/garantia 24x7 *on site* de 3 (três) anos	02
2	Software de gerenciamento centralizado para *cluster* de NGFW com garantia de 3 (três) anos	02
3	Treinamento para operação de *cluster* de NGFW para 06 (seis) pessoas	02

Em tempo, afirme-se que, apesar do quantitativo a ser registrado ser duas vezes superior à necessidade atual do TJPI, o registro dobrado visa atender eventual necessidade futura quando da inauguração do novo Palácio da Justiça, mantendo um ambiente redundante nos *datacenters* atual e novo.

3.7. Análise do mercado de TIC (art. 18, §3, II, g)

Com o intuito de atender ao disposto na resolução 182/2013 e Instrução Normativa nº 01/2019, este último na qualidade de boa prática administrativa, procedeu-se à pesquisa no Painel de Compras do Governo Federal (http://paineldeprecos.planejamento.gov.br/) em busca de contratações semelhantes no âmbito da administração pública. Ademais, foram contatados revendas das principais fabricantes do mercado com o intuito de complementar a pesquisa de mercado. O resultado é apresentado abaixo:

Nome da Solução	Fabricante	Pregão / Processo Adm.
Next Generation Threat Prevention & SandBlast (NGTX Appliance)	Checkpoint	Pregão Eletrônico nº 5/2018 CAPES (UASG 154003)
Appliance Firewall Check Point 15600 HPP com HA	CheckPoint	Pregão Eletrônico nº 67/2017 DETRAN-RO (UASG 926002)
Fortigate 3200D	Fortinet	Pregão Eletrônico nº 05/2017 Central de Compras (UASG 201057)
PA-5220-AC	Palo Alto	Pesquisa de mercado junto a fornecedor
6800 Turbo *appliance*	CheckPoint	Pesquisa de mercado junto a fornecedor

Ainda em obediência a regra basilar de planejamento a qual apresenta indubitável importância no âmbito da Administração Pública, buscou-se levantar os valores necessários para as outras despesas necessárias ao funcionamento da solução que se pretende contratar. Nesse sentido, além da solução de NGFW propriamente dita, resta imprescindível a aquisição de **software de gerenciamento** e **treinamento** para a operação da solução.

O software de gerenciamento permite a gestão centralizada da solução. Repise-se que a solução em tela é formada por um *cluster* que consiste de dois equipamentos idênticos operando simultaneamente com regras espelhadas e carga de trabalho balanceadas igualmente. A utilização desse tipo de configuração permite garantir a alta disponibilidade (HA – *high availability* no original em inglês) da solução bem como manter a redundância e prevenir contra falhas.

Faz-se necessário afirmar que os custos para a aquisição do programa pretendido variam conforme a fabricante da solução. Afinal, a fabricante do equipamento detém o domínio da tecnologia que comercializa e, consequentemente, é a única desenvolvedora do software já que este fora desenvolvido para seu próprio equipamento. Dessarte, quando da aquisição deste item, **o fabricante do software deverá ser o mesmo da solução para garantir a compatibilidade**.

Em relação ao treinamento para operar a solução, este pode ser realizado de várias maneiras. Nesse sentido, com vias a observância do princípio constitucional da Eficiência, busca-se a **realização do treinamento nas dependências do TJPI ministrado por profissional habilitado e certificado pelo fabricante da solução a ser adquirida**.

3.8. Natureza do objeto (art. 18, §3, II, h)

O objeto a ser contratado enquadra-se na categoria de bens comuns de que tratam a Lei nº

10.520/02 e os Decretos nº 3.555/00 e nº 5.450/05, por possuir padrões de desempenho e características gerais e específicas que podem ser definidos de forma objetiva nas especificações técnicas, que são usualmente encontradas no mercado, podendo, portanto, ser licitado por meio da modalidade Pregão.

3.9. Parcelamento do objeto (art. 18, §3, II, i)

Considerando que se trata de aquisição integrada na qual o software de gerenciamento e o treinamento para operação são completamente voltados para a solução de NGFW, não é viável dividir os itens a serem licitados em lotes. Portanto, recomenda-se a contratação através de **lote único**.

Ademais, tendo em vista que se pretende atender as necessidades atuais e futuras do TJPI, a escolha por ata de registro de preços torna-se mais adequada pois, assim, é possível realizar a contratação em momentos distintos, de acordo com a disponibilidade orçamentária e financeira do Tribunal.

3.10. Forma e critério de seleção do fornecedor (art. 18, §3, III, j)

Tratando-se de lote único, a adjudicação do objeto deverá ser realizada para o mesmo fornecedor com vias a garantir a interoperabilidade entre os itens constantes do lote.

Considerando que os bens e serviços são caracterizados como comuns no mercado de TIC, cujos padrões de desempenho e de qualidade podem ser objetivamente definidos, recomenda-se a utilização do sistema de pregão, na sua modalidade eletrônica.

Os seguintes documentos servirão como condição para aceite da proposta:

i. Especificação clara, completa e minuciosa do produto cotado, informando a marca, o modelo e o fabricante, bem como a indicação precisa da comprovação de cada característica constante nas especificações técnicas deste Termo de Referência;

a) Entende-se por documento (s) a documentação técnica oficial do fabricante do equipamento ofertado, seja em meio eletrônico ou materializada em papel;

b) Não serão aceitas declarações ou cartas de conformidade ou adequação ao solicitado e especificado no termo de referência em substituição ou complementação da documentação técnica oficial e original.

ii. Declaração da licitante de que a mesma tem autorização para comercializar, instalar e prestar serviços de garantia a seus produtos, inclusive treinamento oficial do fabricante, caso não seja fabricante dos itens oferecidos.

3.11. Impacto ambiental (art. 18, §3, III, k)

Não haverá alteração das propriedades físicas, químicas e biológicas do meio ambiente, causada por qualquer forma de matéria ou energia resultante das atividades humanas que, direta ou indiretamente afetam as condições estéticas e sanitárias do meio ambiente. Dentro do quadro existente a melhoria das condições ambientais será trazida pela destinação adequada dos equipamentos e componentes não utilizados, descarte de resíduos eletrônicos e adoção de critérios de sustentabilidade evitando-se o consumo excessivo de energia elétrica, além de limitar o uso de materiais poluentes (graxas, óleos, gases, etc.).

3.12. Conformidade técnica e legal (art. 18, §3, III, l)

No escopo desta contratação, não foram identificados regulamentos técnicos que precisem ser observados.

3.13. Obrigações contratuais (art. 18, §3, III, m)

3.13.1. Das obrigações da Contratante

Além das obrigações resultantes da observância da Lei 8.666/93, o CONTRATANTE deverá:

3.13.1.1. Acompanhar, atestar e remeter nas notas fiscais/faturas a efetiva entrega do objeto;

3.13.1.1.1. Validar e aprovar os produtos e serviços liberados.

3.13.1.1.2. Receber o objeto de acordo com as disposições deste Termo de Referência.

3.13.1.1.3. Definir o Gestor do Contrato, responsável por gerir a execução contratual e, sempre que possível e necessário, o Fiscal Administrativo, responsáveis por fiscalizar a execução contratual, conforme disposto no Art. 16 da Resolução 182/2013 do Conselho Nacional de Justiça – CNJ.

3.13.1.2. Efetuar o pagamento do material, nas condições e preços pactuados, dentro do prazo fixado neste contrato, após a entrega da documentação pelo Fiscal de Contrato à SOF.

3.13.1.2.1. Nenhum pagamento será efetuado enquanto houver pendência de liquidação ou qualquer obrigação financeira em virtude de penalidade ou inadimplência;

3.13.1.3. Comunicar à CONTRATADA, o mais prontamente possível, qualquer anormalidade observada no fornecimento do objeto requisitado que possa comprometer a tempestividade, a qualidade e a eficácia do uso a que se destina;

3.13.1.4. Exigir o cumprimento de todos os compromissos assumidos pela Contratada.

3.13.1.5. Fornecer, a qualquer tempo e com a máxima presteza, mediante solicitação escrita da CONTRATADA, informações adicionais, dirimir dúvidas e orientá-la em todos os casos julgados necessários;

3.13.1.6. Manter os contatos com a CONTRATADA por escrito, ressalvados os entendimentos verbais determinados pela urgência que, posteriormente, devem ser confirmados por escrito no prazo de até 72 (setenta e duas) horas.

3.13.1.7. O Contratante não aceitará, sob nenhum pretexto, transferência de responsabilidade da CONTRATADA para terceiros, sejam fabricantes, representante ou quaisquer outros.

3.13.1.8. Permitir acesso dos empregados da contratada às dependências do TJPI para entrega do objeto.

3.13.1.8.1. Fornecer a infraestrutura necessária para a realização das atividades que devam ser executadas em suas instalações conforme as especificações estabelecidas neste Termo de Referência.

3.13.1.8.2. Providenciar o acesso controlado aos recursos de TIC do TJPI para os profissionais da contratada durante a fase de execução do objeto, caso necessário.

3.13.1.9. Supervisionar, gerenciar e fiscalizar os procedimentos a serem realizados pelos ficais de contrato.

3.13.1.10. Exigir o afastamento de qualquer funcionário ou preposto da CONTRATADA que venha a causar embaraço ou que adote procedimentos incompatíveis com o exercício das funções que lhe forem atribuídas.

3.13.1.11. Responsabilizar-se pela observância às Leis, Decretos, Regulamentos, Portarias e demais normas legais, direta e indiretamente aplicáveis ao contrato.

3.13.1.12. Aplicar à CONTRATADA as penalidades regulamentares e contratuais.

3.13.2. Das obrigações da Contratada

Além das obrigações resultantes da observância da Lei 8.666/93, a CONTRATADA deverá:

3.13.2.1. Fornecer o(s) objeto(s) conforme especificações, quantidades, prazos e demais condições estabelecidas no Edital e seus anexos, na Proposta e no Contrato.

3.13.2.2. Responsabilizar-se integralmente pela sua equipe técnica, primando pela qualidade, desempenho, eficiência e produtividade, visando à execução dos trabalhos vinculados ao fornecimento, dentro dos prazos e condições estipulados, sob pena de ser considerada infração passível de aplicação de penalidades previstas contratualmente, caso os prazos e condições não sejam cumpridos.

3.13.2.3. Responsabilizar-se pela observância de Leis, Decretos, Regulamentos, Portarias e normas federais, estaduais e municipais direta e indiretamente aplicáveis ao objeto do contrato.

3.13.2.4. Atender prontamente às solicitações do Tribunal de Justiça do Estado do Piauí no fornecimento do objeto nas quantidades e especificações deste Termo de Referência, de acordo com a necessidade desta Corte, a partir da solicitação do Gestor do Contrato.

3.13.2.5. Seguir as instruções e observações efetuadas pelo Gestor do Contrato, bem como reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, partes do objeto em que se verificarem vícios, defeitos ou incorreções.

3.13.2.6. Reportar formal e imediatamente ao Gestor do Contrato quaisquer problemas, anormalidades, erros e irregularidades que possam comprometer a execução contratual.

3.13.2.7. Assumir responsabilidade irrestrita sobre a totalidade do fornecimento de insumos e serviços associados ao fornecimento do objeto.

3.13.2.8. Indicar, formalmente, preposto apto a representá-la junto ao contratante que deverá responder pela fiel execução do Contrato.

3.13.2.9. Cuidar para que o preposto indicado mantenha permanente contato com o Gestor do Contrato e adote as providências requeridas pelo TJPI, além de comandar, coordenar e controlar a atuação deste quando da execução do objeto.

3.13.2.10. Prestar todos os esclarecimentos que forem solicitados pelo Tribunal de Justiça do Piauí, devendo, ainda, atender prontamente as reclamações.

3.13.2.11. Comunicar, imediatamente e por escrito, qualquer anormalidade ou problema detectados, prestando ao contratante os esclarecimentos que julgar necessários.

3.13.2.12. Manter, durante a execução contratual, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para o fornecimento do objeto.

3.13.2.13. Assumir inteira responsabilidade técnica e operacional pelo fornecimento do objeto e os serviços diretamente vinculados, não podendo, sob qualquer hipótese, transferir para outra empresa a responsabilidade por eventuais problemas na execução.

3.13.2.14. Responder integralmente por quaisquer perdas ou danos causados ao contratante ou a terceiros em razão de ação ou omissão, dolosa ou culposa, sua ou dos seus profissionais em razão da execução contratual, independentemente de outras cominações contratuais ou legais a que estiver sujeito.

3.13.2.15. Arcar com todas as despesas decorrentes de transporte, diárias, tributos, seguros, alimentação, assistência médica e de pronto socorro, ou qualquer outra despesa de seus empregados.

3.13.2.16. Arcar com o pagamento de todas as despesas decorrentes do fornecimento do objeto, incluindo as despesas definidas em leis sociais, trabalhistas, comerciais, tributárias e previdenciárias, impostos e todos os custos, insumos e demais obrigações legais, inclusive todas as despesas que onerem, direta ou indiretamente, o objeto ora contratado, não cabendo, pois, quaisquer reivindicações da CONTRATADA, a título de revisão de preço ou reembolso.

3.13.2.17. Promover, por sua conta e risco, o transporte de seus empregados, materiais e utensílios necessários à execução contratual, até as instalações do contratante.

3.13.2.18. Respeitar e fazer com que seus empregados respeitem as normas de segurança do trabalho, disciplina e demais regulamentos vigentes no Estado do Piauí, bem como atentar para as regras de cortesia onde sejam executados os serviços.

3.13.2.19. Substituir qualquer de seus profissionais cuja qualificação, atuação, permanência ou comportamento durante a execução do objeto forem julgados prejudiciais, inconvenientes ou insatisfatórios à disciplina do órgão ou ao interesse do serviço público por outro de qualificação igual ou superior, sempre que exigido pelo contratante

3.13.2.20. Garantir a execução dos serviços vinculados à execução contratual, mantendo equipe adequadamente dimensionada para tanto, sem ônus adicionais para o órgão contratante.

3.13.2.21. Zelar pela boa e completa execução dos serviços vinculados à execução contratual, mantendo recursos técnicos e humanos necessários para evitar a interrupção indesejada dos mesmos.

3.13.2.22. Facilitar, por todos os meios a seu alcance, a ampla ação fiscalizadora do órgão contratante, atendendo prontamente as observações e exigências que lhe forem dirigidas.

3.13.2.23 Manter sigilo, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto de interesse do contratante ou de terceiros de que tomar conhecimento em razão da execução do objeto do Contrato, especialmente em relação a: dados, informações, regras de negócios, documentos, e outros.

3.13.2.24. Honrar os honorários e encargos sociais devidos pela sua condição de única empregadora do pessoal designado para execução dos serviços vinculados ao fornecimento, incluindo indenizações decorrentes de acidentes de trabalhos, demissões, vales-transporte, entre outros, obrigando-se, ainda, ao fiel cumprimento das legislações trabalhistas e previdenciárias, sendo-lhe defeso invocar a existência deste contrato para eximir-se dessas obrigações ou transferi-las para o contratante.

3.13.2.25. Responder, perante o contratante e terceiros, pela conduta dos seus empregados designados para execução do objeto do contrato, com o propósito de evitar condutas que possam comprometer a segurança ou a credibilidade do Contratante.

3.13.2.26. Adotar regras de vestimenta para seus profissionais adequada com o ambiente do órgão, com trajes em bom estado de conservação e portando crachá de identificação funcional com foto e nome visível, arcando com o ônus de sua confecção.

3.13.2.27. Utilizar as melhores práticas de mercado no gerenciamento de recursos humanos e supervisão técnica e administrativa para garantir a qualidade da execução do objeto e o atendimento das especificações contidas no Contrato, Edital e seus Anexos.

3.13.2.28. Cumprir e fazer cumprir por seus profissionais as normas e procedimentos estabelecidos na Política de Segurança da Informação do Contratante.

3.13.2.29. Identificar qualquer equipamento de sua posse que venha a ser utilizado nas dependências do órgão contratante, afixando placas de controle patrimonial, selos de segurança, entre outros pertinentes e responsabilizar-se por estes.

3.13.2.30. Manter os contatos com o Contratante sempre por escrito, ressalvados os entendimentos verbais determinados pela urgência na execução do Contrato que, posteriormente, devem sempre ser confirmados por escrito, dentro de até 72 (setenta e duas) horas, a contar da data de contato;

3.13.2.31. Aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários de até 25% (vinte e cinco por cento) do valor inicial do contrato.

3.13.2.32. Comunicar ao Contratante, com antecedência de 48 (quarenta e oito) horas os motivos que eventualmente impossibilitem a prestação dos serviços no prazo estipulado, nos casos em que houver impedimento justificado para funcionamento normal de suas atividades, sob a pena de sofrer as sanções da Lei 8.666/93.

3.13.2.33. Vincular-se ao que dispõe a lei nº 3.078, de 11/09/90 (Código de Proteção de Defesa do Consumidor).

3.13.2.34. São expressamente vedadas à CONTRATADA:

I. A contratação de servidor pertencente ao quadro de pessoal do TJ/PI, durante o período de fornecimento.

II. A subcontratação parcial ou total do objeto do Contrato (atenção: a subcontratação deve ser permitida caso a caso pela Administração e deve estar prevista no edital, sob pena de rescisão contratual).

4. Especificação técnica (art. 18, §3º, III)

4.1. Modelo de execução e gestão do contrato (art. 18, §3º, III, a)

4.1.1. Principais papéis

I – Equipe de Apoio à Contratação: equipe responsável por subsidiar a Área de Licitações em suas dúvidas, respostas aos questionamentos, recursos e impugnações, bem como na análise e julgamento das propostas das licitantes;

II – Equipe de Gestão da Contratação: equipe composta pelo Gestor do Contrato, responsável por gerir a execução contratual e, sempre que possível e necessário, pelos Fiscais Demandante, Técnico e Administrativo, responsáveis por fiscalizar a execução contratual, consoante às atribuições regulamentares;

III – Equipe de Fiscalização: equipe composta pelos Fiscais Demandante, Técnico e Administrativo, responsáveis por fiscalizar a execução contratual, consoante às atribuições regulamentares;

IV – Gestor do Contrato: servidor com atribuições gerenciais, técnicas ou operacionais relacionadas ao processo de gestão do contrato, sendo responsável por gerir a execução consoante às atribuições regulamentares;

V – Fiscal Demandante do Contrato: servidor representante da Área Demandante da Solução de Tecnologia da Informação e Comunicação, indicado pela respectiva autoridade competente para fiscalizar o Contrato quanto aos aspectos funcionais da solução;

VI – Fiscal Administrativo do Contrato: servidor representante da Área Administrativa, indicado pela respectiva autoridade competente para fiscalizar o Contrato quanto aos aspectos administrativos da execução, especialmente os referentes ao recebimento, pagamento, sanções, aderência às normas, diretrizes e obrigações contratuais;

VII – Fiscal Técnico do contrato: servidor representante da Área de Tecnologia da Informação e Comunicação, indicado pela respectiva autoridade competente para fiscalizar o contrato quanto aos aspectos técnicos da solução;

VIII – Preposto: funcionário representante da Contratada, responsável por acompanhar a execução do Contrato e atuar como interlocutor principal junto ao Gestor do Contrato, incumbido de receber, diligenciar, encaminhar e responder as questões técnicas, legais e administrativas referentes ao andamento contratual. Em caso de substituição do Preposto, a contratada deverá comunicar formalmente a equipe de fiscalização, via e-mail, o nome do preposto substituto.

4.1.2.1. Prazos e condições de entrega e recebimento do objeto:

4.1.2.1.1. O prazo de entrega do objeto é de **60 (sessenta) dias corridos**, contados a partir da publicação do extrato do Contrato ou da Ordem de Fornecimento.

4.1.2.1.1.1. **Excepcionalmente**, o prazo de recebimento poderá ser prorrogado por até 30 (trinta) dias, desde que solicitado pelo fornecedor e com apresentação de justificativa, nos termos do art. 57, §1º, Lei nº 8.666.

4.1.2.1.1.2. Toda prorrogação de prazo deverá ser justificada por escrito e previamente autorizada pela autoridade competente a assinar o Contrato ou a Ordem de Fornecimento.

4.1.2.1.1.3. Caberá à Equipe de Fiscalização e ao setor demandante auxiliarem a autoridade competente na análise do deferimento da prorrogação.

4.1.2.1.2. A CONTRATADA deverá entregar o objeto em dias úteis, no horário de 08 (oito) às 14 (quatorze) horas, no Departamento de Material e Patrimônio do Tribunal de Justiça do Estado do Piauí, situado na Rua Jornalista Lívio Lopes, S/N, Bairro: Redonda, em Teresina-PI. É obrigatório o

aviso e agendamento da entrega com 24 (vinte e quatro) horas de antecedência, por meio do e-mail: almoxarifado@tjpi.jus.br, e/ou do telefone: (86) 3237-9984.

4.1.2.1.3. Por ocasião do recebimento do objeto serão aferidas a qualidade e a quantidade de acordo com o disposto neste Termo de Referência e na proposta vencedora.

4.1.2.1.4. O objeto deverá ser entregue acompanhado da Nota Fiscal e a cópia do Contrato e/ou Ordem de Fornecimento.

4.1.2.1.5. Nos termos dos artigos 73 a 76 da lei 8.666/1993, o objeto deste Termo de Referência será recebido:

a) **provisoriamente**, por qualquer dos membros da Equipe de Fiscalização, para efeito de posterior verificação da conformidade do material com a especificação constante neste Termo de Referência;

b) **definitivamente**, mediante lavratura de Termo de Recebimento Definitivo assinado pela Equipe de Gestão da Contratação, em até 10 (dez) dias úteis do término da fase de instalação, configuração e testes da solução (item 4.1.2.2.3 deste Termo), ocasião em que se fará constar o Atesto na Nota Fiscal.

4.1.2.1.6. Os produtos entregues em desconformidade com o especificado neste Termo ou o indicado na proposta serão rejeitados parcial ou totalmente, conforme o caso, e a Contratada será obrigada a substituí-los no prazo de até 30 (trinta) dias consecutivos, contados da data do recebimento da Notificação escrita, necessariamente acompanhada do Termo de Recusa do Material, sob pena de incorrer em atraso quanto ao prazo de execução.

4.1.2.1.6.1. A notificação de que trata o item anterior suspende os prazos de pagamento até que a irregularidade seja sanada.

4.1.2.1.7. O recebimento não exclui a responsabilidade da CONTRATADA pelo perfeito desempenho do material fornecido ou dos serviços prestados, cabendo-lhe sanar quaisquer irregularidades quando detectadas.

4.1.2.1.8. Na entrega do objeto, as despesas de embalagem, seguros, transportes, tributos, encargos trabalhistas e previdenciários decorrentes do fornecimento e/ou substituições do objeto, indicadas pela CONTRATANTE, deverão ser de responsabilidade da CONTRATADA, sem ônus para CONTRATANTE.

4.1.2.2. Cronograma de execução dos serviços:

4.1.2.2.1. Planejamento da instalação e entrada em operação: em até 10 (dez) dias contados da publicação do extrato do contrato deverá ser realizada Reunião de Alinhamento entre a STIC e a contratada. Na ocasião serão acordados as datas estimadas para entrega do objeto, instalação, testes, entrega definitiva e treinamento da solução, tendo em vista os prazos acordados pelas partes.

4.1.2.2.2. Prazo de entrega da solução: a CONTRATADA deverá fornecer os equipamentos no prazo máximo de 60 (sessenta) dias corridos contados da publicação do extrato do contrato. Excepcionalmente, o prazo retromencionado poderá ser prorrogado por mais 30 (trinta) dias desde que solicitado pelo CONTRATANTE acompanhado de justificativa e aprovação por parte da Administração.

4.1.2.2.3. Fase de instalação, configuração e testes da solução: a CONTRATADA deverá realizar a instalação, configuração e testes com base nas diretrizes e comandos apontados pelo gerente do projeto da CONTRATANTE, neste Termo de Referência e no acordado no item 4.1.2.2.1 no prazo máximo de 45 (quarenta e cinco) dias contados da entrega da solução. Nesse período, a solução passará por testes extensivos realizados pela equipe da CONTRATANTE. A aprovação desta fase pelo gerente do projeto da CONTRATANTE configura condição necessária para a expedição do termo de recebimento definitivo ou documento equivalente.

4.1.2.2.4. Prazo para emissão do termo de recebimento definitivo ou documento equivalente: em até 10 (dez) dias úteis do término da fase de instalação, configuração e testes da solução a equipe de planejamento da contratação fornecerá o termo de recebimento definitivo atestando a regularidade do fornecimento e dando início ao prazo da garantia da solução.

4.1.2.2.5. Cronograma da realização dos treinamentos: preferencialmente os treinamentos serão realizados durante a fase de testes especificada no item 4.1.2.2.3 deste Termo, de acordo com o acordo com o cronograma pactuado na Reunião de Alinhamento. Alternativamente, poderá ser definido prazo distinto deste item desde que acordado expressamente entre CONTRATANTE e CONTRATADA.

4.1.2.3. Instrumentos formais de solicitação de fornecimento:

4.1.2.3.1. Documento de solicitação de fornecimento: Contrato ou Ordem de fornecimento devidamente assinado por ambos os contratantes.

4.1.2.3.2. Documento de recebimento provisório: recibo assinado por qualquer integrante da equipe de gestão da contratação.

4.1.2.3.3. Documento de recebimento definitivo: Termo de Recebimento Definitivo assinado pela Equipe de Gestão da Contratação.

4.1.2.3.4. Solicitações de chamado técnico:

a. Chamado Técnico por meio de Mensagem eletrônica (e-mail) como ferramenta preferencial de solicitação, acompanhamento e de aferição do serviço prestado pela Contratada;

b. Chamado Técnico de forma eletrônica por meio de Central on-line;

c. Chamado Técnico por meio telefônico para Central de Atendimento

4.1.2.4. Prazos de garantia e níveis mínimos de serviço exigidos:

4.1.2.4.1. Período de garantia técnica: 36 (trinta e seis) meses, contados a partir do recebimento definitivo da instalação.

4.1.2.4.2. Durante o prazo de garantia técnica, a Contratada deverá garantir o funcionamento da solução como um todo, fornecer atualizações, prestar suporte técnico e atender aos chamados técnicos para manutenção.

4.1.2.4.1.1. A Contratada deverá apresentar, até a data do recebimento definitivo da instalação, instrumento que comprove, junto ao fabricante, o início do serviço de suporte técnico da solução.

4.1.2.4.3. O suporte deverá ser integral durante os 365 (trezentos e sessenta e cinco) dias do ano, na modalidade 24x7 (vinte e quatro horas por dia, sete dias por semana).

4.1.2.4.4. A garantia deverá cobrir defeitos no equipamento bem como incluir todas as atualizações de todos os softwares que compõem a solução durante o período contratado.

4.1.2.4.5. Os Níveis de Serviços Exigidos (NSE) serão classificados conforme os níveis de criticidade a seguir:

Prazo de Solução Definitiva	
Criticidade ALTA	08 (oito) horas
Criticidade MÉDIA	24 (vinte e quatro) horas
Criticidade BAIXA	48 (quarenta e oito) horas

i. Criticidade ALTA: Esse nível de criticidade é aplicado quando há indisponibilidade de qualquer item de software ou hardware que a solução inoperante;

ii. Criticidade MÉDIA: Esse nível de criticidade é aplicado quando há falha, simultânea ou não, de hardware ou software que não inviabilize o uso da solução, mas diminua alguma funcionalidade ou afete negativamente a performance;

iii. Criticidade BAIXA: Esse nível de criticidade é aplicado para a instalação, configuração, manutenções, esclarecimentos técnicos relativos ao uso e aprimoramento da solução, bem como chamados técnicos que não requeiram imediatos atendimentos.
4.1.2.4.6. Os Níveis de Serviços Exigidos (NSE) serão tratados da seguinte forma:

i. Prazo de Solução Definitiva: Tempo decorrido entre o envio da mensagem de chamado técnico efetuado pelo Fiscal Técnico ou Gestor do Contrato, e a efetiva recolocação da solução em seu pleno estado de funcionamento;

ii. Caso seja verificado que a solução apresentada pela empresa não resolveu o problema definitivamente, o chamado será reaberto pelo Fiscal Técnico ou Gestor do Contrato e o prazo continuará a ser contado a partir do momento de sua suspensão.

iii. O atendimento aos chamados técnicos de criticidade ALTA poderá ser realizado também de forma on-site, desde que solicitado pelo Fiscal Técnico ou Gestor do Contrato;

iv. A interrupção do suporte de um chamado técnico classificado no tipo de criticidade ALTA pela Contratada e que não tenha sido previamente autorizado pelo Fiscal Técnico ou Gestor do Contrato, poderá ensejar em aplicação de penalidades previstas.

v. Após a conclusão do suporte, a equipe técnica da Contratada comunicará formalmente (preferencialmente por mensagem eletrônica) ao Fiscal Técnico ou Gestor do Contrato e solicitará autorização para o fechamento do chamado;

vi. Caso não seja confirmada a solução definitiva do problema, o chamado permanecerá aberto até que seja efetivamente solucionado pela Contratada. Nesse caso o Fiscal Técnico ou Gestor do Contrato informará as pendências relativas ao chamado aberto.

vii. Por necessidade excepcional de serviço, o Fiscal Técnico ou Gestor do Contrato poderá solicitar o escalonamento de chamado para níveis superiores de criticidade. Nesse caso, o escalonamento deverá ser justificado e os prazos dos chamados técnicos reiniciar-se-ão.

viii. Sempre que houver quebra dos níveis de serviços exigidos ou problemas que afetem a execução do objeto, o Gestor do Contrato enviará notificação por mensagem eletrônica para a Contratada que terá o prazo de até 48 (quarenta e oito) horas corridas e contadas a partir do recebimento da notificação para apresentar as justificativas para as falhas verificadas;

ix. Caso não haja manifestação dentro desse prazo ou caso o Gestor do Contrato entenda serem improcedentes as justificativas apresentadas, será iniciado processo de aplicação de penalidades previstas, conforme o nível de serviço transgredido.

4.1.2.5. Formas de comunicação e acompanhamento

4.1.2.5.1. Além da reunião de alinhamento e validação de expectativas, deverão ser realizadas, se necessárias, outras reuniões presenciais ou não entre o Gestor do Contrato e o Preposto da Contratada para avaliação do(s) serviço(s) prestado(s) no período, e verificação do atendimento aos requisitos contratuais estabelecidos;

4.1.2.5.2. Poderão ser realizados, alternativamente, e a critério do Gestor do Contrato, o controle e o acompanhamento da prestação de serviço mediante o uso de mensagens eletrônicas. Nesse caso, o Fiscal Técnico ou Gestor do Contrato deverá apresentar descritivo contendo situações merecedoras de avaliação por parte da Contratada.

4.1.2.6. Forma de pagamento

4.1.2.6.1. O pagamento obedecerá, para cada fonte diferenciada de recursos, a estrita ordem cronológica das datas de suas exigibilidades, conforme determinado pela IN TCE/PI nº 02/2017 e art.5º da Lei 8.666/93.

4.1.2.6.2. O pagamento será efetuado pela Administração, em moeda corrente nacional, por Ordem Bancária, acompanhado dos seguintes documentos, remetidos pelo Fiscal de Contrato ou pela Comissão de Fiscalização:

a) Termo de Recebimento Definitivo ou Recibo, devidamente preenchido e assinado;

b) Apresentação da Nota Fiscal com dados bancários, fatura ou documento equivalente, atestado pelo setor competente;

c) Cópia do Contrato Administrativo ou da Ordem de Fornecimento; e

d) Cópia da Nota de Empenho;

e) Prova de regularidade perante o Instituto Nacional do Seguro Social – INSS;

f) Prova de regularidade do FGTS;

g) Prova de regularidade com a Fazenda Pública Federal, Estadual e Municipal do domicílio ou sede e dívida ativa;

h) Certidão Negativa de Débitos Trabalhistas; e

g) Consulta ao Cadastro de Empresas Inidôneas e Suspensas - CEIS.

4.1.2.6..3. As certidões extraídas do Sistema de Cadastramento Unificado de Fornecedores – SICAF substituirão os documentos relacionados nas letras e, f, g e h, nos termos da Instrução Normativa nº 03/2018 - SEGES/MPDG.

4.1.2.6..4. A Nota Fiscal/Fatura deverá ser emitida pela licitante vencedora, obrigatoriamente com o número de inscrição no CNPJ apresentado nos documentos de habilitação e das propostas, não se admitindo Notas Fiscais/Faturas emitidas com outros CNPJ, mesmo aquelas de filiais ou da matriz. As Notas Fiscais deverão conter discriminação idêntica à contida na respectiva Nota de Empenho.

4.1.2.6..5. O banco ao qual pertence à conta da empresa deve ser cadastrado no sistema do Banco Central do Brasil, para que seja possível a compensação bancária, na qual o SOF / FERMOJUPI creditará os pagamentos a que faz jus a empresa contratada.

4.1.2.6..6. Nenhum pagamento será efetuado enquanto houver pendência de liquidação ou qualquer obrigação financeira em virtude de penalidade ou inadimplência.

4.1.2.6..7. Na existência de erros, omissões ou irregularidades, a documentação será devolvida à empresa contratada/fornecedora, para as correções devidas, passando o novo prazo para pagamento a ser contado a partir da data da apresentação dos documentos corrigidos.

4.1.2.6..8. Não haverá, em hipótese alguma, pagamento antecipado.

4.1.2.6..9. Nos casos de eventuais atrasos de pagamento, desde que a licitante vencedora não tenha concorrido de alguma forma para tanto, incidirão correção monetária e juros moratórios.

4.1.2.6..10. Fica convencionado que a correção monetária e os encargos moratórios serão calculados entre a data do adimplemento da parcela e a do efetivo pagamento da nota fiscal/fatura, com a aplicação da seguinte fórmula:

EM = I x N x 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 compensação financeira = 0,0001638, assim apurado:

I = TX/365 I = 0,06/365 I = 0,0001644

TX = Percentual da taxa anual = 6%.

4.1.2.6..11. A correção monetária será calculada com a utilização do índice IGP-M da Fundação Getúlio Vargas.

4.1.2.6..12. No caso de atraso na divulgação do IGPM, será pago à licitante vencedora a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja divulgado o índice definitivo.

4.1.2.6..13. Caso o IGPM estabelecido venha a ser extinto ou de qualquer forma não possa mais ser utilizado, será adotado em substituição o que vier a ser determinado pela legislação então em vigor.

4.1.2.6..14. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial.

4.1.2.6..15. Qualquer atraso ocorrido na apresentação da nota fiscal, ou dos documentos exigidos como condição para pagamento por parte da CONTRATADA importará em prorrogação automática do prazo de vencimento da obrigação do CONTRATANTE.

4.1.2.7. Transferência de conhecimento

4.1.2.7.1. Os seguintes procedimentos deverão ser seguidos durante toda a execução do objeto, em especial durante a prestação de serviço de garantia técnica:

i. A equipe da CONTRATADA deverá apresentar ao Fiscal Técnico do Contrato de forma objetiva e por escrito todos os procedimentos realizados nos chamados abertos pelo TJPI em vistas de problemas ou interrupções na solução que forem sanados.

ii. Para que ocorra a transferência de conhecimento, no fechamento dos chamados técnicos de garantia técnica, a Contratada deverá apresentar por mensagem eletrônica ou em documento apropriado, a solução para o problema que originou a abertura do chamado;

iii. O envio da solução pelos meios devidos não exime a Contratada da apresentação do Relatório Gerencial de Serviços com a consolidação dos chamados técnicos abertos;

iv. Os conhecimentos técnicos repassados para a equipe da Secretaria de Tecnologia da Informação serão utilizados em casos de interrupção, transição e encerramento contratual, de modo a minimizar impactos e permitir que as necessidades do TJPI não sejam prejudicadas ou interrompidas.

4.1.2.8. Direitos de propriedade intelectual

4.1.2.8.1 Os direitos de propriedade intelectual permanecerão de posse da empresa fabricante do produto a ser adquirido, não havendo transferência de direitos de propriedade em face de contratação, salvo os direitos de uso da solução contratada.

4.1.2.9. Qualificação técnica e formação dos profissionais envolvidos

4.1.2.9.1. Os profissionais da CONTRATADA deverão possuir qualificação condizente com o fornecimento do objeto, em especial deverão possuir certificação ou documento equivalente emitido pela fabricante do equipamento a ser fornecido que ateste a qualificação técnica do profissional na operação, manutenção e instalação do equipamento.

4.1.2.9.2. O instrutor que ministrar o treinamento objeto do item 3 do lote único deste Termo deverá ser credenciado como instrutor autorizado pela fabricante do equipamento.

4.1.2.10. Penalidades administrativas

4.1.2.10.1. Comete infração administrativa nos termos da Lei nº 8.666/93 e da Lei nº 10.520/02, a licitante vencedora que:

4.1.2.10.1.1. Não Celebrar o Contrato;

4.1.2.10.1.2. Deixar de entregar ou apresentar documentação falsa exigida para o certame;

4.1.2.10.1.3. Ensejar o retardamento da execução de seu objeto;

4.1.2.10.1.4. Não mantiver a proposta;

4.1.2.10.1.5. Falhar ou fraudar na execução do contrato;

4.1.2.10.1.6. Comportar-se de modo inidôneo;

4.1.2.10.1.7. Cometer fraude fiscal;

4.1.2.10.2. Para os fins do item 4.1.2.10.1.6, reputar-se-ão inidôneos atos tais como os descritos nos artigos 92, parágrafo único, 96 e 97, parágrafo único, da Lei n.º 8.666/1993.

4.1.2.10.3. A Contratada que cometer qualquer das infrações discriminadas acima ficará sujeita, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções, tomando por base o Anexo II:

a) Advertência, em caso de faltas ou descumprimentos de regras contratuais que não causem prejuízo ao CONTRATANTE

b) Multa:

b.1.) Multa moratória de até 15% (quinze por cento) sobre o valor da parcela inadimplida, no caso de atraso injustificado, até o limite de 30 (trinta) dias;

b.2) Multa compensatória de até 30% (trinta por cento) sobre o valor do contrato, no caso de inexecução total do objeto, configurada após o nonagésimo dia de atraso;

b.3) Em caso de **inexecução parcial**, aplicar-se-á a multa compensatória, no mesmo percentual do subitem anterior, de forma proporcional à obrigação inadimplida;

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

d) Declaração de inidoneidade para licitar ou contratar com a Administração Pública enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade.

e) Impedimento de licitar e contratar com a União, Estados, Distrito Federal ou Municípios, pelo prazo de até 05 (cinco) anos, sem prejuízo das multas previstas neste Contrato e demais cominações legais.

4.1.2.10.4. As sanções previstas nas alíneas "a", "c" e "d" do subitem anterior poderão ser aplicadas cumulativamente à pena de multa, de acordo com o Anexo I, do TR.

4.1.2.10.5. Também ficam sujeitas às penalidades do art. 87, III e IV da Lei nº 8.666, de 1993, as empresas ou profissionais que:

4.1.2.10.5.1. Tenham sofrido condenação definitiva por praticar, por meio dolosos, fraude fiscal no recolhimento de quaisquer tributos;

4.1.2.10.5.2. Tenham praticado atos ilícitos visando a frustrar os objetivos da licitação;

4.1.2.10.5.3. Demonstrem não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.

4.1.2.10.6. Após o nonagésimo dia de atraso, o TJ/PI poderá rescindir o contrato, caracterizando-se a inexecução total do seu objeto.

4.1.2.10.7. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa à Contratada, observando-se o procedimento previsto na Lei nº 8.666, de 1993.

4.1.2.10.8. A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

4.1.2.10.9. O valor da multa aplicada será descontado da garantia prestada, se houver, ou descontado de pagamentos eventualmente devidos à Contratada. Na inexistência destes, será pago mediante depósito bancário em conta a ser informada pela Contratante ou judicialmente.

4.1.2.10.10. Ad cautelam, o TJ/PI poderá efetuar a retenção do valor presumido da multa, antes da instauração do regular procedimento administrativo.

4.1.2.10.11. Se o valor do pagamento for insuficiente, fica a contratada obrigada a recolher a importância devida no prazo de 15 (quinze) dias, contado da comunicação oficial.

4.1.2.10.12. Esgotados os meios administrativos para cobrança do valor devido pela contratada ao TJ/PI, a contratada será encaminhada para inscrição em dívida ativa.

4.1.2.10.13. Do ato que aplicar a penalidade caberá recurso, no prazo de 05 (cinco) dias úteis, a contar da ciência da intimação, podendo a Administração reconsiderar ou não sua decisão ou nesse prazo, encaminhá-lo, devidamente informados para a apreciação e decisão superior, dentro do mesmo prazo;

4.1.2.10.14. Serão publicadas no Diário da Justiça do TJPI as sanções administrativas previstas, inclusive a reabilitação perante a Administração Pública.

5. Requisitos técnicos específicos (art. 18, §3º, IV)

ITEM 1 - CLUSTER DE FIREWALL COM LICENÇA DE FILTRO URL, LICENÇAS DE PROTEÇÃO CONTRA AMEAÇAS CONHECIDAS E DESCONHECIDAS E SUPORTE/GARANTIA DE 3 ANOS

1. O *cluster* deve ser composto por 2 *appliances* idênticos em características de hardware e software/licenças para operar em alta disponibilidade;
2. O *cluster* de Firewall com licença de Filtro URL, licenças de proteção contra ameaças conhecidas e desconhecidas e suporte/garantia de 3 anos, deve possuir a capacidade e as características mínimas abaixo, por equipamento:
    a. *Throughput* de 12 Gbps com a funcionalidade de controle de aplicação habilitada para todas as assinaturas que o fabricante possuir;
    b. *Throughput* de 8 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;
    c. Os throughputs devem ser comprovados por documento de domínio público do fabricante;
    d. Os documentos públicos devem comprovar os *throughputs* aferidos com tráfego HTTP ou *blend* de protocolos de tráfego real padrão de mercado (*real-word traffic blend, enterprise mix* ou similar);
    e. Não será aceito aceleração de pacotes na placa de rede limitando a análise somente até camada 4.
    f. Suporte a, no mínimo, 3.800.000 (três milhões e oitocentos mil) conexões simultâneas;
    g. Suporte a, no mínimo, 110.000 (cento e dez mil) novas conexões por segundo;
    h. Fonte 120/240 AC, redundante e *hot-swap* (possibilitando que a mesma seja substituída de forma rápida e simples, sem a necessidade de que o equipamento seja desligado);
    i. Cooler *hot-swap*;
    j. Discos de, no mínimo, 480 GB, em redundância;
    k. 08 (oito) interfaces de rede 10 Gbps SFP+, com 08 *transceivers* SFP+ multimodo compatíveis com o equipamento ofertado;
    l. 02 (duas) interfaces de rede de, no mínimo, 40 Gbps padrão QSFP+ ou QSFP28;
    m. Caso a solução ofertada possua quantidade de interfaces de rede superior ao exigido, estas devem ser entregues totalmente licenciadas, permitindo o uso de todas as interfaces disponíveis simultaneamente sem necessidade de licenciamento adicional;
    n. Deve possuir interface e acompanhar cabo para interconectar os *appliances* em modo de alta disponibilidade;
    o. 01 (uma) interface do tipo console ou similar;
    p. 01 (uma) interface USB;
    q. 01 (uma) interface de, no mínimo, 1 Gbps para gerenciamento out-of-band;
    r. Suporte a, no mínimo, 2.000 (dois mil) zonas de segurança;
    s. Estar licenciada para ou suportar sem o uso de licença, 10.000 (dez mil) clientes de VPN SSL simultâneos;
    t. Estar licenciada para ou suportar sem o uso de licença, 3.000 (três mil) túneis de VPN IPSEC simultâneos;
    u. Deve ser entregue com licenciamento ativo para suportar, no mínimo, 10 sistemas virtuais lógicos (contextos) no firewall físico;
3. Deve permitir expansão futura a até 20 sistemas virtuais lógicos (contextos) no firewall físico;
4. Os contextos virtuais devem suportar as funcionalidades nativas do *gateway* de proteção incluindo: Firewall, IPS, Antivírus, Anti-Spyware, Filtro de URL, Filtro de Dados, VPN, Controle de Aplicações, QOS, NAT e Identificação de usuários;

5. Por cada equipamento que compõe a plataforma de segurança, entende-se o hardware e as licenças de softwares necessárias para o seu funcionamento;
6. Por console de gerência e monitoração, entende-se as licenças de software necessárias para as suas funcionalidades, bem como hardware dedicado para o funcionamento das mesmas;
7. Na data da proposta, nenhum dos modelos ofertados poderá estar listado no site do fabricante em listas de *end-of-life, end-of-sale e end-of-support*, ou seja, não poderá haver previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante;

CARACTERÍSTICAS GERAIS

8. A solução deve consistir de *appliances* de proteção de rede com funcionalidades de Next Generation Firewall (NGFW), e console de gerência e monitoramento;
9. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, inspeção de tráfego SSL, prevenção de ameaças, identificação de usuários e controle granular de permissões;
10. 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;
11. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;
12. O hardware e software que executem as funcionalidades de proteção de rede, bem como a console de gerência e monitoração, devem ser do tipo *appliance*. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;
13. Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19", incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;
14. O software deverá ser fornecido em sua versão mais atualizada;
15. Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:
    a. Suporte a 1024 VLAN Tags 802.1q;
    b. Agregação de links 802.3ad e LACP;
    c. *Policy based routing* ou *policy based forwarding*;
    d. Roteamento multicast (PIM-SM);
    e. DHCP Relay;
    f. DHCP Server;
    g. Jumbo Frames;
    h. Suporte a criação de objetos de rede que possam ser utilizados como endereço IP de interfaces L3;
16. Suportar sub-interfaces ethernet lógicas;
17. O firewall deve ter a capacidade de testar o funcionamento de rotas estáticas e rota default com a definição de um endereço IP de destino que deve estar comunicável através de uma rota ou o endereço do *gateway* da rota. Caso haja falha na comunicação o firewall deve ter a capacidade de usar rota alternativa para estabelecer a comunicação;
18. Deve suportar os seguintes tipos de NAT:
    a. Nat dinâmico (Many-to-1);
    b. Nat dinâmico (Many-to-Many);
    c. Nat estático (1-to-1);
    d. NAT estático (Many-to-Many);
    e. Nat estático bidirecional 1-to-1;
    f. Tradução de porta (PAT);
    g. NAT de Origem;
    h. NAT de Destino;
    i. Suportar NAT de Origem e NAT de Destino simultaneamente;
    j. Deve possuir tecnologia capaz de prevenir problemas de roteamento assimétrico;
    k. Deve implementar o protocolo ECMP;
    l. Deve implementar balanceamento de link por hash do IP de origem ou do IP de origem;
    m. Deve implementar balanceamento de link por hash do IP de origem e destino ou do IP de origem e de destino;
    n. Deve implementar balanceamento de link através do método round-robin;
    o. 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. Deve suportar o balanceamento de, no mínimo, dois links;
    p. Deve implementar balanceamento de link através de políticas por usuário e grupos de usuários do LDAP/AD;
    q. Deve implementar balanceamento de link através de políticas por aplicação e porta de destino;
    r. Enviar log para sistemas de monitoração externos, simultaneamente;
    s. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;
    t. Deve permitir configurar certificado caso necessário para autenticação no sistema de monitoração externo de logs;
    u. Proteção contra anti-spoofing;
    v. Deve permitir bloquear sessões TCP que usarem variações do 3-way hand-shake, prevenindo desta forma possíveis tráfegos maliciosos;
    w. Deve permitir bloquear conexões que contenham dados no payload de pacotes TCP-SYN e SYN-ACK, de acordo com a RFC 793;
    x. Deve exibir nos logs de tráfego o motivo para o término da sessão no firewall, incluindo sessões finalizadas onde houver de-criptografia de SSL;
    y. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);

z. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);

aa. Suportar a OSPF graceful restart;

ab. Deve suportar o protocolo MP-BGP (Multiprotocol BGP);

ac. Deve suportar IPv6 para as funcionalidades de Firewall, Controle de Aplicação e IPS;

19. 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);
    a. Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
    b. Modo Camada 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;
    c. Modo Camada 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas;
    d. Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;
20. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo:
    a. Em modo transparente;
    b. Em layer 3;
    c. A configuração em alta disponibilidade deve sincronizar:
        i. Sessões;
        ii. Configurações, incluindo, mas não limitado a políticas de Firewall, NAT, QOS e objetos de rede;
        iii. Certificados de-criptografados;
        iv. Associações de Segurança das VPNs;
        v. Tabelas FIB;
        vi. O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link.
21. As funcionalidades de controle de aplicações, VPN IPSec e SSL, QOS, SSL Decryption e protocolos de roteamento dinâmico 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.

CONTROLE POR POLÍTICA DE FIREWALL

22. Deverá suportar controles por zona de segurança;
23. Controles de políticas por porta e protocolo;
24. Controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;
25. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;
26. Deve suportar a consulta a fontes externas de endereços IP, domínios e URLs podendo ser adicionados nas políticas de firewall para bloqueio ou permissão do tráfego.
    a. Deve permitir autenticação segura através de certificado nas fontes externas de endereços IP, domínios e URLs;
    b. Deve permitir consultar e criar exceção para objetos das listas externas a partir da interface de gerência do próprio firewall;
27. Controle de políticas por código de País (Por exemplo: BR, USA, UK, RUS);
28. Controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e Saída (Outbound);
29. Deve suportar offload de certificado em inspeção de conexões SSL de entrada (Inbound);
30. Deve de-criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.2, ou superior;
31. Deve de-criptografar sites e aplicações que utilizam certificados ECC, incluindo Elliptical Curve Digital Signature Algorithm (ECDSA);
32. Controle de inspeção e de-criptografia de SSH por política;
33. A plataforma de segurança deve implementar espelhamento de tráfego de-criptografado (SSL e TLS) para soluções externas de análise (Forense de rede, DLP, Análise de Ameaças, entre outras);
    a. É permitido uso de appliance externo, específico para a de-criptografia de (SSL e TLS), com espelhamento de cópia do tráfego de-criptografado tanto para o firewall, quanto para as soluções de análise.
34. Bloqueios dos seguintes tipos de arquivos: bat, cab, dll, exe, pif, e reg;
35. Traffic shaping QoS baseado em Políticas (Prioridade, Garantia e Máximo);
36. QoS baseado em políticas para marcação de pacotes (diffserv marking), inclusive por aplicações;
37. Suporte a objetos e regras IPV6;
38. Suporte a objetos e regras multicast;
39. Deve suportar, no mínimo, três tipos de ações de tráfego nas políticas de firewall: Drop sem notificação do bloqueio ao usuário, Drop com opção de envio de mensagem para máquina de origem do tráfego e aceitar o tráfego;
40. Suportar a atribuição de agendamento às políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;

CONTROLE DE APLICAÇÕES

41. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:
    a. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;
    b. Reconhecer pelo menos 1700 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;

c. 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, onedrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs, etc;

d. Deve inspecionar o payload de pacote de dados com o objetivo de detectar através de expressões regulares assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo. A checagem de assinaturas também deve determinar se uma aplicação está utilizando a porta default ou não, incluindo, mas não limitado a RDP na porta 80 ao invés de 389;

e. Deve aplicar heurística a fim de detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a Encrypted Bittorrent e aplicações VOIP que utilizam criptografia proprietária;

f. 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 ataques mediante a porta 443;

g. 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;

h. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado a Yahoo Instant Messenger usando HTTP. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação, incluindo, mas não limitado a compartilhamento de arquivo dentro do Webex. Além de detectar arquivos e outros conteúdos que devem ser inspecionados de acordo as regras de segurança implementadas;

i. Deve permitir a utilização de aplicativos para um determinado grupo de usuário e bloquear para o restante, incluindo, mas não limitado a Skype. Deve permitir também a criação de políticas de exceção concedendo o acesso a aplicativos como Skype apenas para alguns usuários;

j. Identificar o uso de táticas evasivas via comunicações criptografadas;

k. Atualizar a base de assinaturas de aplicações automaticamente;

l. Reconhecer aplicações em IPv6;

m. Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos do LDAP/AD;

n. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;

o. Deve ser possível adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;

p. Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos e análise heurística;

q. Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;

r. Permitir a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do órgão;

s. 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;

t. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;

u. Deve alertar o usuário quando uma aplicação for bloqueada;

v. Deve possibilitar que o controle de portas seja aplicado para todas as aplicações;

w. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc.) possuindo granularidade de controle/políticas;

x. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Gtalk, Facebook Chat, etc.) possuindo granularidade de controle/políticas;

y. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Gtalk chat e bloquear a transferência de arquivos;

z. Deve possibilitar a diferenciação de aplicações Proxies (freegate, etc.) possuindo granularidade de controle/políticas;

aa. Deve ser possível a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como:

i. Tecnologia utilizada nas aplicações (Client-Server, Browser Based, Network Protocol, etc);

ii. Nível de risco da aplicação;

iii. Categoria e subcategoria de aplicações;

iv. Aplicações que usem técnicas evasivas, utilizadas por malwares, como transferência de arquivos e/ou uso excessivo de banda, etc.

IDENTIFICAÇÃO DE USUÁRIOS

42. 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;

43. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

44. Deve possuir integração com Radius para identificação de usuários e grupos, permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

45. Deve possuir integração com Ldap para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;

46. 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);

47. Suporte a autenticação Kerberos;

48. Deve suportar autenticação via Kerberos para administradores da plataforma de segurança, Captive Portal e usuário de VPN SSL;

49. 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;
50. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;
51. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em servidores acessados remotamente, mesmo que não sejam servidores Windows.

QOS

52. 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;
53. Suportar a criação de políticas de QoS por:
    a. Endereço de origem;
    b. Endereço de destino;
    c. Por usuário e grupo do LDAP/AD;
    d. Por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube;
    e. Por porta.
54. O QoS deve possibilitar a definição de classes por:
    a. Banda Garantida;
    b. Banda Máxima;
    c. Fila de Prioridade.
55. Suportar priorização RealTime de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype;
56. Suportar marcação de pacotes Diffserv, inclusive por aplicação;
57. Deve implementar QOS (traffic-shaping), para pacotes marcados por outros ativos na rede (DSCP). A priorização e limitação do tráfego deve ser efetuada nos dois sentidos da conexão (inbound e outbound);
58. Disponibilizar estatísticas RealTime para classes de QoS;
59. Deve suportar QOS (traffic-shaping), em interface agregadas;
60. Deverá permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário.

FILTRO DE DADOS

61. Permitir a criação de filtros para arquivos e dados pré-definidos;
62. Os arquivos devem ser identificados por extensão e assinaturas;
63. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (P2P, InstantMessaging, SMB, etc);
64. Suportar identificação de arquivos compactados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
65. 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;
66. Permitir listar o número de aplicações suportadas para controle de dados;
67. Permitir listar o número de tipos de arquivos suportados para controle de dados;

GEOLOCALIZAÇÃO

68. Suportar a criação de políticas por geolocalização, permitindo que o tráfego de determinado País/Países seja bloqueado;
69. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;
70. Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas.

VPN

71. Suportar VPN Site-to-Site e Client-To-Site;
72. Suportar IPSec VPN;
73. Suportar SSL VPN;
74. A VPN IPSEc deve suportar:
    a. 3DES;
    b. Autenticação MD5 e SHA-1;
    c. Diffie-Hellman Group 1 , Group 2, Group 5 e Group 14;
    d. Algoritmo Internet Key Exchange (IKEv1 e v2);
    e. Pelo menos AES 128 e 256 (Advanced Encryption Standard)
    f. Autenticação via certificado IKE PKI.
75. Deve possuir interoperabilidade com, pelo menos, os seguintes fabricantes:
    a. Cisco;
    b. Checkpoint;
    c. Juniper;
    d. Palo Alto Networks;
    e. Fortinet;

f. Sonic Wall;

76. Deve permitir habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPSEc a partir da interface gráfica da solução, facilitando o processo de troubleshooting;
77. A VPN SSL deve suportar:
    a. O usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;
    b. As funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;
    c. Atribuição de endereço IP nos clientes remotos de VPN SSL;
    d. Deve permitir a atribuição de IPs fixos nos usuários remotos de VPN SSL;
    e. Deve permitir a criação de rotas de acesso e faixas de endereços IP atribuídas a clientes remotos de VPN de forma customizada por usuário AD/LDAP e grupo de usuário AD/LDAP, ou fazer o controle dos usuários e grupos por meio de políticas de acesso;
    f. 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;
    g. Atribuição de DNS nos clientes remotos de VPN;
    h. Deve permitir que seja utilizado mais de um método de autenticação para conexão de VPN;
    i. A solução de VPN deve verificar se o cliente que está conectando é o mesmo para o qual o certificado foi emitido inicialmente. O acesso deve ser bloqueado caso o dispositivo ou o usuário não seja o correto;
    j. Deve possuir lista de bloqueio para dispositivos que forem reportados como roubado/perdido pelo usuário ou opção para apagar o conteúdo do dispositivo roubado/perdido;
    k. Deve exibir mensagens de notificação customizada toda vez que um usuário remoto se conectar a VPN;
    l. Deve permitir criar políticas de controle de aplicações, IPS/Antivírus/Antispyware e filtro de URL (se licenciado para estas funcionalidades) para tráfego dos clientes remotos conectados na VPN SSL;
    m. A VPN SSL deve suportar proxy arp e uso de interfaces PPPOE ou L2TP;
    n. Suportar autenticação via AD/LDAP, OTP (One Time Password), certificado e base de usuários local;
    o. Permitir estabelecer um túnel VPN client-to-site do cliente à plataforma de segurança, fornecendo uma solução de single-sign-on aos usuários, integrando-se com as ferramentas de Windows-logon;
    p. Suportar leitura e verificação de CRL (certificate revocation list);
    q. Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;
    r. O agente de VPN a ser instalado nos equipamentos desktop e laptops deve ser capaz de ser distribuído de maneira automática via Microsoft SMS e Active Directory;
    s. O agente deverá comunicar-se com o portal para determinar as políticas de segurança do usuário;
    t. Deve manter uma conexão segura com o portal durante a sessão;
    u. O agente de VPN SSL client-to-site deve ser compatível com pelo menos Windows 7, Windows 10 e Mac OSx;
    v. Deve possuir a capacidade de identificar se a origem da conexão de VPN é externa ou interna.

PREVENÇÃO DE AMEAÇAS CONHECIDAS

78. 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 ou entregue através de composição com outro equipamento, contanto que todos os equipamentos da composição sejam do mesmo fabricante, possuam gerência unificada e a comunicação entre eles seja realizada através de portas out-of-band;
79. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);
80. 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;
81. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;
82. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS e Antispyware: permitir, permitir e gerar log, bloquear, bloquear IP do atacante por um intervalo de tempo;
83. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;
84. Exceções por IP de origem ou de destino devem ser possíveis nas regras, de forma geral e assinatura a assinatura;
85. Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;
86. Deve permitir o bloqueio de vulnerabilidades;
87. Deve permitir o bloqueio de exploits conhecidos;
88. Deve incluir proteção contra ataques de negação de serviços;
89. Deve suportar a inspeção e criação de regras de proteção de DOS e QOS para o conteúdo de tráfego tunelados pelo protocolo GRE;
90. 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. Análise heurística;
    e. IP Defragmentation;
    f. Remontagem de pacotes de TCP;
    g. Bloqueio de pacotes malformados.
91. Ser imune e capaz de impedir ataques básicos como: Synflood, ICMPflood, UDPflood, etc;

92. Detectar e bloquear a origem de portscans com possibilidade de criar exceções para endereços IPs de ferramentas de monitoramento da organização;
93. Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões;
94. Suportar os seguintes mecanismos de inspeção contra ameaças de rede: análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, análise heurística, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados;
95. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;
96. Possuir assinaturas para bloqueio de ataques de buffer overflow;
97. Deverá possibilitar a criação de assinaturas customizadas;
98. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
99. É permitido uso de appliance externo (antivírus de rede), para o bloqueio de vírus e spywares em protocolo SMB de forma a conter malwares se espalhando horizontalmente pela rede;
100. Suportar bloqueio de arquivos por tipo;
101. Identificar e bloquear comunicação com botnets;
102. Deve suportar várias técnicas de prevenção;
103. Deve suportar referência cruzada com CVE;
104. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:
    a. O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo.
105. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS e Antispyware;
106. Deve permitir que na captura de pacotes por assinaturas de IPS e Antispyware seja definido o número de pacotes a serem capturados;
107. Deve possuir a função resolução de endereços via DNS, para que conexões com destino a domínios maliciosos sejam resolvidas pelo Firewall com endereços previamente definidos;
108. Os eventos devem identificar o país de onde partiu a ameaça;
109. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;
110. Proteção contra downloads involuntários usando HTTP de arquivos executáveis maliciosos;
111. Rastreamento de vírus em pdf;
112. Deve permitir a inspeção em arquivos comprimidos que utilizam o algoritmo deflate (zip, gzip, etc.);
113. 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 diferentes de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.

ANÁLISE DE MALWARES MODERNOS

114. Devido aos Malwares hoje em dia serem muito dinâmicos e um antivírus comum reativo não ser capaz de detectá-los com a mesma velocidade que suas variações são criadas, a solução ofertada deve possuir funcionalidades para análise de Malwares não conhecidos incluídas na própria ferramenta ou entregue com composição com outro fabricante;
115. O dispositivo de proteção deve ser capaz de enviar arquivos trafegados de forma automática para análise "In Cloud" ou local, onde o arquivo será executado e simulado em ambiente controlado;
116. Selecionar através de políticas granulares quais tipos de arquivos sofrerão esta análise incluindo, mas não limitado a: endereço IP de origem/destino, usuário/grupo do AD/LDAP, aplicação, porta, URL/categoria de URL de destino, tipo de arquivo e todas estas opções simultaneamente;
117. Deve possuir a capacidade de diferenciar arquivos analisados, pelo menos, nas seguintes categorias: malicioso e não malicioso;
118. Suportar a análise de comportamentos maliciosos para ameaças não conhecidas;
119. Suportar a análise de arquivos maliciosos em ambiente controlado contemplando, no mínimo, os seguintes sistemas operacionais: Windows 7 e Windows 10;
120. Deve suportar a monitoração de arquivos trafegados na internet (HTTPS, FTP, HTTP, SMTP) como também arquivos trafegados internamente entre servidores de arquivos usando SMB em todos os modos de implementação: sniffer, transparente e L3;
121. A solução deve possuir a capacidade de analisar em sand-box links (HTTP e HTTPS) presentes no corpo de e-mails trafegados em SMTP e/ou POP3. Deve ser gerado um relatório caso a abertura do link pela sand-box o identifique como site hospedeiro de exploits ou possibilitar a identificação de usuários que clicaram no link;
122. A análise de links em sand-box deve ser capaz de classificar sites falsos na categoria de phishing;
123. Para ameaças trafegadas em protocolo SMTP e/ou POP3, a solução deve ter a capacidade de mostrar nos relatórios o remetente, destinatário e assunto dos e-mails permitindo identificação ágil do usuário vítima do ataque;
124. O sistema de análise “In Cloud” ou local deve prover informações sobre as ações do Malware na máquina infectada, informações sobre quais aplicações são utilizadas para causar/propagar a infecção, detectar aplicações não confiáveis utilizadas pelo Malware, gerar assinaturas de Antivírus e Anti-spyware automaticamente;
125. Deve permitir exportar o resultado das análises de malwares de dia Zero em PDF a partir da própria interface de gerência;
126. Deve permitir o download dos malwares identificados a partir da própria interface de gerência;
127. Deve permitir visualizar o resultado das análises de malwares de dia zero nos diferentes sistemas operacionais suportados;
128. Deve permitir informar ao fabricante quanto a suspeita de ocorrências de falso-positivo e falso-negativo na análise de malwares de dia Zero a partir da própria interface de gerência;
129. Caso a solução seja fornecida em appliance local, deve possuir ambientes controlados (sand-box) independentes para execução simultânea de arquivos suspeitos para, pelo menos, os seguintes sistemas operacionais: Windows 7 e Windows 10;
130. Caso seja necessário licenças de sistemas operacional e softwares para execução de arquivos no ambiente controlado (sand-box), as mesmas devem ser fornecidas em sua totalidade, sem custos adicionais para a CONTRATANTE;

131. Suportar a análise de arquivos executáveis, DLLs, ZIP e criptografados em SSL no ambiente controlado;

132. Suportar a inspeção de, no mínimo, 60 dos seguintes tipos de arquivo: ACE, ACM, APK, APP, ARJ, AX, AXF, BAT, BIN, BUNDLE, BZ2, CAB, CLASS, CMD, COM, CPL, CSV, DLL, DMG, DOC, DOCX, DOCM, DOT, DOTM, DOTX, DRV, DYLIB, EFI, ELF, EML, EXE, FLA, FLV, GZ, HTM, HTML, HWP, IQY, ISO, JAR, JS, KGB, KO, LNK, LZH, Mach-O, MOD, MSI, MSG, MUI, O, OCX, PDF, PIF, POT, POTM, POTX, PPAM, PKG, PPS, PPSM, PPSX, POTX, POTM, PPT, PPTM, PPTX, PRX, PS1, PUB, PUFF, RAR, RTF, SCR, SH, SLDM, SLDX, SLK, SO, SWC, SWF, SWT, SYS, TAR, TB2, TBZ, TBZ2, TGZ, TSP, UPX, UUE, VBS, WSF, XLA, XLAM, XLL, XLW, XLS, XLSB, XLSX, XLT, XLM, XLTX, XLSM, XLTM, XPS, XZ, Z, 7Z e ZIP;

133. Deve atualizar a base de assinaturas para bloqueio dos malwares identificados em sand-box por até 24hs ou possibilidade de criação de assinaturas dinâmicas para distribuição local entre o sandbox e o Next Generation Firewall;

134. Permitir o envio de arquivos e links para análise no ambiente controlado de forma automática via API;

135. Deve permitir o envio para análise em sand-box de malwares bloqueados pelo antivírus da solução.

FILTRO DE URL

136. A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:
    a. Permitir especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
    b. Possibilitar a criação de políticas por Usuários, Grupos de Usuários, IP's, Redes e Zonas de segurança;
    c. Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via ldap, Active Directory, E-directory e base de dados local;
    d. Permitir popular todos os logs de URL com as informações dos usuários conforme descrito na integração com serviços de diretório.

137. Suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;

138. Suportar base ou cache de URLs local no appliance, evitando delay de comunicação/validação das URLs;

139. Possuir pelo menos 60 categorias de URLs;

140. A categorização de URL deve analisar toda a URL e não somente até o nível de diretório;

141. Deve suportar a criação de categorias de URLs customizadas;

142. Deve suportar a exclusão de URLs do bloqueio, por categoria;

143. Permitir a customização de página de bloqueio;

144. Deve proteger contra o roubo de credenciais, usuários e senhas;

145. Deve permitir bloquear o acesso do usuário em sites classificados como phishing pelo filtro de URL da solução;

146. Permite 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);

147. Permitir que as atividades dos usuários possam ser registradas nos logs do produto;

148. Deve salvar nos logs as informações dos seguintes campos do cabeçalho HTTP nos acessos a URLs: UserAgent e Referer.

SUPORTE E GARANTIA PARA A SOLUÇÃO DE SEGURANÇA DA INFORMAÇÃO DESCRITA NESTA ESPECIFICAÇÃO TÉCNICA

149. Deve possuir garantia do fabricante no Brasil com validade de 36 (trinta e seis) meses;

150. Durante o prazo de garantia, deve ser possível realizar a atualização de sistema operacional dos equipamentos para obter novas funcionalidades e correção de bugs;

151. A garantia deve incluir envio de peças ou equipamentos de reposição nos locais especificados neste edital, obedecendo a modalidade NBD (Next Business Day);

152. Os chamados poderão ser abertos diretamente com a CONTRATADA ou autorizada oficial do fabricante através de ligação telefônica gratuita (0800) no idioma Português, website e e-mail durante a vigência da garantia (36 meses). O suporte deverá ser na modalidade de 24x7 (24 horas por dia, 7 dias por semana);

153. A licitante deverá possuir suporte local em Teresina/PI para atendimento de chamados emergenciais, de severidades Crítica e Alta. Para o atendimento presencial será aceito SUBCONTRATADA, desde que atenda os prazos e requisitos definidos em item posterior;

154. Deverá ser apresentado, até a assinatura do contrato, uma declaração de que possui suporte local em Teresina/PI no idioma português brasileiro. Para fins de prestação de suporte, será exigida da efetiva prestadora que apresente documentação que comprove ter em seus quadros, pelo menos 01 (um) profissional que seja certificado na solução ofertada;

155. Em qualquer das hipóteses, o responsável direto pela prestação da garantia é a empresa CONTRATADA, que assumirá os ônus de qualquer defeito na prestação deste serviço, direta ou indiretamente;

156. O suporte deverá ter no mínimo o seguinte tempo de resposta para os níveis de severidade abaixo:
    a. Crítico: Significa que o produto ficou inoperante ou ocorreu falha de grande impacto. Para este nível de severidade o atendimento deve ser imediato e com tempo de resposta de até 2 (duas) horas para resolução total ou encontro de solução temporária de contorno. Deve ter visita presencial para resolução ou apoio;
    b. Alta: Impacto moderado no sistema, travamento, ou parada de ambiente parcial. Para este nível de severidade o tempo de resposta deve ser de até 3 (três) horas, em horário comercial, para resolução total ou encontro de solução temporária de contorno. Deve ter visita presencial para resolução ou apoio;
    c. Média: Redução de performance do equipamento ou aplicação de solução temporária de contorno bem-sucedida. Para este nível de severidade o tempo de resposta deve ser de até 4 (quatro) horas, em horário comercial, para resolução total ou encontro de solução temporária de contorno;
    d. Baixa: Dúvidas de configuração ou anomalia de baixo impacto. Para este nível de severidade o tempo de resposta deve ser de até 8 (oito) horas em horário comercial.

DA MIGRAÇÃO, INSTALAÇÃO E CONFIGURAÇÃO DA SOLUÇÃO

157. A CONTRATADA será responsável pela instalação física e configuração dos equipamentos adquiridos:

a. A instalação compreende, entre outros, a desembalagem, a montagem de todos os componentes que integram a especificação, a instalação dos equipamentos montados em rack padrão 19", conforme o caso, a energização do equipamento (não contempla a infraestrutura de energia elétrica, circuitos, tomadas, etc);

b. A configuração compreende, entre outros, os seguintes procedimentos e requisitos:

i. A realização dos ajustes de hardware e software necessários ao funcionamento da solução. Quando aplicável, considerar instalação em modo Alta Disponibilidade (ativo/passivo);

ii. Reunião de alinhamento para criação do escopo do projeto previamente a instalação;

iii. Análise da topologia e arquitetura da rede, considerando todos equipamentos já existentes e instalados;

iv. Análise do acesso à Internet, sites remotos, serviços de rede oferecidos aos funcionários e aos usuários externos;

v. Migração das regras e configurações de firewall existentes na solução atualmente em produção no TJ-PI e aplicáveis à solução ofertada, considerando a adequação às políticas de aplicações em camada 7;

vi. Análise do posicionamento de qualquer outro equipamento ou sistema relevante na segurança de qualquer perímetro protegido pela solução;

vii. Configuração do sistema de firewall, VPN, IPS, Filtro URL, Anti-vírus e Anti-malware de acordo com as exigências levantadas;

viii. Toda configuração do sistema deverá ser realizada de acordo com as melhores práticas recomendadas pelo fabricante da solução ofertada.

ix. A CONTRATADA deverá disponibilizar ferramenta gratuita para acompanhamento da evolução da parametrização de proteção dos firewalls a fim de garantir a melhor eficiência da solução contratada durante o período de vigência das licenças;

x. Configuração do sistema de gerenciamento centralizado considerando adição dos novos appliances;

xi. Deve haver geração de relatório com as configurações efetuadas e as decisões tomadas em formato legível e tecnicamente fundamentado;

xii. Todas as atualizações de firmware ou qualquer outro software componente da solução, para a versão mais atualizada disponível ou a última compatível com as demais soluções deste lote e considerada estável;

xiii. Habilitação de licenças que porventura sejam adquiridas e recursos do equipamento que serão utilizados no projeto;

xiv. As verificações dos recursos e o seu perfeito funcionamento e integração com os demais, conforme as melhores práticas indicadas pelo fabricante;

158. A CONTRATADA deverá fazer o repasse de conhecimento à equipe técnica da CONTRATANTE compreendendo:

a. Repasse da tecnologia, demonstrando no ambiente instalado os recursos habilitados e configurações realizadas para o funcionamento do(s) equipamento(s), explicitando a forma de utilização do equipamento e de seus recursos;

b. A carga horária mínima do repasse de tecnologia é de 4 horas;

159. Os serviços deverão ser realizados por pessoal técnico experiente e certificado pelo fabricante dos equipamentos. Em momento anterior à instalação, a CONTRATANTE poderá solicitar os comprovantes da qualificação profissional do(s) técnico(s) que executará(ão) os serviços, sendo direito da mesma a sua aceitação ou exigência de troca de profissional no caso de este não satisfazer às condições supramencionadas;

160. A CONTRATADA deverá garantir a confidencialidade das informações, dados e senhas compartilhadas pela CONTRATANTE;

161. Durante as atividades realizadas na prestação do serviço, o técnico da CONTRATADA deverá demonstrar à equipe técnica de acompanhamento da CONTRATANTE como instalar e configurar os equipamentos e os softwares fornecidos (instalação assistida);

162. As atividades deverão ser realizadas dentro do horário comercial (de segunda à sexta-feira de 08h às 18h);

163. A realização dos serviços deve ser planejada de acordo com a disponibilidade de ambas as partes. O planejamento anterior ao serviço pode ser realizado remotamente através de webconferência ou videoconferência;

164. O planejamento dos serviços de configuração deve resultar num documento tipo SOW (em tradução livre, escopo de trabalho). Neste documento devem estar contidos a relação, descrição e quantidades dos produtos fornecidos, descrição da infraestrutura atual e desejada, detalhamento dos serviços que serão executados, premissas do projeto, locais e horários de execução dos serviços, condições de execução dos serviços, pontos de contato da CONTRATANTE e CONTRATADA, cronograma de execução do projeto em etapas, com responsáveis, data de início e fim (se aplicável), relação da documentação a ser entregue ao final da execução dos serviços, responsabilidade da CONTRATANTE e CONTRATADA, plano de gerenciamento de mudanças, itens excluídos no projeto e termo de aceite. Os serviços não poderão ser iniciados antes da apresentação e assinatura de concordância por ambas as partes;

165. Todos os parâmetros a serem configurados deverão ser alinhados entre as partes em reuniões de pré-projeto, devendo a CONTRATADA sugerir as configurações de acordo com normas técnicas e boas práticas, cabendo à CONTRATANTE a sua aceitação expressa ou recusa nos casos de não atendimento das condições estabelecidas;

166. Ao término dos serviços deve ser criado um relatório detalhado contendo todos os itens configurados no projeto (relatório as-built), etapas de execução e toda informação pertinente para posterior continuidade e manutenção da solução instalada, como usuários e endereços de acesso, configurações realizadas e o resumo das configurações dos equipamentos. Este relatório deve ser enviado com todas as informações em até 15 dias após a finalização dos serviços;

167. A implantação deverá abranger a configuração de quaisquer funcionalidades suportadas pelo equipamento. Estas informações serão documentadas no termo de abertura do projeto a ser documentado pela CONTRATADA após alinhamento do escopo de trabalho entre CONTRATADA e CONTRATANTE;

168. Todo o processo de instalação e configuração realizado deverá ser documentado pela CONTRATADA sob a forma de relatório.

169. Dos prazos:

a. A CONTRATADA deverá seguir o seguinte cronograma mínimo para o serviço de Instalação, migração e configuração da solução:

i. Reuniões de planejamento (podem ser realizadas à distância): 4 horas;

ii. Reunião de planejamento da Instalação da solução (presencial): 4 horas;

iii. Instalação: 4 horas;

iv. Configuração e migração: 8 horas;

v. Implementação e validação do ambiente: 8 horas

vi. Repasse de conhecimento: 4 horas.

170. Mais detalhes e informações estão definidos no item 4. deste Termo de Referência.

ITEM 2 - SOLUÇÃO DE GESTÃO CENTRALIZADA DE FIREWALL COM SUPORTE/GARANTIA DE 3 ANOS

1. Deve possuir solução de gerenciamento centralizado, possibilitando o gerenciamento de diversos equipamentos;
2. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança;
3. Controle sobre todos os equipamentos da plataforma de segurança em uma única console, com administração de privilégios e funções;
4. O gerenciamento centralizado poderá ser entregue como appliance físico ou virtual. Caso seja entregue em appliance físico deve ser compatível com rack 19 polegadas e possuir todos os acessórios necessários para sua instalação. Caso seja entregue em appliance virtual deve ser compatível com VMware ESXi 6.0 ou superior;
5. Deve permitir controle global de políticas para todos os equipamentos que compõe a plataforma de segurança;
6. Deve suportar organizar os dispositivos administrados em grupos: os sistemas virtuais devem ser administrados como dispositivos individuais, os grupos podem ser geográficos, por funcionalidade (por exemplo, IPS), e distribuição;
7. Deve implementar sistema de hierarquia entre os firewalls gerenciados, onde seja possível aplicar configurações de forma granular em grupos de firewalls;
8. Deve implementar a criação de perfis de usuários com acesso a plataforma de gerenciamento com definição exata de quais informações e de quais firewalls e grupos de firewalls o usuário terá acesso referente a logs e relatórios;
9. Deve permitir a criação de objetos e políticas compartilhadas;
10. Deve consolidar logs e relatórios de todos os dispositivos administrados;
11. Deve permitir exportar backup de configuração automaticamente via agendamento;
12. Deve permitir que a configuração dos firewalls seja importada de forma automática na plataforma de gerenciamento centralizado e que possa ser usada em outros firewalls e grupos de firewalls;
13. Deve mostrar os status dos firewalls em alta disponibilidade a partir da plataforma de gerenciamento centralizado;
14. Centralizar a administração de regras e políticas do cluster, usando uma única interface de gerenciamento;
15. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;
16. Deve permitir substituir o certificado de fábrica no acesso HTTPS a gerência do firewall como possibilidade de uso de certificado criado localmente na própria solução ou importado de fonte externa;
17. Caso haja a necessidade de instalação de cliente para administração da solução o mesmo deve ser compatível com sistemas operacionais Windows e/ou Linux;
18. O gerenciamento deve permitir/possuir:
    a. Criação e administração de políticas de firewall e controle de aplicação;
    b. Criação e administração de políticas de IPS/Antivírus/Anti-Spyware; (se licenciado para esta funcionalidade);
    c. Criação e administração de políticas de Filtro de URL (se licenciado para esta funcionalidade);
    d. Monitoração de logs;
    e. Ferramentas de investigação de logs;
    f. Debugging;
    g. Captura de pacotes;
    h. Acesso concorrente de administradores.
19. Deve permitir que administradores concorrentes façam modificações, validem configurações e revertam configurações do firewall simultaneamente e que cada administrador consiga aplicar as suas alterações de forma independente das realizadas por outro administrador;
20. Deve mostrar ao administrador do firewall a hora e data do último login e tentativas de login com falha para acessos a partir da interface gráfica e CLI.
21. A solução deve possuir mecanismo de busca global onde seja possível realizar consulta por strings tais como: nome de objetos, ID ou nome de ameaças, nome de aplicações, nome de políticas, endereços IPs, permitindo a localização e uso dos mesmos na configuração do dispositivo;
22. Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;
23. Deve permitir usar palavras chaves e cores ou permitir agrupar regras, de modo a facilitar a identificação destas;
24. Deve permitir monitorar falhas de hardware, inserção ou remoção de fontes, discos e coolers, uso de recursos por número elevado de sessões, número de túneis estabelecidos na VPN client-to-site, porcentagem de utilização em referência ao número total suportado/licenciado e número de sessões estabelecidas, estatísticas/taxa de logs, uso de disco, período de retenção dos logs e status do envio de logs para soluções externas;
25. Deve suportar também o monitoramento dos seguintes recursos via SNMP: IP fragmentation, TCP state e dropped packets;
26. Bloqueio de alterações, no caso de acesso simultâneo de dois ou mais administradores;
27. Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;
28. Autenticação integrada ao Microsoft Active Directory e servidor Radius;
29. Localização das regras onde um endereço IP, IP Range, subnet ou objetos estão sendo utilizados;
30. Deve atribuir sequencialmente um número a cada regra de firewall, NAT, QOS e regras de DOS;
31. Criação de regras que fiquem ativas em horário definido;
32. Criação de regras com data de expiração;
33. Backup das configurações e rollback de configuração para a última configuração salva;
34. Suportar Rollback de Sistema Operacional para a última versão local;
35. Habilidade de upgrade via SCP e interface de gerenciamento;

36. Deve possuir mecanismo de análise de impacto na política de segurança antes de atualizar a base com novas aplicações disponibilizadas pelo fabricante;
37. Validação de regras antes da aplicação;
38. Deve implementar mecanismo de validação de configurações antes da aplicação das mesmas permitindo identificar erros, tais como: rota de destino inválida, regras em shadowing, etc;
    a. É permitido o uso de appliance externo para permitir a validação de regras antes da aplicação.
39. Validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);
    a. É permitido o uso de appliance externo para permitir a validação de políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing).
40. Deve possibilitar a visualização e comparação de configurações atuais, configuração anterior e configurações antigas;
41. Deve possibilitar a integração com outras soluções de SIEM de mercado (third-party SIEM vendors);
42. Geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;
43. Deverá ter a capacidade de gerar um relatório gráfico que permita visualizar as mudanças na utilização de aplicações na rede no que se refere a um período de tempo anterior, para permitir comparar os diferentes consumos realizados pelas aplicações no tempo presente com relação ao passado;
44. Geração de relatórios com mapas geográficos gerados em tempo real para a visualização de origens e destinos do tráfego gerado na instituição;
45. Deve prover relatórios com visão correlacionada de aplicações, ameaças (IPS/Antivírus/Anti-Spyware), URLs (se licenciado para estas funcionalidades) e filtro de arquivos, para melhor diagnóstico e resposta a incidentes;
46. Deve permitir a criação de Dash-Boards customizados para visibilidades do tráfego de aplicativos, usuários, categorias de URL, ameaças identificadas pelo IPS/antivírus/anti-spyware, malwares "Zero Day"detectados em sand-box (se licenciado para estas funcionalidades) e tráfego bloqueado;
47. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos dispositivos de segurança;
48. Deve permitir a visualização dos logs de malwares modernos (se licenciado para esta funcionalidade), tráfego (IP de origem, destino, usuário e porta), aplicação, IPS/antivírus/anti-spyware (se licenciado para esta funcionalidade), Filtro de URL (se licenciado para esta funcionalidade) e filtro de arquivos em uma única tela;
49. Deve possuir relatórios de utilização dos recursos por aplicações, URL, ameaças (IPS/Antivírus/Anti-Spyware) (se licenciado para estas funcionalidades), etc;
50. Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS/Antivírus/Anti-Spyware), e URLs (se licenciado para estas funcionalidades) que passaram pela solução;
51. Deve possuir mecanismo "Drill-Down" para navegação nos relatórios em RealTime;
52. Nas opções de "Drill-Down", ser possível identificar o usuário que fez determinado acesso;
53. Deve possuir relatório de visibilidade e uso sobre aplicativos (SaaS). O relatório também deve mostrar os riscos para a segurança do ambiente, tais como a entrega de malwares através de aplicativos SaaS com a informação do usuário responsável pelo acesso;
54. Os relatórios de visibilidade e uso sobre aplicativos (SaaS) devem poder ser extraídos por grupo de usuários apresentando o uso e consumo de aplicações por grupo de usuário;
55. Deve ser possível exportar os logs em CSV;
56. Deverá ser possível acessar o equipamento e aplicar configurações durante momentos onde o tráfego é muito alto e a CPU e memória do equipamento estiverem totalmente utilizadas;
57. Caso a solução possua licenciamento relacionado a armazenamento, este deve ser entregue com a maior capacidade suportada ou ilimitada sem a necessidade de licenciamento adicional;
58. Caso a solução possua módulo de relatórios estendido, este deve ser entregue junto com a solução sem a necessidade de licenciamento adicional;
59. Deve permitir que os logs e relatórios sejam rotacionados manualmente ou automaticamente baseado no tempo em que estão armazenados na solução, assim como no espaço em disco usado;
60. Deve permitir fazer o envio de logs para soluções externas de forma granular podendo selecionar quais campos dos logs serão enviados incluindo, mas não limitado a: tipo de ameaça, usuário, aplicação, etc;
61. Exibição das seguintes informações, de forma histórica e em tempo real (atualizado de forma automática e contínua a cada 1 minuto):
    a. Situação do dispositivo e do cluster;
    b. Principais aplicações;
    c. Principais aplicações por risco;
    d. Administradores autenticados na gerência da plataforma de segurança;
    e. Número de sessões simultâneas;
    f. Status das interfaces;
    g. Uso de CPU.
62. Geração de relatórios. No mínimo os seguintes relatórios devem ser gerados:
    a. Resumo gráfico de aplicações utilizadas;
    b. Principais aplicações por utilização de largura de banda de entrada e saída;
    c. Principais aplicações por taxa de transferência de bytes;
    d. Principais hosts por número de ameaças identificadas; (se licenciado para esta funcionalidade);
    e. Atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas, categorias de URL, URL/tempo de utilização e ameaças (IPS/Antivírus/Anti-Spyware) (se licenciado para estas funcionalidades) de rede vinculadas a este tráfego;
    f. Deve permitir a criação de relatórios personalizados.
63. Em cada critério de pesquisa do log deve ser possível incluir múltiplas entradas (ex. 10 redes e IP’s distintos; serviços HTTP, HTTPS e SMTP), exceto no campo horário, onde deve ser possível definir um faixa de tempo como critério de pesquisa;
64. Gerar alertas automáticos via:

a. Email;
b. SNMP;
c. Syslog.

65. A plataforma de segurança deve permitir através de API (Application Program Interface) a integração com sistemas existentes no ambiente da CONTRATANTE de forma a possibilitar que aplicações desenvolvidas na CONTRATANTE possam interagir em RealTime com a solução possibilitando assim que regras e políticas de segurança possam ser modificadas por estas aplicações por meio da utilização de scripts de linguagens de programação.
66. A solução de gestão centralizada de firewall deve ser entregue, instalada, configurada e em perfeita integração com o cluster NGFW.

ITEM 3 - TREINAMENTO DE INSTALAÇÃO E ADMINISTRAÇÃO PARA SOLUÇÃO DE FIREWALL DE PRÓXIMA GERAÇÃO PARA UMA TURMA DE 06 PESSOAS

1. O treinamento deverá ser ministrado abrangendo teoria e prática de implantação, configuração, migração, administração e solução de problemas no ambiente deste órgão, bem como assuntos teóricos relacionados;
2. Deve conter no mínimo a seguinte ementa:
   a. Administração e Gerenciamento;
   b. Configuração de Interfaces;
   c. Roteamento;
   d. Regras de camada 7;
   e. IPS, Antivírus e Antispyware;
   f. Sandboxing;
   g. Filtro URL;
   h. Decriptografia;
   i. Integração com base de Usuários;
   j. Alta Disponibilidade;
   k. VPN;
   l. Gerenciamento Centralizado;
   m. Troubleshooting (Solução de Problemas).
3. A carga horária total deverá ser de 40 horas, no mínimo;
4. O treinamento deverá ser ministrado na cidade de TERESINA-PI em instalações fornecidas pela CONTRATANTE;
5. A CONTRATADA fornecerá os materiais didáticos para ministrar o curso;
6. Os eventuais deslocamentos, refeições e estadia do(s) instrutor(es) será(ão) por conta da CONTRATADA;
7. O período de realização do treinamento será fixado pela STIC em conjunto com a CONTRATADA, no prazo máximo de 30 (trinta) dias após o recebimento definitivo da entrega e instalação da solução;
8. O treinamento deverá ser realizado, de segunda a sexta-feira, das 8:00 às 12:00, e das 14:00 às 18:00 ou das 8:00 às 18:00, à critério da STIC, em TERESINA-PI,
9. A CONTRATADA deverá emitir para o servidor participante, sem ônus para o TJPI e no prazo máximo de até 10 (dez) dias úteis após o término do treinamento, o certificado de conclusão, no qual deverá constar o nome do treinando, a data, o local e a carga horária.
10. Todo o material didático para a realização dos treinamentos deverá ser oficial do fabricante da Solução, ser de primeiro uso e atualizados. O material deverá ser em português ou inglês, e as aulas ministradas em língua portuguesa do Brasil.
11. Caso o fabricante/importador não disponibilize treinamento nos moldes supra, deverão ser disponibilizados vouchers ou documentos equivalentes para treinamento em centro oficial do fabricante. As despesas com deslocamento e hospedagem da equipe a ser treinada deverão ser pagas com recursos do TJPI.

ANEXO I

(Infrações, graus, multas e penalidades)

Item	Infração	Grau	Multa
1	Descumprimento de quaisquer outras obrigações contratuais, não explicitadas nos demais itens, que sejam consideradas leves	1	Moratória
2	Não entrega de documentação simples solicitada pelo CONTRATANTE	1	Moratória
3	Atraso parcialmente justificado na entrega até 30 dias.	2	Moratória
4	Atraso parcialmente justificado na entrega acima de 30 dias até 60 dias.	3	Moratória
5	Atraso parcialmente justificado ou injustificado na entrega acima de 60 dias.	4	Compensatória
6	Descumprimento de outros prazos, previstos do TR	2	Moratória
7	Erros de execução do objeto	3	Moratória
8	Desatendimento às solicitações do CONTRATANTE	3	Moratória
9	Descumprimento de quaisquer outras obrigações contratuais, não explicitadas nos demais anteriores, que seriam consideradas médias	3	Moratória

Item	Infração	Grau	Multa
10	Execução imperfeita do objeto	3	Moratória
11	Não manutenção das condições de habilitação e de licitar e contratar com a Administração Pública durante a vigência contratual	4	Compensatória
12	Não entrega de documentação importante solicitada pelo CONTRATANTE	4	Compensatória
13	Descumprimento de quaisquer outras obrigações contratuais, não explicitadas nos demais itens, que seriam consideradas graves	4	Compensatória
14	Inexecução parcial do Contrato	4	Compensatória
15	Descumprimento da legislação (legais e infralegais) afeta à execução do objeto (direta ou indireta)	5	Compensatória
16	Cometimento de atos protelatórios durante a execução visando adiamento dos prazos contratados	5	Compensatória
17	Inexecução total do Contrato	5	Compensatória

Grau	Advertência - 1ª Ocorrência	Mora moratória Valor Mensal	Multa Compensatória	Impedimento Prazo
1	Sim	Não	Não	Não
2	Não	1% a 4,9% por ocorrência ou contrato	1,5% a 4,9% por ocorrência ou contrato	Mínimo: 1 mês Máximo: 2 anos
3	Não	5% a 8,9% por ocorrência ou contrato	8,0% a 14,9% por ocorrência ou contrato	Mínimo: 6 meses Máximo: 3 anos
4	Não	9% a 11,9% por ocorrência ou contrato	15,0% a 24,9% por ocorrência ou contrato	Mínimo: 3 anos Máximo: 5 anos
5	Não	12% a 15% por ocorrência ou contrato	25% a 30% por ocorrência ou contrato	Mínimo: 4 anos Máximo: 5 anos

ANEXO II

MODELO DE PROPOSTA DE PREÇO

Item	Nome	Quantidade	Valor Unitário	Valor Total
1	Cluster de Firewall com licença de Filtro URL e identificação de aplicações, licenças de proteção contra ameaças conhecidas e desconhecidas (Zero-Day) e suporte/garantia 24x7 *on site* de 3 (três) anos	02		
2	Software de gerenciamento centralizado para *cluster* de NGFW com garantia de 3 (três) anos	02		
3	Treinamento para operação de *cluster* de NGFW para 06 (seis) pessoas	02		
Total da Proposta				

Documento assinado eletronicamente por **Fabiano Galeno da Costa Pereira**, **Coordenador de Infraestrutura - STIC**, em 30/01/2020, às 12:39, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Giovanny Lima de Castro**, **Analista de Sistemas / Desenvolvimento**, em 30/01/2020, às 12:39, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Francisco Igor de Lima e Silva**, **Coordenador de Governança de TI**, em 30/01/2020, às 12:42, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Francisco de Assis Ribeiro Madeira Campos Filho**, **Secretário de Tecnologia da Informação de Comunicação - STIC**, em 30/01/2020, às 13:11, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Josué Almeida do Nascimento**, **Servidor TJPI**, em 30/01/2020, às 13:14, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site http://sei.tjpi.jus.br/verificar.php informando o código verificador **1503104** e o código CRC **2305CA4D**.