1. DO OBJETO

Contratação de empresa especializada no fornecimento de soluções de segurança de redes compostas de firewall corporativo e multifuncional para prover segurança e proteção da rede dos órgãos e dos servidores de rede, contemplando gerência unificada com garantia de funcionamento pelo período de **60 (sessenta) meses**, incluídos todos os *softwares* e suas licenças de uso, gerenciamento centralizado, serviços de implantação, garantia de atualização contínua, suporte técnico e repasse de conhecimento de toda a solução a fim de atender às necessidades dos órgãos contratantes.

2. DA JUSTIFICATIVA

2.1 Necessidade do objeto

A informação é um dos principais ativos das organizações e instituições públicas, tratando-se de um elemento fundamental para a tomada de decisões em todos os níveis, sendo determinante para a gestão governamental. Nesse sentido, os gestores precisam promover ações para prover a segurança de tais informações. Os constantes ataques cibernéticos, a necessidade de continuidade do negócio e a evolução de ameaças das mais variadas espécies criam a necessidade de contratação de uma solução que proteja as informações dos órgãos e diminua os riscos de acesso indevido as mesmas.

Inseridos dentro de um contexto muito dinâmico de evolução constante de tecnologia, em um curto intervalo de tempo, os equipamentos destinados à segurança da informação podem se tornar obsoletos a tal ponto de não suportarem o aumento do tráfego de internet e dados, o crescente número de novos usuários e as novas tentativas de invasões nas redes corporativas.

Dentro do contexto analisado, o firewall representa um quesito de segurança fundamental, uma vez que regula o tráfego de dados entre redes distintas e impede a transmissão e recepção de informações a partir de acessos nocivos ou não autorizados na rede.

Partindo-se de tais pressupostos, a contratação consistirá na aquisição de uma solução de segurança integrada que englobe equipamento firewall corporativo e multifuncional. Essa solução podeincluir, dentre outras funcionalidades, alta disponibilidade, anti-malware, anti-spyware, anti-vírus, anti-bot, filtro de conteúdo e filtro de URL, controle de aplicações, inspeção de pacotes, IPS, IDS, relatórios, inspeção SSL, VPNs. QoS, Autenticação de usuários e Anti-DoS de rede . Tais funcionalidades podem ser combinadas para atender as diversas necessidades dos órgãos participantes ou não da contratação compartilhada por meio da ata de registros de preços.

Para essa contratação, dada a complexidade técnica do objeto, optou-se pela criação de um grupo de trabalho com componentes de vários órgãos da administração pública, buscando incorporar múltiplas visões e experiências de contratações sobre objeto contratado.. Previamente aos trabalhos, foi realizado um estudo de inteligência que envolveu a análise das soluções disponíveis no âmbito da Administração Pública Federal (APF) e das soluções no âmbito externo, ofertadas pelo mercado por meio de fabricantes das soluções, permitindo, assim, uma melhor compreensão do cenário atual das soluções de segurança de redes.

Para o levantamento das necessidades e qualificação da demanda, o grupo de trabalho elaborou um questionário e fez uma pesquisa, enviando as perguntas aos órgãos do SISP, que voluntariamente responderam aos esclarecimentos suscitados. Essas perguntas faziam menção

ao cenário presente nos órgãos, às maiores dificuldades nas soluções de segurança, aos pontos fracos e fortes e às possíveis melhorias no setor com a contratação de uma nova solução. De posse das respostas, o grupo de trabalho fez um levantamento dos perfis de acordo com parâmetros relevantes para essa abordagem de segurança de redes, tais como quantidade de banda de internet, usuários, volume de sessões, entre outros. A partir de tais informações, foi realizada uma análise que culminou no agrupamento de soluções e formação de lotes na busca de atender as faixas de necessidades encontradas através da pesquisa junto ao SISP.

Além do já exposto, a contratação da solução de segurança vai além da aquisição de um equipamento. É uma busca por uma solução que melhore a maturidade em segurança de redes dos órgãos envolvidos, aumentando o ganho de escala e permitindo o gerenciamento por equipes menores, uma vez que centraliza a solução de várias funcionalidades numa solução integrada.

2.2 Mecanismo de compras compartilhadas pelo Sistema de Registro de Preços

Por intermédio do Decreto nº 7.892, de 23 de janeiro de 2013, estabeleceu-se o Sistema de Administração de Recursos de Tecnologia da Informação - SISP para a Administração Pública Federal, Autárquica e Fundacional. Atualizado depois pelo Decreto nº 8.250 de 22 de maio de 2014.

A Comissão de Coordenação do SISP, composta pelos gestores de modernização administrativa e de informática dos órgãos e entidades da Administração Pública Federal e pela Secretaria e Tecnologia da Informação – STI do Ministério do Planejamento, Orçamento e Gestão – MP, exerce a função de órgão central, e é responsável por exarar as principais normas e diretrizes para a condução da TI no Governo Federal.

Para fortalecer as políticas governamentais de uso do poder de compra do Estado, a proposição das compras compartilhadas, apresentada neste certame, é liderada pelo Núcleo de Contratações de Tecnologia da Informação – NCTI, integrante do SISP e vinculado à Comissão de Coordenação do SISP, que executa o levantamento das demandas de modernização tecnológica nos órgãos da Administração Pública Federal.

São diversos os argumentos que justificam a adoção do mecanismo de compras compartilhadas, no caso utilizando-se do Sistema de Registro de Preços (SRP), com manifestação prévia de intenção de registro de preços (IRP). É importante destacar, como ganho de eficiência, a redução do esforço administrativo e processual na realização de diversos processos licitatórios, uma vez que a execução conjunta culmina em um único certame. Ou seja, há uma redução do número dos processos de contratação de bens e serviços pela Administração para o mesmos objeto.

Outro ganho significativo é a padronização do parque tecnológico na Administração Pública, proporcionando redução de custos de manutenção e melhor eficiência pelo uso racional dos recursos públicos.

Além da redução do esforço administrativo, destaca-se, em especial, o ganho de economia de escala com as compras compartilhadas, pois, ao concentrar expressivosvolumes licitados, a Administração Pública Federal amplia as possibilidades de conseguir propostas mais vantajosas, em razão do ganho de escala e as possíveis reduções consideráveis dos preços ofertados por fornecedores.

Soma-se às vantagens o fato de o Registro de Preços não obrigar à contratação imediata, sendo as aquisições realizadas somente quando for conveniente e oportuno para os órgãos ou entidades, ou seja, surgir a necessidade em se adquirir os bens e serviços registrados.

Em decorrência, não se tem despesas de armazenamento e é possível atender demandas imprevisíveis, com celeridade, uma vez que o particular fica vinculado ao Registro de Preços durante a vigência da ata de RP.

2.3 Planejamento da contratação

As experiências com as contratações conjuntas de Ativos de Redes levaram a equipe da CGINF/DEIST/STI a gerir o projeto de aquisição compartilhada da solução de segurança de redes. Assim, foi instituído um Grupo de Trabalho Técnico para o projeto, formalizado pela Portaria nº 03 de 21 de janeiro de 2016.

Destarte, de acordo com o que disciplina a Instrução Normativa STI/MP nº 04, de 11 de setembro de 2014, tanto o processo de Planejamento da Contratação como os trâmites de elaboração do Edital do certame, inclusive as especificações técnicas, foram elaborados por representantes do DEIST/STI e da Central de Compras e Contratações - ASEGE/MP, que compõem a equipe de planejamento da contratação – EPC do processo em questão.

Deste feito, o MP ficará responsável pela distribuição e veiculação oficial do instrumento convocatório. Por sua vez, o apoio ao pregoeiro será feito pelo grupo de trabalho, durante a licitação, na prestação dos esclarecimentos e respostas aos questionamento e às impugnações, por ventura interpostos.

2.3 Aderência estratégica do projeto

A Solução de Segurança de Redes atende à Estratégia de Governo Digital (EGD) 2016 - 2019. A EGD 2016 busca aumentar a efetividade da geração de valor público para a sociedade brasileira por meio da melhoria do acesso às informações governamentais, dos serviços públicos digitais e da ampliação da participação social. Assim, a contratação de solução de segurança tem relação direta com a EGD 2016, uma vez que a ampliação da participação social e a prestação de serviços públicos por meios digitais irão gerar um aumento do número de acessos aos sistemas do governo, exigindo assim o estabelecimento de uma solução de segurança mais robusta de forma a resguardar tais informações

Os três eixos da EGD possuem pontos de atenção de segurança. As tecnologias para implantar as estratégias da EGD são baseadas em princípios de segurança da informação no que se refere à confiabilidade, disponibilidade, autenticidade e integridade. O firewall multifuncional corporativo proposto na solução de segurança é uma das mais importantes ferramentas para implantar os requisitos de segurança que requer a EGD nos ambientes dos órgãos e entidades da APF.

Na EGD, a solução de segurança está relacionada aos seguintes indicadores:

a) Proporção de órgãos que compartilham sistemas ou infraestruturas. Tal indicador objetiva reduzir custos e desperdícios e evitar esforços desnecessários e perda de dados e informações.

b) Garantir a disponibilidade, integridade, confidencialidade e autenticidade dos ativos de informação custodiados pelo Estado, bem como a proteção da informação pessoal e da propriedade intelectual.

As iniciativas da EGD envolvidas com a contratação da solução de segurança são:

a) Fomentar parcerias com institutos de pesquisa e desenvolvimento, promovendo a pesquisa aplicada na área de Segurança da Informação e Comunicação.

b) Estabelecer mecanismos mais eficazes para viabilizar a efetiva classificação da informação nos órgãos da APF.

c) Implantar e fortalecer as equipes de tratamento de incidentes de segurança nas redes de computadores do Estado.

d) Desenvolver uma política nacional de Segurança da Informação e Comunicação e de Segurança Cibernética.

3. DOS ITENS E QUANTITATIVOS

3.1 Os itens e quantitativos serão discriminados na Planilha de Quantitativos e Preços Máximos, constante no ANEXO A, após realização da Intenção de Registro de Preços – IRP.

4. DO ENQUADRAMENTO DO OBJETO A SER CONTRATADO

4.1 O objeto a ser contratado enquadra-se na categoria de bens comuns, de que tratam a Lei nº 10.520/02 e o Decreto nº 5.450/05, por possuir padrões de desempenho e características gerais e específicas, , que podem ser definidos de forma objetiva nas especiafações téncnicas, que são usualmente encontradas no mercado, podendo, portanto, ser licitado por meio da modalidade Pregão.

5. DA ADOÇÃO DO SISTEMA DE REGISTRO DE PREÇOS

5.1 O Decreto nº 7.892, de 23 de janeiro de 2013, que disciplina o Sistema de Registro de Preços, define as hipóteses especiais, sobre sua admissão pela Administração Pública.

5.2 Em função das características peculiares dessa contratação, entre as quais se destacam: possibilidade de atendimento a vários órgãos da Administração Pública, por ocasião do mecanismo de compras compartilhadas e necessidade de contratações frequentes, conforme as demandas dos órgãos, optou-se pelo Sistema de Registro de Preços - SRP, conforme Decreto nº 7.892, de 23 de janeiro de 2013**.**

5.3 Será realizado o procedimento daIntenção de Registro de Preços - IRP, para verificação da intenção de participação no Registro de Preços, bem como será permitida a adesão para aquisição máxima de 100% do quantitativo total estimado da contratação, considerado para este limite o somatório dos quantitativos requeridos pelos órgãos não participantes, por meio de adesão.

6. DAS ESPECIFICAÇÕES TÉCNICAS

6.1 Conforme ANEXO “B” deste Termo de Referência.

7 DO PRAZO E DO LOCAL DE ENTREGA

7.1 Os objetos especificados neste Termo de Referência deverão ser entregues pela CONTRATADA nos endereços indicados pela CONTRATANTE na Ordem de Serviço de Entrega - OSE, observados os municípios relacionados na Pauta de Distribuição constante no ANEXO C.

7.2 A CONTRATANTE solicitará a entrega dos equipamentos por meio de Ordem de Serviço de Entrega - OSE, que deverá ser cumprida no prazo máximo de até 60 (sessenta) dias corridos, a partir da sua emissão.

7.2.1 A OSE indicará a quantidade, os endereços de entrega e da instalação e nome do responsável pelo recebimento, acompanhado de e-mail e/ou telefone para contato, além da solicitação de entrega do Projeto Provisório de Instalação - PPI.

7.3 A CONTRATADA deverá informar à CONTRATANTE, quando da entrega dos equipamentos com, no mínimo, 5 (cinco) dias corridos de antecedência, ficando a CONTRATADA responsável pelo transporte e entrega dos equipamentos e partes componentes da solução integrada de segurança da informação. A CONTRATADA será responsável por elaborar e entregar o PPI dos equipamentos em até 10 (dez) dias corridos, contados a partir da solicitação da CONTRATANTE, constante no item 7.2, ou seja, da emissão da OSE.

7.4 Os equipamentos descritos no ANEXO A deverão ser entregues instalados e operacionais em até 15 (quinze) dias corridos, contados a partir da emissão da Ordem de Serviço de Instalação – OSI.

7.4.1 A substituição do equipamento que apresentar divergência na especificação técnica, falhas de componentes, defeitos de fabricação e operação ou qualquer outro defeito apresentado durante o transporte, a entrega e a instalação dos equipamentos deverão ser efetuadas em até 5 (cinco) dias úteis, contados a partir da notificação da ocorrência por parte da CONTRATANTE, observado o disposto neste TR.

7.4.2 A CONTRATADA deverá entregar o Projeto Definitivo de Instalação - PDI ("As Built") em até 2 (dois) dias úteis após a instalação, observadas as condições do item 8.2.6 deste termo de referência.

8 . INSTALAÇÃO DOS FIREWALLS

8.1 Projeto de instalação

8.1.1 No PPI deverá constar a prévia de projeto de instalação, contendo, no mínimo, relação de materiais e serviços que comporão a entrega, croquis e plantas de instalação, topologia física e lógica, detalhamento da configuração do equipamento, relatório de vistoria, planos de migração e ativação e plano de retorno.

8.1.2 Cabe a CONTRATADA verificar durante o planejamento da instalação e vistorias, o padrão da CONTRATANTE quanto à: arquitetura de cabeamento, padrão de conectores ópticos, patch panels, tomadas elétricas e entregar os equipamentos dentro desses padrões ou com as adaptações necessárias.

8.1.3 A CONTRATADA será responsável por elaborar e entregar o PPI dos equipamentos em até 10 (dez) dias corridos, contados a partir da solicitação da CONTRATANTE, constante no item 7.2, ou seja, da emissão da OSE.

8.1.4 A CONTRATANTE fará análise e validação do PPI, em até 3 (três) dias úteis, apontando as devidas correções e ou ajustes no documento, ficando a CONTRATADA responsável por ajustar o plano em até 2 (dois) dias úteis, a partir da comunicação da CONTRATANTE das não conformidades e das alterações necessárias, apontadas pela CONTRATANTE.

8.1.5 Após entrega dos equipamentos e do Projeto Provisório de Instalação já ajustado pela CONTRATADA, a CONTRATANTE emitirá, em até 5 (cinco) dias úteis, a Ordem de Serviço da Instalação - OSI.

8.2 Da instalação

8.2.1 Os equipamentos descritos no ANEXO A, quando adquiridos conjunta ou isoladamente, deverão ser entregues instalados e operacionais, incluindo todos os acessórios necessários para o seu pleno funcionamento, no prazo do item 7.5 deste termo de referência.

8.2.2 Fica a critério da CONTRATANTE, definir o horário de instalação e configuração dos equipamentos e *softwares*, podendo tais procedimentos serem? executados em feriados ou finais de semana e em horário noturno, conforme as necessidades da CONTRATANTE.

8.2.3 A CONTRATADA deverá fornecer todos os materiais necessários à instalação física completa, à configuração e ao perfeito funcionamento da totalidade dos itens adquiridos.

8.2.4 Constatada a ocorrência de divergência na especificação técnica, falhas de componentes, defeitos de fabricação e operação ou qualquer outro defeito apresentado durante o transporte, a entrega e a instalação dos equipamentos, fica a CONTRATADA obrigada a providenciar a substituição do equipamento, no prazo do item 7.5.1, sujeitando-se a CONTRATADA às penalidades previstas na legislação vigente e neste edital.

8.2.5 Eventuais despesas de custeio com deslocamento de técnicos da CONTRATADA ao local de instalação, bem como todas as despesas de transporte, diárias, seguro ou quaisquer outros custos envolvidos ficam a cargo exclusivo da CONTRATADA.

8.2.6 A CONTRATADA deverá comunicar a CONTRATANTE a conclusão da instalação dos equipamentos e entregar toda documentação técnica prevista, dentro do prazo definido no item 7.5.2.

8.2.7 A CONTRATADA deverá entregar o Projeto Definitivo de Instalação - PDI (“As Built”), que por sua vez deve contemplar todas as informações constantes previamente do PPI, juntamente com os ajustes, que se mostraram necessários quando da instalação de fato dos ativos.

8.2.8 A CONTRATADA entregará toda a documentação de instalação física dos equipamentos descritos no ANEXO A, a qual deverá prover nível de informação suficiente para que um técnico possa entender e refazer, caso necessário, as instalações e configurações dos equipamentos adquiridos e implantados.

8.2.9 Após a CONTRATADA concluir toda a instalação dos equipamentos, deixando-os completamente operacionais, e a entrega de toda documentação técnica e do PDI, conforme condições e prazos exigidos neste termo de referência, a CONTRATANTE emitirá o Termo de Recebimento Provisório, em até 5 (cinco) dias úteis, contados a partir da comunicação de conclusão da instalação.

8.2.10 Após 15 (quinze) dias úteis da emissão do Termo de Recebimento Provisório, sendo confirmada a operação e desempenho a contento dos equipamentos, nos termos das especificações técnicas e do atestado de homologação, a CONTRATANTE emitirá o Termo de Recebimento Definitivo, verificada a condição estabelecida no item 8.3.9.

8.3 Escopo do Serviço de Instalação

8.3.1 Fornecimento de ferragens e todos os acessórios necessários para instalação dos equipamentos em rack padrão 19” polegadas, exceto para os lotes 1 e 2, conforme descrito no Anexo B deste termo de referência.

8.3.2 Fornecimento de todos os serviços necessários ao planejamento e a execução da instalação, incluindo projetos, configuração dos equipamentos, planos de retorno e contingenciamento, de acordo com as necessidades da CONTRATANTE.

8.3.3 A CONTRATADA deverá executar todas as atividades (físicas e lógicas) de migração dos serviços que se encontrem em operação, incluindo a elaboração do De/Para de portas e a configuração dos equipamentos. A CONTRATANTE deverá disponibilizar a topologia de rede existente para que estas atividades sejam efetuadas.

8.3.4 O plano de retorno e contingenciamento visa garantir a disponibilidade total dos serviços durante e imediatamente após o processo de instalação dos novos equipamentos. Assim, a CONTRATADA, no caso de algum incidente que comprometa os serviços, deverá retornar toda solução conforme estado imediatamente anterior ao processo de instalação. Isso inclui *fallback* tanto de eventuais configurações alteradas (lógicas), bem como também do respectivo cabeamento (físico).

8.3.5 Para garantir esse perfeito funcionamento e a transição das mudanças, a CONTRATADA deverá disponibilizar, conforme acionamento da CONTRATANTE, durante o período de aceitação previsto nos itens 8.2.1 e 8.2.10, um técnico qualificado, com as respectivas ferramentas necessárias, para solucionar o problema ou restabelecer a rede original em até 2 (duas) horas. Caso não seja obedecido o prazo anterior, a CONTRATADA estará sujeita as penalidades previstas na Tabela 3 - Descumprimento dos Níveis Mínimos de Serviço e Penalidades do item 14.1, conforme severidade apontada na Tabela 2 – Classificação de Incidentes do item 11.1.1

8.3.6 A CONTRATADA deverá ainda, independente de outras atividades necessárias para garantir a disponibilidade total dos serviços, executar:

a) Todos os *backups* necessários e relacionados à atividade em questão dos equipamentos da rede em produção;

b) Todos os testes, antes e após as atividades de intervenção e/ou instalação, dos serviços em funcionamento no órgão que tenham relação com os equipamentos em questão.

8.3.7 A CONTRATADA deverá fornecer à equipe de gestão da implantação do órgão demandante, com antecedência mínima de 5 (cinco) dias úteis anteriores a instalação dos equipamentos, em cada localidade indicada pela CONTRATANTE no ANEXO C, os nomes dos técnicos, juntamente com os respectivos números de documento de identidade, para que sejam identificados durante o procedimento de instalação.

8.3.8 Os serviços de instalação deverão ser executados e supervisionados por pelo menos 1 (um) técnico certificado pelo fabricante da solução proposta.

8.3.9 Os acessórios, peças e manuais não utilizados durante a instalação, assim como as embalagens dos equipamentos deverão ser removidas pela CONTRATADA antes da emissão do Termo de Recebimento Definitivo, para que não permaneça no local de instalação nenhum resíduo da embalagem ou qualquer peça solta. Tal exigência é condicionante para emissão do Termo de Recebimento Definitivo, previsto no item 8.2.10.

8.3.10 Somente será considerado instalado o equipamento entregue, quando instalado no respectivo rack de 19´´ polegadas, cabeado, operacional, em plenas condições de

funcionamento, integrado com a rede local e com capacidade de permitir acesso remoto por parte da equipe da CONTRATANTE, exceto para os lotes 1 e 2, conforme Anexo B.

A CONTRATADA deverá realizar a configuração inicial do equipamento para acesso remoto, assim como prestar o fornecimento de quaisquer outros acessórios e serviços que sejam necessários para a completa operacionalização da rede, de acordo com as necessidades da CONTRATANTE.

8.3.11 Cabe à CONTRATADA realizar a instalação dos *firmwares* necessários para o funcionamento e a operação completa dos equipamentos, sendo obrigatória a inclusão no equipamento, no momento da instalação, da versão estável mais atual de todos os *firmwares*.

8.3.12 Todos os *softwares* necessários à operação dos equipamentos e soluções devem, igualmente, ser entregues instalados e operacionais. Também devem estar incluídos e licenciados (se for o caso) todos os componentes de *software* básico necessários ao funcionamento dos equipamentos, tais como: sistemas operacionais, controladores de dispositivos e outros pertinentes.

8.4 Documentação técnica

8.4.1 A documentação técnica de instalação deverá conter, no mínimo:

a) Descrição dos recursos de *hardware* e *software* utilizados nos equipamentos.

b) Lista de todos os elementos instalados contendo: nome e endereço IP do equipamento, juntamente com todas as interconexões físicas (equipamento/porta origem e equipamento/porta destino), local de instalação (prédio, andar, sala), número de série, número do bem utilizado pelo CONTRATANTE, data da instalação, data de aquisição, data de vencimento da garantia.

c) Listagem das configurações dos equipamentos com comentários sobre os principais comandos e as justificativas das opções de parametrização.

d) Plantas de instalação e *bay-plan* dos racks usados na instalação dos equipamentos.

e) Com relação às configurações dos equipamentos, a CONTRATADA deverá implementar todas as funcionalidades requisitadas pela CONTRATANTE, estando essas minimamente restritas aos requisitos constantes na especificação técnica. Nas implementações dos ativos a serem instalados que dependam de integração com os demais elementos da rede, a CONTRATANTE será responsável por disponibilizar as informações à CONTRATADA, necessárias à harmonização desses novos ativos com os equipamentos preexistentes na rede local da CONTRATANTE.

f) Configuração dos equipametnos segundo as especificações da CONTRATANTE, o que pode incluir, por exemplo, ativação de mecanismos avançados de segurança de rede local e integração com serviços de diretório para autenticação de usuários.

8.4.2 O Projeto Definitivo de Instalação – PDI, conforme estabelecido neste Termo de Referência.

8.4.3 Toda documentação exigida neste Termo de Referência deverá ser entregue em mídia eletrônica ou, a critério da CONTRATANTE, em material impresso.

8.4.4 A documentação técnica deverá garantir a transferência de conhecimento à CONTRATANTE, a fim de proporcionar o nível de informação necessário à operação da rede e possíveis intervenções.

9 DAS OBRIGAÇÕES DA CONTRATADA

9.1 Fornecer o objeto para o qual se sagrar vencedora, em estrita conformidade com as especificações e condições exigidas neste Termo de Referência, bem como naquelas resultantes de sua proposta, devendo já estar inclusos nos valores propostos todos os custos, impostos, taxas e demais encargos pertinentes à execução do objeto do contrato. não sendo aceitas quaisquer modificações.

9.2 Substituir os equipamentos não aceitos pela CONTRATANTE em prazo não superior ao indicado no item 7.5.1, contados da ciência da rejeição.

9.3 Responsabilizar-se pelo ônus e a logística da retirada e devolução dos equipamentos para realização de serviços de garantia fora das dependências da CONTRATANTE, bem como da substituição de equipamentos não aceitos.

9.4 Comprovar, no ato da assinatura da ata de registro de preços:

9.4.1 Que os serviços de garantia serão prestados pelo fabricante dos equipamentos, ou por meio de empresas credenciadas por este, com disponibilidade de atendimento nas localidades especificadas no ANEXO C.

9.4.2 No momento da assinatura da ARP a licitante vencedora deverá entregar a relação da rede de assistência técnica autorizada contemplando todos os locais listados nesse edital, declarando que os técnicos são devidamente treinados e com capacitação técnica inerente ao desempenho da atividade pertinente e compatível com as características do objeto da licitação, bem como da entrega, montagem, instalação física e garantia dos equipamentos que irão atender a CONTRATANTE.

9.4.3 No ato da assinatura de cada contrato, a CONTRATADA deverá informar, por escrito, a equipe técnica, qualificada para a execução dos serviços no(s) endereço(s) de entrega.

9.5 Responsabilizar-se pelo fornecimento dos itens, objeto do Contrato, respondendo administrativa, civil e criminalmente por todos os danos, perdas e prejuízos que, por dolo ou culpa sua, de seus empregados, prepostos, ou terceiros no exercício de suas atividades, vier a, direta ou indiretamente, causar ou provocar à CONTRATANTE e a terceiros.

9.6 Manter as condições de habilitação e qualificação exigidas na licitação, durante a execução da Ata de RP e dos contratos, informando ao CONTRATANTE a ocorrência de qualquer alteração nas referidas condições apresentando, sempre que exigido, os comprovantes de regularidade.

9.7 Sujeitar-se à fiscalização do CONTRATANTE no tocante à verificação das especificações técnicas, prestando os esclarecimentos solicitados, atendendo às reclamações procedentes, caso ocorram, e prestando toda assistência técnica operacional.

9.8 Sujeitar-se à mais ampla e irrestrita fiscalização, acatar as orientações do FISCAL DE CONTRATO, prestando os esclarecimentos sobre o objeto contratado e sobre o atendimento das reclamações formuladas, nos devidos prazos.

9.9 Não transferir a outrem, no todo ou em parte, as obrigações oriundas da contratação, sem prévia e expressa anuência da CONTRATANTE.

9.10 Garantir o perfeito funcionamento da solução, quando ocorrer a implantação em campo, não cabendo ônus adicional aos órgãos CONTRATANTES.

9.11 Entende-se como perfeito funcionamento: compatibilidade do objeto com todas as descrições exigidas deste Termo de Referência e seus anexos, bem como o atendimento às exigências da legislação vigente.

9.12 Executar os serviços conforme especificações deste Termo de Referência e de sua proposta, com a alocação dos empregados necessários ao perfeito cumprimento das cláusulas contratuais, além de fornecer os materiais e equipamentos, ferramentas e utensílios necessários, na qualidade e quantidade especificadas neste Termo de Referência e em sua proposta;

9.13 Reparar, corrigir, remover ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os serviços efetuados em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;

9.14 Manter o empregado nos horários predeterminados pela Administração;

9.15 Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, de acordo com os artigos 14 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990), ficando a Contratante autorizada a descontar da garantia, caso exigida no edital, ou dos pagamentos devidos à Contratada, o valor correspondente aos danos sofridos;

9.16 Utilizar empregados habilitados e com conhecimentos específicos dos serviços a serem executados, em conformidade com as normas e determinações em vigor;

9.17 Apresentar os empregados devidamente uniformizados e identificados por meio de crachá, além de provê-los com os Equipamentos de Proteção Individual - EPI, quando for o caso;

9.18 Apresentar à Contratante, quando for o caso, a relação nominal dos empregados que adentrarão o órgão para a execução do serviço;

9.19 Responsabilizar-se por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas na legislação específica, cuja inadimplência não transfere responsabilidade à Contratante;

9.20 Apresentar, quando solicitado, atestado de antecedentes criminais e distribuição cível de toda a mão de obra oferecida para atuar nas instalações do órgão;

9.21 Atender as solicitações da Contratante quanto à substituição dos empregados alocados, no prazo fixado pelo fiscal do contrato, nos casos em que ficar constatado descumprimento das obrigações relativas à execução do serviço, conforme descrito neste Termo de Referência;

9.22 Instruir seus empregados quanto à necessidade de acatar às recomendações aceitas pela boa técnica, normas e legislação;

9.23 Instruir seus empregados a respeito das atividades a serem desempenhadas, alertando-os a não executar atividades não abrangidas pelo contrato, devendo a Contratada relatar à Contratante toda e qualquer ocorrência neste sentido, a fim de evitar desvio de função;

9.24 Relatar à Contratante toda e qualquer irregularidade verificada no decorrer da prestação dos serviços;

9.25 Não permitir a utilização de qualquer trabalho do menor de dezesseis anos, exceto na condição de aprendiz para os maiores de quatorze anos; nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre;

9.26 Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;

9.27 Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato;

9.28 Arcar com os ônus necessários aos fornecimentos descritos neste processo;

9.29 Assumir, a responsabilidade pelos encargos fiscais e comerciais resultantes da adjudicação do contrato;

9.30 Responder pelo cumprimento dos postulados legais vigentes no âmbito federal, estadual ou municipal;

9.31 Preservar as informações do órgão, não divulgar nem permitir a divulgação, sob qualquer hipótese, das informações a que venha a ter acesso em decorrência dos serviços realizados, sob pena de responsabilidade civil e/ou criminal.

9.32 Obriga-se a aceitar, nas mesmas condições contratuais, e mediante Termo Aditivo, os acréscimos ou supressões que se fizerem necessários, no montante de até 25% (vinte e cinco por cento) do valor inicial atualizado do Contrato, de acordo com os Parágrafos Primeiro e Segundo do Artigo 65 da Lei nº 8.666/93.

9.33 Credenciar por escrito, junto a CONTRATANTE, um preposto idôneo com poderes de decisão para representar a CONTRATADA, principalmente no tocante à eficiência e agilidade da execução dos serviços objeto deste Termo de Referência.

10 DAS OBRIGAÇÕES DA CONTRATANTE

10.1 Prestar à CONTRATADA as informações e esclarecimentos necessários para a efetivação do fornecimento.

10.2 Efetuar o pagamento à CONTRATADA, após o cumprimento das obrigações e formalidades legais, conforme previsto neste Termo de Referência e na legislação vigente.

10.3 Exigir o cumprimento de todas as obrigações assumidas pela Contratada, de acordo com as cláusulas contratuais e os termos de sua proposta;

10.4 Exercer o acompanhamento e a fiscalização dos serviços, por servidor especialmente designado, anotando em registro próprio as falhas detectadas, indicando dia, mês e ano, bem como o nome dos empregados eventualmente envolvidos, e encaminhando os apontamentos à autoridade competente para as providências cabíveis;

10.5 Notificar a Contratada por escrito da ocorrência de eventuais imperfeições no curso da execução dos serviços, fixando prazo para a sua correção;

10.6 Prestar as informações e esclarecimentos relativos ao objeto desta contratação que venham ser solicitados pelo consultor designado pela CONTRATADA.

10.7 Garantir, quando necessário, o acesso dos empregados da CONTRATADA às suas dependências para recolhimento dos aparelhos com defeitos referentes ao objeto contratado.

10.8 Controlar as ligações realizadas e documentar as ocorrências havidas.

10.9 Dirimir as dúvidas que surgirem no curso da entrega dos produtos por intermédio do Fiscal do contrato, que de tudo dará ciência à Administração, conforme art. 67 da Lei nº 8.666, de 1993 e IN 02/2008 e posteriores alterações.

10.10 Informar o nome da pessoa designada para manter entendimentos durante a execução do fornecimento.

10.11 Efetuar a entrega dos materiais de acordo com a especificação e demais condições estipuladas no Edital.

10.12 Substituir, às suas expensas, no todo ou em parte, os materiais em que se verifique defeito de fabricação ou danos em decorrência do transporte, no prazo máximo de 05 (cinco) dias úteis, contados da notificação que lhe for entregue oficialmente.

10.13 Assumir todo e qualquer ônus referente a salário, horas extras, adicionais e demais encargos socais relativamente a seus empregados.

10.14 Assumir a responsabilidade pelos encargos fiscais e comerciais resultantes da adjudicação desta Licitação.

10.15 Garantir que todos os materiais a serem fornecidos são de boa qualidade, atendem aos padrões de mercado e satisfaçam as especificações e recomendações do fabricante e fornecedor.

10.16 Manter compatibilidade com as obrigações por ele assumidas, todas as condições de habilitação e qualificação exigidas na licitação.

10.17 Fazer constar nas notas fiscais as marcas dos materiais, definidas por ocasião do processo licitatório, para a devida conferência e documentação.

11 DOS NÍVEIS MÍNIMOS DE SERVIÇOS

11.1 Os níveis mínimos de serviço esperados para essa contratação, bem como para os atendimentos aos eventos associados estão indicados na ‘Tabela 1- Níveis Mínimos de Serviço’, cabendo os seguintes detalhamentos:

11.1.1 A classificação da severidade do evento será determinada pela CONTRATANTE respeitando-se o descrito na 'Tabela 2 - Classificação de Incidentes';

11.1.2 Todos os prazos especificados na 'Tabela 1 - Níveis Mínimos de Serviço' são contados a partir da abertura do respectivo número de identificação do chamado.

Tabela 1 - Níveis Mínimos de Serviço

Equipamentos	Localidade dos órgãos	Severidade	Medidas para o Indicador
Tipos 1, 2, 3, 4 e 5	Capitais: Brasília, Rio de Janeiro e São Paulo	A	4 horas
		B	6 horas
		C	24 horas
	Demais Capitais e regiões metropolitanas	A	6 horas
		B	8 horas
		C	24 horas
	Demais regiões	A	8 horas
		B	12 horas
		C	24 horas

11.1.3 A abertura do chamado com fornecimento do seu número de identificação (protocolo de atendimento) deve ocorrer no prazo máximo de 15 minutos a partir da tentativa de contato pela CONTRATANTE com o número fornecido pela CONTRATADA.

11.1.4 O atendimento aos chamados pode ocorrer remotamente (preferencialmente, inclusive em alguma representação regional do órgão), ou de forma presencial. Atendimentos remotos não resolvidos que ultrapassem 12 horas nas capitais Brasília, Rio de Janeiro e São Paulo, ou ultrapassem 24 horas nas demais capitais, ou ultrapassarem 48 horas nas demais regiões devem ser continuados de forma presencial.

Tabela 2 – Classificação de Incidentes

(A) EMERGENCIAL	São consideradas como "Emergência" todas as falhas cujas consequências tenham impactos negativos, gerando indisponibilidade sobre o serviço e o tráfego e/ou recursos. São situações que exijam atenção imediata. Ex: Situação de indisponibilidade total do equipamento, funcionamento intermitente ou parcial do equipamento, que possa levar à interrupção intermitente, parcial ou total de serviços ou perda de tráfego.
(B) GRAVE	Problemas que não prejudicam significativamente o funcionamento dos sistemas/serviços do equipamento. São problemas sérios ou perturbações, que afetam uma área específica ou determinada funcionalidade do equipamento. Ex: Perda de redundância, reinicialização de módulos, *slots* ou portas com defeitos, degradação de desempenho, perda de funcionalidades.

(C) PEDIDO DE INFORMAÇÃO	Solicitação de informações sobre o funcionamento dos equipamentos, possíveis configurações ou usos, que não gerem interrupções, nem indisponibilidade de determinada área ou uma funcionalidade especifica..

11.1.5 Um chamado classificado de acordo com essas severidades não pode ser reclassificado a medida que é resolvido em outra. A severidade deve levar em conta o fator que foi usado na sua abertura e seguir esse mesmo critério até a sua completa solução.

12 DA GARANTIA DOS PRODUTOS

12.1 Durante o período de garantia, a CONTRATADA deverá estar apta a atender chamados encaminhados pela CONTRATANTE ao Centro de Atendimento da CONTRATADA, sem ônus adicional para o CONTRATANTE, oferecendo, no mínimo, os seguintes serviços:

12.1.1 Deve ser possível tanto acionamento via número 0800, quanto via Web, disponível 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, para solução de problemas decorrentes de defeitos e falhas nos produtos ou equipamento/*software*, ou seja, problemas decorrentes do fato do ativo de rede não realizar uma funcionalidade especificada ou esperada. Poderá ainda, esse serviço, ser usado para solicitar informações quanto às dúvidas, funcionalidades e quanto a procedimentos para configuração dos itens do objeto contratado.

12.1.2 Todos os custos decorrentes da retirada de equipamentos ou componentes para a prestação do serviço de garantia serão de responsabilidade da CONTRATADA, bem como seu retorno aos locais onde serão instalados os equipamentos pela empresa contratada.

12.2 No atendimento dos chamados, caso a CONTRATADA não consiga resolver o problema por meio da assistência remota, deverá a CONTRATADA realizar uma ação *On-Site* (no local onde está o ativo de rede) para sanar o problema e restabelecer o funcionamento normal do equipamento, obedecendo o disposto no item 11.1.4 e atendendo aos prazos previstos na Tabela 1 - Níveis Mínimos de Serviço do item 11.1, responsabilizando-se pelas despesas de deslocamento de seu técnico/especialista.

12.3 Em qualquer caso, a CONTRATADA deverá arcar com todos os procedimentos necessários à solução do problema, incluindo a substituição de quaisquer módulos defeituosos no(s) equipamento(s), bem como a substituição do(s) próprio(s) equipamentos(s), se for necessário, devendo ser atendida as seguintes condições:

12.3.1 Os chamados serão registrados e informados à CONTRATANTE, nos prazos da Tabela 1, e deverão estar disponíveis, via sistema *web*, para acompanhamento pela equipe designada pela CONTRATANTE, contendo data e hora do chamado, o problema ocorrido, a solução, data e hora de conclusão.

12.3.2 Decorrido os prazos previstos na Tabela 1 – Níveis Mínimos de Serviço do item 11.1, sem o atendimento devido, fica a CONTRATANTE autorizada a penalizar a CONTRATADA dentro dos parâmetros explicitados neste Termo de Referência, respeitado o direito ao contraditório e ampla defesa.

12.3.3 A CONTRATADA deverá encaminhar ao fiscal técnico do contrato, até o 5º dia útil de cada mês, o Relatório de Acompanhamento de Nível Mínimo de Serviço, com informações de TODOS chamados abertos pela CONTRATANTE, em sua central de atendimento, contendo, pelo menos, as seguintes informações:

a) Data, hora da abertura do chamado;
b) Número de série do equipamento alvo do atendimento;
c) Data e hora da chegada do técnico ao local;
d) Data e hora da resolução do problema;
e) Descrição do problema, incidente ou solicitação atendida e Procedimentos efetuados.
f) Ateste(s) de atendimento e solução do(s) problema(s)

12.4 **Garantia dos equipamentos e serviços – disposições gerais**

12.4.1 A CONTRATADA deverá garantir a completa interoperabilidade e compatibilidade entre os *Firewalls* a serem adquiridos no presente Termo de Referência e os Ativos já em funcionamento na CONTRATANTE. Não podendo se excusar de suas responsabilidades quanto à prestação da solução técnica para possíveis falhas ou inconsistências, bem como o auxílio técnico necessários à interoperação da rede, a fim de garantir o perfeito funcionamento dos ativos adquiridos com os demais ativos com os quais deverão interoperar.

12.4.2 Sendo a CONTRATADA designada para realizar a instalação dos Firewalls, será de sua responsabilidade a correção das falhas decorrentes de erros durante as atividades de instalação, sejam operacionais ou por problemas de mau funcionamento, responsabilizando-se por todos os custos envolvidos na correção dos desvios, sejam de interoperabilidade, incompatibilidade ou quaisquer outras falhas que impeçam a instalação ou o perfeito funcionamento dos Firewalls adquiridos.

12.4.3 A CONTRATADA deverá garantir o pleno funcionamento dos Firewalls, prestando o serviço de garantia remoto e *on-site* (quando, a critério da CONTRATANTE, for necessário), por um período de 60 (sessenta) meses, contados a partir da data de emissão do Termo de Recebimento Definitivo.

12.4.4 A CONTRATADA deve garantir o funcionamento dos equipamentos, considerados isoladamente ou interligados aos demais, de acordo com as características descritas nos manuais e nas especificações aplicáveis, desde que o restante dos equipamentos de rede da CONTRATANTE esteja em condições normais de operação.

12.4.5 Para a referida garantia, serão considerados os eventos descritos conforme a Tabela 2 - Classificação de Eventos do item 11.1.1, devendo ser considerado para o enquadramento o grau de impacto para o serviço ou cliente afetado.

12.4.6 A CONTRATADA, no caso da atualização de equipamento para corrigir falhas apresentadas, deve se responsabilizar pelos custos envolvidos, inclusive eventuais trocas de hardware.

12.5 **Garantia de *Hardware***

12.5.1 A troca de qualquer unidade defeituosa deverá ser realizada em conformidade com os prazos estabelecidos na Tabela 1 – Níveis Mínimos de Serviço do item 11.1.

12.5.2 A CONTRATADA deve garantir que os equipamentos fornecidos são apropriados para suportar as condições climáticas, conforme características exigidas nas especificações técnicas constantes no ANEXO B.

12.6 **Garantia de *Software***

12.6.1 A CONTRATADA deve disponibilizar, sem quaisquer custos adicionais à CONTRATANTE, a atualização de novas versões dos *software*(s) e *firmware*(s) fornecido(s), ou de parte(s) dele(s), decorrentes da evolução funcional ou correções do(s) anteriormente fornecido(s), durante o prazo da garantia da solução integrada de segurança .

12.6.2 Cabe à CONTRATADA informar, por intermédio de carta ou mensagem eletrônica, a disponibilidade de novas versões e atualizações, assim como quanto aos respectivos procedimentos de instalação. Por nova versão, entende-se por aquele que, mesmo sendo comercializado com novo nome, número de versão ou marca, retenha as funcionalidades exigidas na presente especificação técnica.

12.6.3 A CONTRATANTE reserva-se o direito de aceitar ou não atualizações no *software* ou parte dele.

12.6.4 A CONTRATADA deve garantir que uma nova versão do *software* ou *firmware* mantenha a compatibilidade e contenha todas as funções das versões anteriores e que a introdução desta não prejudique a interoperabilidade da mesma na rede.

12.6.5 A CONTRATADA deve garantir a independência entre a correção de defeitos (*patches*) e a geração de novas versões do *software*, sem ônus adicional à CONTRATANTE, em função da necessidade de atualização de componente para suportar nova versão do *software*.

12.6.6 A CONTRATADA deverá garantir o correto funcionamento de todo *software* instalado no equipamento durante um período de garantia de 60 (sessenta) meses, a contar da data do Termo de Recebimento Definitivo.

12.6.7 Durante todo o período de garantia, a CONTRATADA obriga-se a substituir, recuperar e/ou modificar os *softwares* e *firmwares* instalados, sem ônus de qualquer natureza à CONTRATANTE, nos casos comprovados de mau funcionamento e de outras falhas, de modo a ajustá-los aos resultados que atendam às especificações técnicas solicitadas para o equipamento, conforme ANEXO B.

13 DAS SANÇÕES ADMINISTRATIVAS

13.1 A LICITANTE que, convocada dentro do prazo de validade da sua proposta, não assinar Ata de Registro de Preço ou o contrato, deixar de entregar documentação exigida neste Termo de Referência, apresentar documentação falsa, ensejar o retardamento na execução de seu objeto, não mantiver a proposta, falhar ou fraudar no fornecimento do material ou na instalação, comportar-se de modo inidôneo, fizer declaração falsa ou cometer fraude fiscal, poderá ser impedida de licitar e de contratar com a União, Distrito Federal, Estados ou Municípios, e será descredenciada no SICAF ou nos Sistemas de Cadastramento de Fornecedores a que se refere o inciso XIV do art. 4º da Lei nº 10.520, de 17 de julho de 2002, pelo prazo de até 5 (cinco) anos, sem prejuízo das multas previstas neste Edital e das demais cominações legais.

13.1.1 Em caso de inexecução do contrato, erro de execução, execução parcial (imperfeita), mora na execução e inadimplemento contratual, a CONTRATADA ficará sujeita, ainda, às seguintes penalidades:

a) Advertência;

b) Multa;

b1) multa moratória de 5% (cinco por cento) sobre o valor do Contrato, pela recusa da CONTRATADA em assinar Contrato, e pela não apresentação da documentação exigida no Edital para sua celebração, nos prazos e condições estabelecidas, caracterizando o descumprimento total da obrigação assumida, com base no art. 81 da Lei nº 8.666, de 1993, independentemente das demais sanções cabíveis;

b2) multa moratória de 1% (um por cento) sobre o valor do item, ou conjuntos de itens, por dia de atraso, no caso da CONTRATADA não entregar e/ou não instalar os equipamentos no prazo estipulados no item 7.5, até o limite máximo de 30 (trinta) dias.

b3) multa de moratória no percentual de 10% (dez por cento), calculada sobre o valor total do contrato, pela inadimplência, sem preluzo das demais sanções cabíveis e/ou rescisão contratual.

b4) multa moratória de 5% (cinco por cento) sobre o valor do contrato, pela inexecução parcial, total ou execução insatisfatória do contrato, aplicada em dobro na sua reincidência, ou pela interrupção da execução do contrato sem prévia autorização da CONTRATANTE, independentemente das demais sanções cabíveis;

b5) multa moratória de 1% (um por cento) sobre o valor do contrato, pela recusa em corrigir qualquer objeto rejeitado ou com defeito, caracterizando-se a recusa caso a correção não se efetivar nos 10 (dez) dias que se seguirem à data da comunicação formal da rejeição ou defeito, independentemente das demais sanções cabíveis;

b6) multa moratória de 1% (um por cento) sobre o valor do contrato, pela mora na apresentação, do PPI, do PDI ou do Relatório de Acompanhamento de Nível Mínimo de Serviço, constante do item 12.3.3, ou mesmo com a apresentação desse documento com informações incorretas;

b7) multa moratória de 1% (um por cento) sobre o valor total do Contrato, por descumprir ou infringir qualquer das obrigações estabelecidas nos demais itens referentes ao item 9 –DAS OBRIGAÇÕES DA CONTRATADA, estabelecidos neste Termo de Referência, aplicada em dobro na sua reincidência, independentemente das demais sanções cabíveis;

b8) multa compensatória de 10% (dez por cento) sobre o valor do Contrato, sendo deste valor, deduzido o (s) valor (es) referente(s) à(s) multa(s) moratória(s), no caso de rescisão do Contrato por ato unilateral da administração, motivado por culpa da CONTRATADA, garantida a defesa prévia e o contraditório, independentemente das demais sanções cabíveis.

c) Suspensão temporária de participação em licitação e impedimento de licitar e contratar com a Administração pelo prazo de até 2 (dois) anos.

d) Declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição, conforme disposto no inciso IV do Art. 87 da Lei nº 8.666, de 1993.

13.1.2 A critério da Administração, as multas poderão ser descontadas das garantias de fornecimento apresentadas pela LICITANTE VENCEDORA;

13.1.3 No processo de aplicação de penalidades e da incidência de multas, será garantido a CONTRATADA o direito a ampla defesa e o contraditório, frente aos resultados da apuração do Nível Mínimo de Serviço, bem como a apresentação das justificativas que se fizerem necessárias;

13.1.4 As justificativas, devidamente fundamentadas, aceitas pelo gestor e pelo fiscal técnico do contrato poderão anular a incidência de multas e advertências na aplicação do Nível Mínimo de Serviço.

13.1.5 Os valores de multas não pagos serão descontados da fatura ou da garantia prestada pela CONTRATADA;

13.1.6 Se a multa aplicada for superior ao valor da garantia prestada, além da perda desta, responderá a CONTRATADA pela diferença, que será descontada dos pagamentos eventualmente devidos à Administração ou cobrada judicialmente;

13.1.7 As penalidades serão obrigatoriamente registradas no SICAF e, no caso de suspensão de licitar, por descumprimento parcial ou total do contrato, a Licitante deverá ser descredenciada por igual período, ou seja, por prazo não superior a 05 (cinco) anos, conforme art. 7º da Lei nº 10.520, de 17 de julho de 2002, sem prejuízo das multas previstas no instrumento convocatório e das demais combinações legais. ;

13.1.8 A declaração de inidoneidade para licitar ou contratar com a Administração Pública dar-se-á pela autoridade máxima do órgão CONTRATANTE, nos termos da Lei nº 8.666, de 1993.

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

14 DESCUMPRIMENTO DOS NÍVEIS MÍNIMOS DE SERVIÇO E PENALIDADES

14.1 O descumprimento total ou parcial das obrigações assumidas pela CONTRATADA, referente ao não atendimento aos Níveis Mínimos de Serviço da Tabela 1, do item 11.1, resguardados os procedimentos legais pertinentes, sem prejuízo nas demais sanções cabíveis, poderá acarretar as seguintes penalidades de acordo com a Tabela 3 – Descumprimento dos Níveis de Serviço e Penalidades:

Tabela 3 – Descumprimento dos Níveis de Serviço e Penalidades.

Equipamento	Severidade	Localidade	Descrição	Penalidades
Tipo1, 2, 3, 4 e 5	A	Capitais: Brasília, São Paulo e Rio de Janeiro.	Até 4 horas corridas de atraso, além do prazo indicado na Tabela 1 - Níveis Mínimos de Serviço.	1) Advertência; 2) Havendo recorrência, multa de 0,1% (zero vírgula um por cento) por hora de atraso, calculada sobre o valor do equipamento.
			Superior a 4 horas e inferior ou igual a 8 horas corridas de atraso, além do prazo definido nos Níveis Mínimos de Serviços.	3) Multa de 0,2% (zero vírgula dois por cento) por hora de atraso, calculada sobre o valor do equipamento, sem prejuízo ao item anterior.
			Superior a 8 horas corridas, além do prazo indicado na Tabela 1 – Níveis Mínimos de Serviço.	4) Multa de 0,4% (zero vírgula quatro por cento) por hora de atraso, calculada sobre o valor do equipamento, sem prejuízo ao item anterior, e outras sanções administrativas a critério da CONTRATANTE.
		Demais capitais e regiões metropolitanas	Até 6 horas corridas de atraso, além do prazo indicado na Tabela 1 - Níveis Mínimos de Serviço.	5) Advertência; 6) Havendo recorrência, multa de 0,1% (zero vírgula um por cento) por hora de atraso, calculada sobre o valor do equipamento.
			Superior a 6 horas e inferior ou igual a 12 horas corridas de atraso, além do prazo definido nos Níveis Mínimos de Serviços.	7) Multa de 0,2% (zero vírgula dois por cento) por hora de atraso, calculada sobre o valor do equipamento, sem prejuízo ao item anterior.

			Superior a 12 horas corridas, além do prazo indicado na Tabela 1 – Níveis Mínimos de Serviço.	8) Multa de 0,4% (zero vírgula quatro por cento) por hora de atraso, calculada sobre o valor do equipamento, sem prejuízo ao item anterior, e outras sanções administrativas a critério da CONTRATANTE.
		Demais regiões	Até 8 horas corridas de atraso, além do prazo indicado na Tabela 1 - Níveis Mínimos de Serviço.	9) Advertência; 10) Havendo recorrência, multa de 0,1% (zero vírgula um por cento) por hora de atraso, calculada sobre o valor do equipamento.
			Superior a 8 horas e inferior ou igual a 16 horas corridas de atraso, além do prazo definido nos Níveis Mínimos de Serviços.	11) Multa de 0,2% (zero vírgula dois por cento) por hora de atraso, calculada sobre o valor do equipamento, sem prejuízo ao item anterior.
			Superior a 16 horas corridas, além do prazo indicado na Tabela 1 – Níveis Mínimos de Serviço.	12) Multa de 0,4% (zero vírgula quatro por cento) por hora de atraso, calculada sobre o valor do equipamento, sem prejuízo ao item anterior, e outras sanções administrativas a critério da CONTRATANTE.
			-	13) Se o somatório das multas aplicadas, com relação às obrigações relativas a um mesmo equipamento ultrapasse 20% do seu valor de aquisição, poderá ensejar a rescisão do Contrato, independentemente da aplicação das sanções administrativas previstas neste Termo de Referência e na legislação vigente.
	B	Capitais: Brasília, São Paulo e Rio de Janeiro.	Até 6 horas corridas de atraso, além do prazo indicado na Tabela 1 – Níveis Mínimos de Serviço.	14) Advertência; 15) Para as demais ocorrências, multa de 0,05% (zero vírgula zero cinco por cento) por hora de atraso, calculada sobre o valor do equipamento.

			Superior a 6 horas e inferior ou igual a 12 horas corridas de atraso, além do prazo definido nos Níveis Mínimos de Serviços.	16) Multa de 0,1% (zero vírgula um por cento) por hora de atraso, calculada sobre o valor do equipamento, sem prejuízo ao item anterior.
			Superior a 12 horas corridas de atraso, além do prazo definido nos Níveis Mínimos de Serviços.	17) Multa de 0,2% (zero vírgula dois por cento) por hora de atraso, calculada sobre o valor do equipamento, sem prejuízo ao item anterior, e outras sanções administrativas a critério da CONTRATANTE.
		Demais capitais e regiões metropolitanas	Até 8 horas corridas de atraso, além do prazo indicado na Tabela 1 – Níveis Mínimos de Serviço.	18) Advertência; 19) Para as demais ocorrências, multa de 0,05% (zero vírgula zero cinco por cento) por hora de atraso, calculada sobre o valor do equipamento.
			Superior a 8 horas e inferior ou igual a 16 horas corridas de atraso, além do prazo definido nos Níveis Mínimos de Serviços.	20) Multa de 0,1% (zero vírgula um por cento) por hora de atraso, calculada sobre o valor do equipamento, sem prejuízo ao item anterior.
			Superior a 16 horas corridas de atraso, além do prazo definido nos Níveis Mínimos de Serviços.	21) Multa de 0,2% (zero vírgula dois por cento) por hora de atraso, calculada sobre o valor do equipamento, sem prejuízo ao item anterior, e outras sanções administrativas a critério da CONTRATANTE.

		Demais regiões	Até 12 horas corridas de atraso, além do prazo indicado na Tabela 1 – Níveis Mínimos de Serviço.	22) Advertência; 23) Para as demais ocorrências, multa de 0,05% (zero vírgula zero cinco por cento) por hora de atraso, calculada sobre o valor do equipamento.
			Superior a 12 horas e inferior ou igual a 24 horas corridas de atraso, além do prazo definido nos Níveis Mínimos de Serviços.	24) Multa de 0,1% (zero vírgula um por cento) por hora de atraso, calculada sobre o valor do equipamento, sem prejuízo ao item anterior.
			Superior a 24 horas corridas de atraso, além do prazo definido nos Níveis Mínimos de Serviços.	25) Multa de 0,2% (zero vírgula dois por cento) por hora de atraso, calculada sobre o valor do equipamento, sem prejuízo ao item anterior, e outras sanções administrativas a critério da CONTRATANTE.
			-	26) Se o somatório das multas aplicadas, com relação às obrigações relativas a um mesmo equipamento ultrapasse 20% do seu valor de aquisição, poderá ensejar a rescisão do Contrato, independentemente da aplicação das sanções administrativas previstas neste Termo de Referência e na legislação vigente.
	C	Todas as capitais e demais regiões	Até 24 horas corridas de atraso, além do prazo indicado na Tabela 1 – Níveis Mínimos de Serviço.	27) Advertência; 28)Para as demais ocorrências, multa de 0,05% (zero vírgula zero cinco por cento) por hora de atraso, calculada sobre o valor do equipamento. 29) Se o somatório das multas aplicadas com relação às obrigações relativas a um mesmo equipamento ultrapasse 20% do seu valor de aquisição, poderá ensejar a rescisão do Contrato, independentemente de aplicação das sansões administrativas cabíveis.

15 DO PAGAMENTO

15.1 O pagamento será efetuado até o 10° (décimo) dia útil, mediante apresentação da Nota Fiscal/Fatura pela empresa, devidamente atestada pelo setor competente, após a emissão do Termo de Recebimento Definitivo do objeto, sendo efetuada a retenção de tributos sobre o pagamento a ser realizado, conforme determina a legislação vigente.

15.2 A Fatura/Nota Fiscal deverá ser entregue no endereço estipulado pela CONTRATANTE, devidamente discriminada em nome desta, com a descrição dos itens e quantidades que foram efetivamente realizados.

15.3 O pagamento será creditado em conta corrente, por meio de ordem bancária a favor da instituição bancária indicada na Nota Fiscal da CONTRATADA, devendo para isso ficar explícito o nome do banco, agência, localidade e número da conta corrente em que deverá ser efetivado o crédito.

15.4 Caso a CONTRATADA seja optante pelo Sistema Integrado de Pagamento de Impostos e Contribuições das Microempresas e Empresas de Pequeno Porte – SIMPLES, deverá apresentar, juntamente com a Nota Fiscal, a devida comprovação, a fim de evitar a retenção na fonte dos tributos e contribuições, de acordo com a Lei Complementar nº 123, de 14 de dezembro de 2006.

15.5 Havendo erro na Nota Fiscal ou circunstância que impeça a liquidação da despesa, a mesma será devolvida à CONTRATADA, e o pagamento ficará pendente até que a mesma providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a regularização da situação ou reapresentação do documento fiscal não acarretando qualquer ônus adicional para a CONTRATANTE.

15.6 Ocorrendo eventuais atrasos de pagamento, provocados exclusivamente pelo órgão CONTRATANTE, o valor devido deverá ser acrescido de atualização financeira, e sua apuração se fará desde a data de seu vencimento até a data do efetivo pagamento, em que os juros de mora serão calculados à taxa de 0,5% (meio por cento) ao mês, ou 6% (seis por cento) ao ano, mediante a aplicação das seguintes fórmulas:

$$I = (TX/100) / 365$$

$$EM = I \times N \times VP$$

Onde:

I = Índice de atualização financeira;
TX = Percentual da taxa de juros de mora anual;
EM = Encargos moratórios;
N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;
VP = Valor da parcela em atraso.

16 DA PROPOSTA

16.1 A licitante deverá apresentar proposta de preço dos itens discriminados no ANEXO A. Os preços deverão ser expressos em reais (R$) com duas casas decimais e conter todos os custos operacionais, encargos previdenciários,trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente no fornecimento dos equipamentos e da prestação dos serviços relativos a esta contratação. Ou seja, a Proposta de Preços deverá ser preenchida com os preços cotados para cada item do lote com todos os custos inclusos.

16.2 A proposta deverá ser formulada contendo as especificações do objeto de forma clara, comprovando ponto a ponto, por escrito, o atendimento aos requisitos técnicos e às funcionalidades requeridas em cada item que compõe o lote, conforme modelo apresentado no ANEXO D, detalhando os componentes, peças, chassis, fonte de alimentação, placas de serviço, placas de interface, módulos de *softwares*, componentes e licenças de software e serviços de instalação.

16.3 A comprovação exigida acima se dará por meio de manuais técnicos, declaração (ões) do(s) fabricantes(s) ou outros meios documentais, de que os *softwares* e equipamentos ofertados atendem todos os requisitos especificados neste Termo de Referência, os quais poderão ser apresentados em papel ou em mídia eletrônica.

16.4 Deverão constar nos documentos acima citados as demais informações referentes às dimensões físicas, quantidade de U's para instalação em rack, necessidade de espaço de guarda, mecanismo de refrigeração, consumo de energia, dissipação térmica e peso que demonstrem o atendimento aos requisitos técnicos estabelecidos neste documento.

16.5 A licitante deverá apresentar, juntamente com a proposta, o ANEXO D para avaliação do atendimento aos requisitos técnicos e aprovação pelo grupo técnico de apoio ao DEIST/STI que dará apoio ao pregoeiro.

16.6 Indicar o(s) sítio na Internet do(s) fabricante(s) do(s) produto(s).

16.7 No caso de entender tais documentos como insuficientes para a análise, poderá o pregoeiro, suportado pelo grupo técnico de apoio ao DEIST/STI, solicitar complementação a ser apresentada em até 48 horas, e/ou realizar diligência(s) para obter informações mais detalhadas sobre os produtos ofertados, conforme previsto no parágrafo § 3º do Art. 43 da Lei nº 8.666/93.

16.8 As propostas devem conter toda documentação necessária para subsidiar o julgamento técnico das soluções ofertadas pelo órgão pregoeiro, suportado pelo grupo técnico de apoio ao DEIST/STI, incluindo manuais técnicos e outros documentos que a LICITANTE julgar necessário.

16.9 Todas as exigências feitas em relação à proposta de preços devem ser atendidas, sob pena de desclassificação da proposta.

16.10 A proposta de preços deverá ser redigida em língua portuguesa, datilografada ou digitada, em uma via, sem emendas, rasuras, entrelinhas ou ressalvas, devendo a última folha ser assinada e as demais rubricadas pelo representante legal da licitante.

16.11 Após aceitação da proposta, o pregoeiro solicitará à licitante que apresente uma AMOSTRA, juntamente com o CADERNO DE TESTES que deverá ser analisado pelo grupo técnico de apoio ao DEIST/STI de acordo com o descrito no ANEXO E.

16.12 A exigência da AMOSTRA visa à aferição da real capacidade técnica dos equipamentos ofertados pela licitante. Busca-se comprovar tecnicamente, juntamente com a documentação do fabricante, se os equipamentos de fato atendem aos requisitos constantes nas especificações técnicas do ANEXO B. Nesse sentido, os testes poderão ser efetuados em todos ou em determinados itens do lote.

16.13 A aprovação da comprovação por escrito da documentação técnica, bem como das AMOSTRAS e do CADERNO DE TESTE pela equipe técnica de apoio ao pregoeiro são condições necessárias para a adjudicação do vencedor da licitação.

17 QUALIFICAÇÃO TÉCNICA

17.1 A LICITANTE deverá apresentar o(s) atestado(s), emitido por pessoa jurídica de direito público ou privado, que comprove(m) que a LICITANTE já forneceu satisfatoriamente soluções de segurança compatíveis com o objeto. Em virtude do mecanismo de compras compartilhadas ora adotado pelo MP e pela possibilidade de fornecimento simultâneo aos diversos órgãos da Administração Pública, participantes do certame ou não, exige-se o fornecimento de atestado de capacidade técnica que comprove a entrega, instalação e manutenção/assistência técnica dos equipamentos e softwares que compõe a solução, objeto deste Termo de Referência, conforme quantitativo mínimo definido por lote, na tabela abaixo.

Tabela 4 – Comprovação por Atestado de Quantitativo Mínimo para o Lote.

Descrição dos Equipamentos a serem fornecidos		**Descrição dos Equipamentos compatíveis que deverão constar do(s) Atestado(s)**	**Quantidade Total dos Equipamentos do Lote**
Lote 1	Firewall Multifuncional	Firewall multifuncional de mesmo tamanho de throughput que atenda as especificações desse lote	15

Lote 2	Firewall Multifuncional	Firewall multifuncional de mesmo tamanho de throughput que atenda as especificações desse lote ou superiores	10
Lote 3	Firewall Multifuncional	Firewall multifuncional de mesmo tamanho de throughput que atenda as especificações desse lote ou superiores	6
Lote 4	Firewall Multifuncional	Firewall multifuncional com tamanho de throughput que atenda as especificações do lote ou superior	3
Lote 5	Firewall Multifuncional	Firewall multifuncional com tamanho de throughput que atenda as especificações do lote	2

17.2 Para comprovação de atendimento ao item 17.1 será permitida a soma de atestados separados a fim de alcançar a quantidade mínima exigida na tabela 4.

18 TESTES DE CONFORMIDADE

18.1 Conforme ANEXO “E” deste Termo de Referência..

19 DA VIGÊNCIA DA ATA E DO(S) CONTRATO(S)

19.1 A Ata de registro de Preços terá vigência de 12 (doze) meses.

19.2 O(s) contrato(s) terá(ão) vigência de até 60 (sessenta) meses, a contar da data de sua assinatura.

20 DA FISCALIZAÇÃO

20.1 A CONTRATANTE designará responsável para acompanhar e fiscalizar a execução do contrato, que registrará em relatório todas as ocorrências relacionadas com

a sua execução, determinando o que for necessário à regularização das falhas ou defeitos observados, conforme definido no art. 67 da Lei nº 8.666/93 e nas especificações de níveis mínimos de serviço definidos neste Termo de Referência.

Equipe de Planejamento da Contratação		
Integrante Técnico	**Integrante Requisitante**	**Integrante Administrativo**
_____	_____	_____

Brasília, de 2016.

Aprovo o presente Termo de Referência, conforme proposto.

Brasília, de 2016.

Secretário

ANEXO A DO TERMO DE REFERÊNCIA

PLANILHA DE QUANTITATIVOS E PREÇOS UNITÁRIOS MÁXIMOS,
(QUANTIDADES E PREÇO TOTAL ESTIMADO PARA O LOTE)

ANEXO B DO TERMO DE REFERÊNCIA

ESPECIFICAÇÕES TÉCNICAS

1 LOTES

1.1 Relação dos lotes

1.1.1 A tabela abaixo apresenta a descrição dos itens dos lotes que podem ser adquiridos na ata de contratação conjunta. O detalhamento dos itens encontra-se descrito nos tópicos 2 – Especificações e 3- Definição dos Lotes e Itens

1.1.2 Os itens 1 dos Lotes 1,2,3,4 e 5 são de aquisição obrigatória tanto para partícipes da ata quanto para órgãos que façam a aquisição como não participantes.

Lote	Item	Descrição	Quantidade
1	Item 1	Firewall multifuncional Tipo 1	A definir
	Item 2	Conjunto de funcionalidades IPS/IDS	A definir
	Item 3	Conjunto de funcionalidades anti-virus e anti-malware	A definir
	Item 4	Conjunto de funcionalidades para tratamento de conteúdo web	A definir
	Item 5	Conjunto de funcionalidades para controle de aplicações e analise profunda	A definir
	Item 6	Treinamento oficial para 5 pessoas	A definir
	Item 7	Solução de gerência centralizada	
2	Item 1	Firewall multifuncional Tipo 2	A definir
	Item 2	Conjunto de funcionalidades IPS/IDS	A definir
	Item 3	Conjunto de funcionalidades anti-virus e anti-malware	A definir
	Item 4	Conjunto de funcionalidades para tratamento de conteúdo web	A definir
	Item 5	Conjunto de funcionalidades para controle de aplicações e analise profunda	A definir
	Item 6	Treinamento oficial para 5 pessoas	A definir
	Item 7	Solução de gerência centralizada	
3	Item 1	Firewall multifuncional Tipo 3	A definir
	Item 2	Conjunto de funcionalidades IPS/IDS	A definir
	Item 3	Conjunto de funcionalidades anti-virus e anti-malware	A definir
	Item 4	Conjunto de funcionalidades para tratamento de conteúdo web	A definir
	Item 5	Conjunto de funcionalidades para controle de aplicações e analise profunda	A definir
	Item 6	Treinamento oficial para 5 pessoas	A definir
	Item 7	Solução de gerência centralizada	
4	Item 1	Firewall multifuncional Tipo 4	A definir
	Item 2	Conjunto de funcionalidades IPS/IDS	A definir
	Item 3	Conjunto de funcionalidades anti-virus e anti-malware	A definir

	Item 4	Conjunto de funcionalidades para tratamento de conteúdo web	A definir
	Item 5	Conjunto de funcionalidades para controle de aplicações e analise profunda	A definir
	Item 6	Treinamento oficial para 5 pessoas	A definir
	Item 7	Solução de gerência centralizada	
5	Item 1	Firewall multifuncional Tipo 5	A definir
	Item 2	Conjunto de funcionalidades IPS/IDS	A definir
	Item 3	Conjunto de funcionalidades anti-virus e anti-malware	A definir
	Item 4	Conjunto de funcionalidades para tratamento de conteúdo web	A definir
	Item 5	Conjunto de funcionalidades para controle de aplicações e analise profunda	A definir
	Item 6	Treinamento oficial para 5 pessoas	A definir
	Item 7	Solução de gerência centralizada	A definir

2. ESPEFICIFAÇÕES

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

2.1.1 Todos os equipamentos *firewall* e a solução de gerência integrada devem ser do mesmo fabricante, inclusive os sistemas operacionais executados por esses equipamentos, observado, para o caso dos equipamentos *firewall*, o disposto no item 2.1.11.

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

2.1.3 Não serão aceitos equipamentos em modo End of Life ou End of Support durante a vigência do contrato, estas informações deverão estar no site do fabricante.

2.1.4 O equipamento deverá atualizar *firmeware* e *softwares* para novas versões durante 60 (sessenta) meses, estas informações deverão estar no site do fabricante.

2.1.5 Todas as portas de comunicação, interfaces e afins deverão estar habilitadas, operacionais e prontas para operação, sem custos adicionais.

2.1.6 Todas as licenças de *hardware* e *software* devem ser fornecidas em caráter perpétuo, atualizadas em suas últimas versões disponíveis, não

sendo permitida a cobrança de quaisquer valores adicionais pelo uso dos *hardwares* e *softwares* durante o contrato ou após o seu término.

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

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

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

2.1.10 O equipamento deve ser fornecido com todas as suas portas de comunicação, interfaces e afins habilitadas, operacionais e prontas para operação, inclusive com seus respectivos transceivers instalados, sem custos adicionais.

2.1.11 Fornecido em *hardware* dedicado tipo *appliance* ou chassi, com sistema operacional otimizado, do mesmo fabricante, para o uso como *firewall* multifunção.

2.1.11.1 Os equipamentos dos lotes 1, 2, 3 e 4 da solução ofertada, não deverá exceder 4 Unit Rack individualmente, sendo “caixas” únicas, ou seja, sem empilhamentos.

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

2.1.12 Deve possuir fonte(s) de energia no próprio equipamento.

2.1.13 Suportar topologias de *cluster* redundante de alta disponibilidade (*failover*) nos modos ativo-ativo e ativo-passivo, com sincronização, em tempo real, de configuração e de estados das conexões. No caso de falha de um dos equipamentos do *cluster*, não deverá haver perda das configurações e nem das conexões já estabelecidas e a transição entre os equipamentos deverá acontecer de forma transparente para o usuário.

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

2.1.15 Possuir controle de acesso por endereço IP de origem e destino, por aplicação (independentemente da porta ou protocolo utilizados pela aplicação), por sub-rede e por períodos do dia, permitindo a aplicação de regras por horários e por dias da semana.

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

2.1.17 Suportar tags de VLAN;

2.1.18 Permitir a criação de, no mínimo, 500 VLANs padrão 802.1q;

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

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

2.1.21 Suportar agregação de *links*, segundo padrão IEEE 802.3ad;

2.1.22 Possuir ferramenta de diagnóstico do tipo *tcpdump*;

2.1.23 Não deve possuir restrições ao número de máquinas ou usuários protegidos, salvo pela capacidade do equipamento.

2.1.24 Suportar integração com serviços de diretório LDAP, Microsoft *Active Directory*, RADIUS e senha do sistema operacional no próprio *firewall* para identificação, autenticação e registros de logs, sem limite de número de usuários em relação ao licenciamento;

2.1.25 Deve identificar de forma transparente os usuários autenticados por *single sign-on*, inclusive por meio de serviço de diretório, compatível no mínimo com as seguintes ferramentas: Microsoft Active Directory, de servidores RADIUS Microsoft Network Policy Server e OpenLDAP.

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

2.1.27 Não será permitida a utilização de agentes instalados nos servidores LDAP, Active Directory, RADIUS, Kerberos e proxies internos, e nem nos equipamentos dos usuários.

2.1.28 Deve registrar a identificação do usuário em todos os logs de eventos de acesso ou de ameaças gerados pelo equipamento.

2.1.29 Possuir métodos de autenticação de usuários para aplicações executadas sobre os protocolos TCP e UDP como, por exemplo, aplicações HTTP, HTTPS, FTP;

2.1.30 Suportar *Network Address Translation* (NAT 1-1, NAT 1-N, NAT N-1) de acordo com a RFC3022, nos modo estático e dinâmico;

2.1.31 Deve suportar NAT64.

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

2.1.33 Suportar nativamente IPv6 e tráfego de IPv6 tunelado em pacotes Ipv4;

2.1.33.1 Suportar, no mínimo, os protocolos de roteamento dinâmico RIP v2 e NG, OSPF v2 e v3, MPLS e BGP, bem como as funcionalidades de roteamento estático e roteamento policy-based, inclusive IPv6;

2.1.34 Suportar os protocolos IGMP v2, IGMP v3 e PIM-SM;

2.1.35 Possuir funcionalidades de DHC *client*, *server* e r*elay*;

2.1.36 Possuir proteção e suporte a protocolos de Real Time, contemplando no mínimo: Real Time Transport Protocol (RTP), RTCP, RTMP, RTSP, H323, SIP, tanto em IPv4 quanto em IPv6.

2.1.37 Possuir tecnologia de *firewall stateful*;

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

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

2.1.40 Suportar sincronização de horário por NTP;

2.1.41 Possuir funcionalidade de geração de relatórios e exportação de logs;

2.1.42 Deve suportar, no mínimo, a operação em modo *gateway* e transparente;

2.1.43 Suportar, no mínimo, 1.000 regras ou políticas de firewall;

2.1.44 Permitir a abertura de novas portas por fluxo de dados para serviços que requerem portas dinâmicas;

2.1.45 Possuir mecanismo de *anti-spoofing*;

2.1.46 Possuir funcionalidade de exceção em SSL Inspection para sites e aplicações bancárias, não decriptando o tráfego dessas conexões.

2.1.47 Possuir inspeção profunda de pacotes para tráfego critpografado (no mínimo em tráfego VPN e HTTPS);

2.1.48 Possuir, no mínimo, suporte a SNMPv2 e v3;

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

2.1.50 Possuir suporte a, no mínimo, dois algoritmos de balanceamento de carga para novas conexões de rede a servidores internos;

2.1.51 Possuir conexão criptografada entre estação de gerência e o equipamento, tanto em interface gráfica quanto em interface por linha de comando;

2.1.52 Deve criptografar e autenticar a comunicação com a solução de gerenciamento centralizado.

2.1.53 Permitir o gerenciamento remoto do equipamento por meio da rede local ou WAN e pela solução de gerenciamento centralizado;

2.1.54 Possuir gerenciamento gráfico centralizado das funcionalidades de *firewall* e monitoramento de seus eventos de forma integrada ao gerenciamento centralizado da solução. Deve também permitir o gerenciamento dos processos associados por meio de *CLI (command-line interface);*

2.1.55 Deve identificar os países de origem e destino de todas as conexões estabelecidas através do equipamento.

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

2.1.57 Deve possibilitar a visualização dos países de origem e destino nos logs de eventos de acessos e ameaças.

2.1.58 Funcionalidades de gerência local do *firewall* ou do *cluster* (virtual ou físico) do qual o *firewall* faz parte:

2.1.58.1 Deve suportar, por meio da interface gráfica de gerenciamento, a criação e administração de políticas, filtragem de URLs, monitoração de logs e captura de pacotes.

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

2.1.58.3 Deve permitir a delegação de funções de administração.

2.1.58.4 Deve registrar em log as ações dos usuários administradores.

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

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

2.1.58.7 Deve possibilitar o gerenciamento (incluindo a criação, alteração, monitoração e exclusão) de objetos de rede. Deverá ainda permitir detectar se e onde, na base de regras, está sendo utilizado determinado objeto de rede. Os tipos de objetos deverão permitir especificar de forma distinta grupos e objetos de rede e serviços, diferenciando-os e agrupando-os conforme suas características ou

descrição de maneira a permitir o reaproveitamento dos mesmos em diferentes políticas.

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

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

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

2.1.58.11 Deve prover funcionalidade para análise e auditoria de regras com capacidade de detectar regras conflitantes ou regras equivalentes.

2.1.58.12 Deve suportar a geração de alertas automáticos via email, SNMP e syslog.

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

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

2.1.58.15 Deve informar o número de conexões simultâneas e de novas conexões por segundo dos equipamentos gerenciados.

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

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

2.1.60 Deve possuir gerenciamento gráfico centralizado das funcionalidades de QoS/Trafic Shapping integrado com gerenciamento centralizado da solução*;*

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

2.1.62 As funcionalidades de VPN não podem possuir qualquer restrição de licenciamento, inclusive em relação ao número de clientes, IPs e máquinas.

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

2.1.64 Deve permitir a criação de túneis VPN SSL/TLS;

2.1.65 Deve permitir a criação de túneis VPN IPSec;

2.1.66 A funcionalidade de VPN prevista no item anterior poderá ser atendida por meio de dispositivo *standalone*, caso o *appliance* do *firewall* não possua tal funcionalidade, sem prejuízo do gerenciamento centralizado da solução previsto nos itens 2.1.81 e 2.2;

2.1.67 Deve permitir que o usuário realize a conexão por meio de cliente instalado no sistema operacional do seu equipamento ou por meio de interface *Web* do tipo portal, devendo o cliente instalável estar disponível, no mínimo, para os sistemas operacionais Windows (Vista, 7, 8 e 10), Linux, Mac OS X e para os sistemas móveis Apple iOS e Google Android. O acesso por meio da interface *Web* deverá ser compatível com, no mínimo, os navegadores Internet Explorer 7 ou superior, Firefox 3.6 ou superior;

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

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

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

2.1.71 Suportar os algoritmos RSA, *Diffie-Hellman/*RSA;

2.1.72 Suportar Certificado Digital X.509 v3;

2.1.73 Suportar a inclusão (*enrollment*) de autoridades certificadoras;

2.1.74 Permitir alteração dos algoritmos criptográficos da VPNs permitindo a inserção de criptografia de estado.

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

2.1.76 Suportar os protocolos de roteamento RIPv2, RIP NG, OSPFv2 e OSPFv3 para as funcionalidades de VPN;

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

2.1.78 Suportar certificados emitidos por autoridade certificadora no padrão ICP-Brasil;

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

2.1.80 Suportar NAT *Transversal Tunneling* (NAT-T);

2.1.81 Possuir gerenciamento gráfico centralizado das funcionalidades de VPN e monitoramento de seus eventos de forma integrada ao gerenciamento centralizado da solução. Deve também permitir o gerenciamento dos processos associados por meio de *CLI (command-line interface);*

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

2.1.83 Deve permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis de SSL.

2.1.84 O equipamento deve ser apropriado para o uso em ambiente tropical com umidade relativa na faixa de 10 a 90% (sem condensação) e temperatura ambiente na faixa de 0 a 40°C.

2.2 Solução de gerência centralizada

2.2.1 Deverá ser fornecida solução gerenciável do mesmo fabricante externamente ao equipamento. Podendo ser um "appliance especializado" – equipamento especializado para gerência centralizada ou "appliance virtual" - solução de software baseada em máquina virtual que possa ser instalado e executado em ambientes virtuais, tais como: VMware vSphere, Xen, KVM and Hyper-V platforms.

2.2.1.1 Quando executado em ambientes virtuais, deverão ser fornecidas e implantadas, em caráter perpétuo, todas as licenças dos *softwares* e sistemas operacionais necessários ao funcionamento da solução.

2.2.2 Deve estar licenciada e permitir a gerência centralizada de todos os equipamentos e contextos virtuais que compõem a solução de alta disponibilidade.

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

2.2.4 Deve estar licenciada e permitir a correlação de todos os eventos gerados por todos os equipamentos e contextos virtuais que compõe a solução de alta disponibilidade.

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

2.2.6 Deve permitir a criação de relatórios customizados.

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

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

2.2.9 Deve permitir a geração automática e agendada dos relatórios.

2.2.10 Deve automatizar o sincronismo de regras, objetos e políticas em tempo real.

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

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

2.2.13 Deve permitir distribuição centralizada de pacotes de atualização.

2.2.14 Deve permitir validar as regras antes de aplicá-las.

2.3 Conjunto de funcionalidades IPS/IDS

2.3.1 Possuir tecnologia de detecção baseada em assinatura;

2.3.2 Possuir no mínimo um conjunto de 2.000 assinaturas de detecção e prevenção de ataques, permitindo também ataques baseados em anamolias;

2.3.3 Decodificar múltiplos formatos de *Unicode*;

2.3.4 Suportar fragmentação e desfragmentação IP;

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

2.3.6 Detectar e Proteger contra, no mínimo, os ataques de RPC (*Remote Procedure Call*), Windows ou NetBios, SMTP (*Simple Message*

Transfer Protocol), IMAP (*Internet Message Access Protocol*), *Sendmail* ou POP (*Post Office Protocol*), DNS (*Domain Name System*), FTP, SSH , Telnet, ICMP (*Internet Control Message Protocol*), SIP, SNMP, SSDP, CHARGEN, RDP (*Remote Desktop Protocol*), DoS (*Denial of Service*) e ataques com assinaturas complexas, tais como ataques *TCP hijacking*.

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

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

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

2.3.10 Atualizar automaticamente as assinaturas para o sistema de detecção de intrusos;

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

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

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

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

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

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

2.3.17 Possuir as estratégias de bloqueio, liberar e bloquear, sendo este suportando quarentenar o IP, selecionáveis tanto por conjuntos de assinaturas quanto por cada assinatura;

2.3.18 Suportar a verificação de ataques na camada de aplicação;

2.3.19 Possuir gerenciamento gráfico centralizado das funcionalidades de IPS/IDS e monitoramento de seus eventos de forma integrada ao gerenciamento centralizado da solução. Deve também permitir o gerenciamento dos processos associados por meio de *CLI (command-line interface);*

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

2.3.21 Taxa mínima de detecção de 80% (oitenta), tendo no máximo 15% (quinze) de falso positivo.

2.4 Conjunto de funcionalidades anti-virus e anti-malware

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

2.4.2 Possuir funcionalidade de varredura contra vírus e *malwares* em tráfego HTTPS, HTTP, FTP, POP3, IMAP e SMTP;

2.4.3 Deve ser capaz de, se houver algum atraso ou falha na realização da atualização automática, o equipamento deve ter a capacidade de alertar imediatamente o administrador através de *logs*, SNMP e *e-mail*;

2.4.4 Deve possuir serviço de atualização automática e manual de assinaturas com o fabricante;

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

2.4.6 Possuir gerenciamento gráfico centralizado das funcionalidades de antivírus e *anti-malware* integrado com gerenciamento centralizado da solução. Deve também permitir o gerenciamento dos processos associados por meio de *CLI (command-line interface);*

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

2.4.8 Taxa mínima de detecção de 80% (oitenta), tendo no máximo 15% (quinze) de falso positivo.

2.5 Conjunto de funcionalidades para tratamento de conteúdo web

2.5.1 Possuir base mínima contendo 10 (dez) milhões de *sites* internet *web* já registrados e classificados, distribuídos em, no mínimo, 40 (quarenta) categorias ou subcategorias pré-definidas;

2.5.2 Permitir a criação de categorias personalizadas;

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

2.5.4 Prover o funcionamento mínimo do *engine* de filtragem *web* mesmo que a comunicação com o *site* do fabricante esteja fora de operação;

2.5.5 Suportar filtragem e categorização das URLs, mesmo sem conectividade com a Internet.

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

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

2.5.8 Permitir a criação de regras para acesso/bloqueio por endereço IP de origem e sub-rede de origem;

2.5.9 Permitir a criação de quotas de utilização por categorias;

2.5.10 Capacidade de exibir mensagem de bloqueio customizável pelos Administradores para resposta aos usuários, na tentativa de acesso a recursos proibidos ou restringidos pela política de segurança do órgão;

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

2.5.12 Permitir o bloqueio de URLs inválidas cujo campo CN ou DN do certificado SSL não contém um domínio válido;

2.5.13 Permitir o bloqueio de páginas web por classificação, como páginas que facilitam a busca de áudio, vídeo, imagem, URLs originadas de *spam* e sites de *proxys* anônimos;

2.5.14 Permitir a criação de listas personalizadas de URLs permitidas – lista branca e bloqueadas – lista negra;

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

2.5.16 Categorizar as URLs com taxa de acerto mínima de 85% (oitenta e cinco), tendo no máximo 20% de categorização como desconhecida.

2.5.17 Suportar e forçar pesquisas seguras em sistemas de buscas, comtemplando no mínimo, Google, Bing e Yahoo.

2.6 Conjunto de funcionalidades para controle de aplicações e análise profunda

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

2.6.2 Deve ser capaz de identificar se as aplicações estão utilizando sua porta default.

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

2.6.4 Deve ser capaz de identificar aplicações criptografadas usando SSL.

2.6.5 Permitir o agrupamento de aplicações em grupos personalizados;

2.6.6 Garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações;

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

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

2.6.9 Possuir política de segurança de aplicações pré-configuradas na solução;

2.6.10 Possuir atualização manual e automática de novas assinaturas;

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

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

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

2.6.14 Categorizar as aplicações com taxa de acerto mínima de 85% (oitenta e cinco), tendo no máximo 30% (trinta) de categorização como desconhecida.

2.7 Treinamento oficial para 5 pessoas

2.7.1 Voucher para treinamento oficial do fabricante.

2.7.2 A carga horária mínima do treinamento não poderá ser inferior a 40 horas, a turma conterá 5 pessoas e a ementa deverá contemplar, no mínimo.

2.7.3 Os treinamentos deverão ser realizados no Brasil, em português, em local fornecido pela CONTRATADA, em qualquer uma das capitais das Unidades da Federação a ser indicada pela CONTRATANTE. O local de treinamento deverá possuir todas as facilidades para um perfeito desempenho das atividades incluindo os recursos áudio visuais e laboratórios necessários, sem ônus algum para a CONTRATANTE.

2.7.4 Caberá à CONTRATADA prover todos os recursos didáticos necessários à realização do treinamento, incluindo, sala de aula, datashow, apostilas, bloco de anotações e caneta para cada treinando em cada turno de treinamento.

2.7.5 Os treinamentos deverão ocorrer usando-se dois turnos diários de até 4 horas cada, com intervalos de 15 minutos em cada turno e 1 hora entre os turnos.

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

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

2.7.8 São produtos esperados de todos os treinamentos:

2.7.8.1 Aulas presenciais teóricas e práticas.

2.7.8.2 Material didático contratado e aprovado pela CONTRATANTE.

2.7.8.3 Referências para estudos e pesquisas complementares.

2.7.9 A CONTRATANTE poderá, a seu critério, reproduzir o material didático usado e treinar multiplicadores para repetir o treinamento sem custos adicionais.

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

2.7.11 O valor unitário do treinamento refere-se ao custo para a turma completa de 5 treinandos.

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

3. DEFINIÇÃO DOS LOTES E ITENS

3.1 **LOTE 1** – **item 1:** Firewall multifuncional Tipo 1

3.1.1 Requisitos específicos:

3.1.1.1 Possuir todas as funcionalidades descritas no item 2.1;

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

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

3.1.1.4 Possuir disco rígido com capacidade mínima de 16 GB SSD para armazenamento de logs.

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

3.1.1.6 Vazão de 50 Mbps para IPSec VPN throughput.

3.1.1.7 Quantidade de sessões simultâneas 64.000.

3.1.1.8 Quantidade de novas sessões por segundo 7.500.

3.2 **LOTE 1** – **item 2:** Conjunto de funcionalidades IPS/IDS

3.2.1 Requisitos específicos:

3.2.1.1 Possuir todas as funcionalidades descritas no item 2.3;

3.3 **LOTE 1** – **item 3:** Conjunto de funcionalidades anti-virus e anti-malware

3.3.1 Requisitos específicos:

3.3.1.1 Possuir todas as funcionalidades descritas no item 2.4;

3.4 **LOTE 1** – **item 4:** Conjunto de funcionalidades para tratamento de conteúdo web

3.4.1 Requisitos específicos:

3.4.1.1 Possuir todas as funcionalidades descritas no item 2.5;

3.5 **LOTE 1** – **item 5:** Conjunto de funcionalidades para controle de aplicações e análise profunda

3.5.1 Requisitos específicos:

3.5.1.1 Possuir todas as funcionalidades descritas no item 2.1.47 e no item 2.6;

3.6 **LOTE 1 – item 6:** Treinamento oficial para 5 pessoas

3.6.1 Requisitos específicos:

3.6.1.1 Atender a tudo que foi exposto no item 2.7;

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

3.7.1 Requisitos específicos:

3.7.1.1 Possuir todas as funcionalidades descritas no item 2.2;
3.7.1.2 Possui capacidade mínima para armazenamento de logs de 200 MB.

3.8 **LOTE 2** – **item 1:** Firewall multifuncional Tipo2

3.8.1 Requisitos específicos:

3.8.1.1 Possuir todas as funcionalidades descritas no item 2.1;

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

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

3.8.1.4 Possuir disco rígido com capacidade mínima de 64 GB SSD para armazenamento de logs.

3.8.1.5 Quantidade de sessões simultâneas 250.000.

3.8.1.6 Quantidade de novas sessões por segundo 50.000.

3.8.1.7 Vazão de 50 Mbps para IPSec VPN throughput.

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

3.9.1 Requisitos específicos:

3.9.1.1 Possuir todas as funcionalidades descritas no item 2.3;

3.10 **LOTE 2** – **item 3:** Conjunto de funcionalidades anti-virus e anti-malware

3.10.1 Requisitos específicos:

3.10.1.1 Possuir todas as funcionalidades descritas no item 2.4;

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

3.11.1 Requisitos específicos:

3.11.1.1 Possuir todas as funcionalidades descritas no item 2.5;

3.12 **LOTE 2** – **item 5:** Conjunto de funcionalidades para controle de aplicações e analise profunda

3.12.1 Requisitos específicos:

3.12.1.1 Possuir todas as funcionalidades descritas no item 2.1.47 e no item 2.6;

3.13 **LOTE 2 – item 6:** Treinamento oficial para 5 pessoas

3.13.1 Requisitos específicos:

3.13.1.1 Possuir todas as funcionalidades descritas no item 2.7;

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

3.14.1 Requisitos específicos:

3.14.1.1 Possuir todas as funcionalidades descritas no item 2.2;
3.14.1.2 Possui capacidade mínima para armazenamento de logs de 500 MB.

3.15 **LOTE 3** – **item 1:** Firewall multifuncional Tipo3

3.15.1 Requisitos específicos:

3.15.1.1 Possuir todas as funcionalidades descritas no item 2.1;

3.15.1.2 Possuir no mínimo o throughput de 1 Gbps para todas as funcionalidades dos itens 2.1, 2.2, 2.3, 2.4, 2.5, 2.6 ligadas simultaneamente com inspeção integral de todos os pacotes de dados, independentemente de seu tamanho ou direção de fluxo levando-se em consideração o perfil de tráfego descrito no ANEXO E.

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

3.15.1.4 Possuir no mínimo 4 (quatro) portas SPF e 6 (seis) portas 10/100/100 BASE T, sendo 01 (uma) utilizada para gerência.

3.15.1.5 Possuir disco rígido com capacidade mínima de 120 GB SSD para armazenamento de logs.

3.15.1.6 Virtualização mínima de 150 VDOMs.

3.15.1.7 Quantidade de sessões simultâneas 500.000.

3.15.1.8 Quantidade de novas sessões por segundo 50.000.

3.15.1.9 IPSec VPN throughput 300 Mbps

3.16 **LOTE 3** – **item 2:** Conjunto de funcionalidades IPS/IDS

3.16.1 Requisitos específicos:

3.16.1.1 Possuir todas as funcionalidades descritas no item 2.3;

3.17 **LOTE 3** – **item 3:** Conjunto de funcionalidades anti-virus e anti-malware

3.17.1 Requisitos específicos:

3.17.1.1 Possuir todas as funcionalidades descritas no item 2.4;

3.18 **LOTE 3** – **item 4:** Conjunto de funcionalidades para tratamento de conteúdo web

3.18.1 Requisitos específicos:

3.18.1.1 Possuir todas as funcionalidades descritas no item 2.5;

3.19 **LOTE 3** – **item 5:** Conjunto de funcionalidades para controle de aplicações e analise profunda

3.19.1 Requisitos específicos:

3.19.1.1 Possuir todas as funcionalidades descritas no item 2.1.47 e no item 2.6;

3.20 **LOTE 3 – item 6:** Treinamento oficial para 5 pessoas

3.20.1 Requisitos específicos:

3.20.1.1 Possuir todas as funcionalidades descritas no item 2.7;

3.21 **LOTE 3 – item 7:** Solução de gerência centralizada

3.21.1 Requisitos específicos:

3.21.1.1 Possuir todas as funcionalidades descritas no item 2.2;
3.21.1.2 Possui capacidade mínima para armazenamento de logs de 1 TB.

3.22 **LOTE 4** – **item 1:** Firewall multifuncional Tipo4

3.22.1 Requisitos específicos:

3.22.1.1 Possuir todas as funcionalidades descritas no item 2.1;

3.22.1.2 Possuir no mínimo o throughput de 4 Gbps para todas as funcionalidades dos itens 2.1, 2.2, 2.3, 2.4, 2.5, 2.6 e 2.8 ligadas simultaneamente com inspeção integral de todos os pacotes de dados, independentemente de seu tamanho ou direção de fluxo levando-se em consideração o perfil de tráfego descrito no ANEXO E.

3.22.1.3 O equipamento deve possuir 2 (duas) fontes internas de alimentação independentes, redundantes e hot-swappable, com alimentação nominal de 100~120VAC e 210~230VAC e frequência de 50 ou 60 Hz, ou auto-ranging. Deverá vir acompanhado de cabo de alimentação com, no mínimo, 1,80m (6 pés), com plug tripolar 2P+T no padrão ABNT NBR 14136.

3.22.1.4 Possuir no mínimo 6 (seis) portas 10/100/1000, sendo 01 (uma) utilizada para gerência, 6 (seis) portas GbE SFP e 2 (duas) portas 10 SFP+.

3.22.1.5 Possuir disco rígido com capacidade mínima de 120 GB SSD para armazenamento de logs.

3.22.1.6 Fontes de alimentações internas redundantes.

3.22.1.7 Virtualização mínima de 5 VDOMs.

3.22.1.8 Quantidade de sessões simultâneas 2.000.000.

3.22.1.9 Quantidade de novas sessões por segundo 120.000.

3.22.1.10 IPSec VPN throughput 600 Mbps

3.23 **LOTE 4** – **item 2:** Conjunto de funcionalidades IPS/IDS

3.23.1 Requisitos específicos:

3.23.1.1 Possuir todas as funcionalidades descritas no item 2.3;

3.24 **LOTE 4** – **item 3:** Conjunto de funcionalidades anti-virus e anti-malware

3.24.1 Requisitos específicos:

3.24.1.1 Possuir todas as funcionalidades descritas no item 2.4;

3.25 **LOTE 4** – **item 4:** Conjunto de funcionalidades para tratamento de conteúdo web

3.25.1 Requisitos específicos:

3.25.1.1 Possuir todas as funcionalidades descritas no item 2.5;

3.26 **LOTE 4** – **item 5:** Conjunto de funcionalidades para controle de aplicações e analise profunda

3.26.1 Requisitos específicos:

3.26.1.1 Possuir todas as funcionalidades descritas no item 2.1.47 e no item 2.6;

3.27 **LOTE 4 – item 6:** Treinamento oficial para 5 pessoas

3.27.1 Requisitos específicos:

3.27.1.1 Possuir todas as funcionalidades descritas no item 2.7;

3.28 **LOTE 4 – item 7:** Solução de gerência centralizada

3.28.1 Requisitos específicos:

3.28.1.1 Possuir todas as funcionalidades descritas no item 2.2;
3.28.1.2 Possui capacidade mínima para armazenamento de logs de 2 TB.

3.29 **LOTE 5** – **item 1:** Firewall multifuncional Tipo 5

3.29.1 Requisitos específicos:

3.29.1.1 Possuir todas as funcionalidades descritas no item 2.1;

3.29.1.2 Possuir no mínimo o throughput de 10 Gps para todas as funcionalidades dos itens 2.1, 2.2, 2.3, 2.4, 2.5, 2.6 e 2.8 ligadas simultaneamente com inspeção integral de todos os pacotes de dados, independentemente de seu tamanho ou direção de fluxo levando-se em consideração o perfil de tráfego descrito no ANEXO E.

3.29.1.3 O equipamento deve possuir 2 (duas) fontes internas de alimentação independentes, redundantes e hot-swappable, com alimentação nominal de 100~120VAC e 210~230VAC e frequência de 50 ou 60 Hz, ou auto-ranging. Deverá vir acompanhado de cabo de alimentação com, no mínimo, 1,80m (6 pés), com plug tripolar 2P+T no padrão ABNT NBR 14136.

3.29.1.4 Possuir no mínimo 4 (quatro) portas de 10 Gbps SPF+, 6 (seis) portas SPF e 6 (seis) portas 10/100/1000 Mbps BASE T, sendo 01 (uma) utilizada para gerência.

3.29.1.5 Possuir disco rígido com capacidade mínima de 240 GB SSD para armazenamento de logs.

3.29.1.6 Fontes de alimentação internas redundantes.

3.29.1.7 Virtualização mínima de 150 VDOMs.

3.29.1.8 Quantidade de sessões simultâneas 4.000.000.

3.29.1.9 Quantidade de novas sessões por segundo 120.000.

3.29.1.10 IPSec VPN throughput 1,5 Gbps

3.30 **LOTE 5** – **item 2:** Conjunto de funcionalidades IPS/IDS

3.30.1 Requisitos específicos:

3.30.1.1 Possuir todas as funcionalidades descritas no item 2.3;

3.31 **LOTE 5** – **item 3:** Conjunto de funcionalidades anti-virus e anti-malware

3.31.1 Requisitos específicos:

3.31.1.1 Possuir todas as funcionalidades descritas no item 2.4;

3.31.1.2 Possuir suporte nativo para a funcionalidade de APT (Advanced Persistent Threat) e Zero Day através de ativação de licenciamento.

3.31.1.3 Entende-se por funcionalidade de APT (Advanced Persistent Threat) e Zero Day. Deve possuir capacidade de emular (sandbox) ataques em diferetnse sistemas operacionais, tais como: Windows XP e Windows 7 assim como Office 2003, 2010 e 2013. A tecnologia de máquina virtual deverá possuir diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso sem utilização de assinaturas.

3.32 **LOTE 5** – **item 4:** Conjunto de funcionalidades para tratamento de conteúdo web

3.32.1 Requisitos específicos:

3.32.1.1 Possuir todas as funcionalidades descritas no item 2.5;

3.33 **LOTE 5** – **item 5:** Conjunto de funcionalidades para controle de aplicações e analise profunda

3.33.1 Requisitos específicos:

3.33.1.1 Possuir todas as funcionalidades descritas no item 2.1.47 e no item 2.6;

3.34 **LOTE 5 – item 6:** Treinamento oficial para 5 pessoas

3.34.1 Requisitos específicos:

3.34.1.1 Possuir todas as funcionalidades descritas no item 2.7;

3.35 **LOTE 5 – item 7:** Solução de gerência centralizada

3.35.1 Requisitos específicos:

3.35.1.1 Possuir todas as funcionalidades descritas no item 2.2;
3.35.1.2 Possui capacidade mínima para armazenamento de logs de 4 TB.

ANEXO C DO TERMO DE REFERÊNCIA

PAUTA DE DISTIBUIÇÃO

ANEXO D DO TERMO DE REFERÊNCIA

MODELO DE COMPROVAÇÃO PONTUAL DE ATENDIMENTO À ESPECIFICAÇÃO TÉCNICA

LOTE	ITEM	ITEM	DESCRIÇÃO	PROPOSTA ATENDE ?	REFERENCIA NA DOCUMENTAÇÃO TÉCNICA	OBSER-VAÇÃO
.	.	.	.	.	.	.
.	.	.	.	.	.	.
.	.	.	.	.	.	.

ANEXO E DO TERMO DE REFERÊNCIA

TESTES DE CONFORMIDADE

1. TESTE DE CONFORMIDADE

A exigência da amostra visa à aferição da real capacidade técnica dos equipamentos ofertados pela Licitante Convocada. Busca-se comprovar tecnicamente, juntamente com a documentação do fabricante, se os equipamentos de fato atendem aos requisitos constantes da especificação técnica do Anexo B. Nesse sentido, os testes poderão ser efetuados em todos os lotes e itens.

1.1. Disposições gerais

1.1.1. O Teste de Conformidade deverá ser realizado em laboratório a ser disponibilizado pela licitante na cidade de Brasília-DF com o acompanhamento do grupo técnico de apoio ao DEIST/STI. Horário e suas alterações previamente autorizadas pelo DEIST/STI.

1.1.2. Após aceite da documentação comprobatória, a licitante deverá disponibilizar para realização dos testes de homologação, no prazo de 15 (quinze) dias corridos, contados a partir da solicitação do pregoeiro, uma amostra dos itens escolhidos do lote da mesma marca e modelo ofertado na proposta, a fim de apurar o atendimento da especificação técnica. Destacando-se que a referida solicitação do pregoeiro para a licitante só poderá ocorrer após validação dos Cadernos de Testes.

1.1.2.1. O prazo acima definido poderá, a critério do grupo técnico de apoio ao DEIST/STI, ser revisto ou dilatado caso haja um fato superveniente devidamente comprovado pela licitante.

1.1.3. Os testes serão feitos com base no Caderno de Testes aprovado pelo grupo técnico de apoio ao DEIST/STI. Nesse caderno deverão ser incluídos, minimamente os testes descritos no item 1.1.11 deste anexo.

1.1.4. O prazo para apresentação desse caderno de testes será de até 7(sete) dias úteis a partir da solicitação do pregoeiro. Além disso, o grupo técnico de apoio ao DEIST/STI poderá rejeitar o referido caderno no todo ou em parte, bem como sugerir alterações com o intuito de efetivamente comprovar o atendimento das especificações técnicas conforme Anexo B do Termo de Referência. Essa validação não pode exceder 3 (três) análises por parte do grupo técnico de apoio ao DEIST/STI.

1.1.5. A Licitante Convocada deverá indicar previamente, em até 2 (dois) dias úteis, a contar da data da referida convocação, a composição da "Equipe Técnica da Licitante Convocada". Tal equipe será a responsável pela realização do Teste de Conformidade e deverá ser composta por até 5 (cinco) técnicos ou representantes legais da licitante convocada, do fabricante da solução ou de empresa especializada na realização de testes de bancada, todos devidamente identificados por meio de vínculo contratual ou procuração.

1.1.6. Não será permitida a substituição de qualquer dos componentes da Equipe Técnica da Licitante Convocada sem a autorização prévia do DEIST/STI.

1.1.7. No caso de dispensa da avaliação de amostra, a equipe técnica apresentará a motivação para referida dispensa.

1.1.8. Cada uma das demais licitantes participantes do pregão que queira acompanhar o Teste de Conformidade deverá indicar previamente, em até 2 (dois) dias úteis, a contar da data da referida convocação, 1 (um) técnico ou representante legal da licitante ou do fabricante da solução ofertada, devidamente identificado por meio de vínculo contratual ou procuração, como "Técnico de Acompanhamento da Licitante Participante".

1.1.9. Não será permitida a substituição de qualquer Técnico de Acompanhamento da Licitante Participante sem a autorização prévia do DEIST/STI.

1.1.10. Não será permitida a comunicação direta entre qualquer Técnico de Acompanhamento da Licitante Participante e a Equipe Técnica da Licitante Convocada. Qualquer comunicação ou questionamento deve ser dirigido unicamente ao grupo técnico do DEIST/STI.

1.1.10.1. A não observância dessa regra de comunicação poderá causar o descredenciamento unilateral, por parte do DEIST/STI, de qualquer dos componentes da Equipe Técnica da Licitante Convocada ou de qualquer Técnico de Acompanhamento da Licitante Participante.

1.1.11. O Teste de Conformidade avaliará dois eixos de testes: os Testes de Capacidade e os Testes de Funcionalidades. Os dois eixos de testes possuem caráter obrigatório e serão avaliados simultaneamente.

1.1.12. O grupo técnico de apoio ao DEIST/STI poderá solicitar alteração ou adequação durante os testes, mesmo com o Caderno de Testes apresentado e aprovado, com a finalidade de dirimir quaisquer dúvidas referentes a itens da especificação técnica.

1.1.13. A não realização, a realização incompleta ou a não comprovação de qualquer dos itens previstos do Teste de Conformidade acarretarão na reprovação da solução ofertada. Esses testes devem ser realizados no prazo de até 20 (quinze) dias corridos com agendamento a ser acordado com grupo técnico de apoio ao DEIST/STI.

1.1.14. A STI, em situações excepcionais e de interesse da Administração Pública, reserva o direito de suspender temporariamente a execução do Teste de Conformidade, com a respectiva suspensão dos seus prazos de completa execução.

1.1.15. Caso uma mesma licitante seja convocada para realização de testes em mais de um lote, com o mesmo equipamento por ela ofertado, o teste a ser avaliado será o de maior porte.

1.1.16. A Licitante Convocada deverá prover, integralmente às suas custas, toda a infraestrutura necessária (equipamentos e cabos de conectividade de rede, equipamentos de geração de tráfego e ameaças, *appliances*, servidores de virtualização, desktops, todos os *softwares* e licenças de utilização, etc.) para a completa instalação e execução do Teste de Conformidade.

1.1.17. A solução ofertada, e demais equipamentos necessários à execução do Teste de Conformidade, deverão ser instalados, configurados, operados e acessados pela Equipe Técnica da Licitante Convocada, sempre acompanhada e supervisionada pelo grupo técnico de apoio ao DEIST/STI.

1.1.17.1. A não observância desse item poderá acarretar no reinício do Teste de Conformidade, ou mesmo na reprovação da solução ofertada.

1.1.18. A reprovação da solução ofertada implicará na desclassificação da Licitante Convocada do certame.

1.1.19. Não caberá a STI, sob qualquer hipótese, o pagamento de nenhum tipo de indenização em virtude da realização do Teste de Conformidade, seja a solução ofertada aprovada ou reprovada.

1.2.Amostra

1.2.1. Para o Teste de Capacidade, a Licitante Convocada deverá apresentar 1 (um) dos equipamentos (*appliances*) que fazem parte da solução de firewall multifuncional e a solução de gerenciamento centralizado que compõe a solução ofertada, devidamente licenciados e atendendo a todas as especificações técnicas indicadas no Anexo B do termo de Referência.

1.2.2. A solução de gerenciamento centralizado deverá ser instalada, executada e acessada em equipamentos (servidor de virtualização, desktops, notebooks, etc.) providos pela própria Licitante Convocada, na forma do item 1.1.16 deste anexo.

1.2.3. Todos os equipamentos e produtos que compõe a amostra da solução ofertada deverão estar acompanhados de seus respectivos programas, CDs, manuais, guias de instalação e demais documentos necessários para dirimir dúvidas, a fim de que possam ser realizados procedimentos de verificação de conformidade com as especificações técnicas constantes deste termo.

1.3.Preparação Inicial

1.3.1. A solução ofertada deverá ser inicialmente submetida a procedimento de "factory reset", "factory default" ou equivalente.

1.3.2. A solução ofertada deverá então ser atualizada para a versão mais atual de *firmware*, software, listas de assinaturas e afins disponíveis pelos canais oficiais de suporte técnico do fabricante da solução. Caso a versão atual tenha menos de 3 (três) meses de liberação de uso para o mercado, será admitida a utilização da versão imediatamente anterior.

1.3.2.1. Deverão ser aplicadas todas as correções, patches, fixes e afins recomendados pelo fabricante da solução em seus canais oficiais de suporte técnico.

1.3.2.2. Não serão aceitas versões, correções ou afins em estágios de testes (versões alfa e beta, release candidates, early availability, etc.).

1.3.2.3. Não serão aceitas correções, patches, fixes e afins que não tenham previsão de serem incorporados em futuras versões do *firmware* ou software da solução ofertada.

1.3.3. Uma vez que a solução ofertada tenha sido atualizada na forma do item 1.3.2, não será permitida mais nenhuma atualização adicional durante a execução de todo o Teste de Conformidade.

1.4.Teste de Capacidade e de Funcionalidade

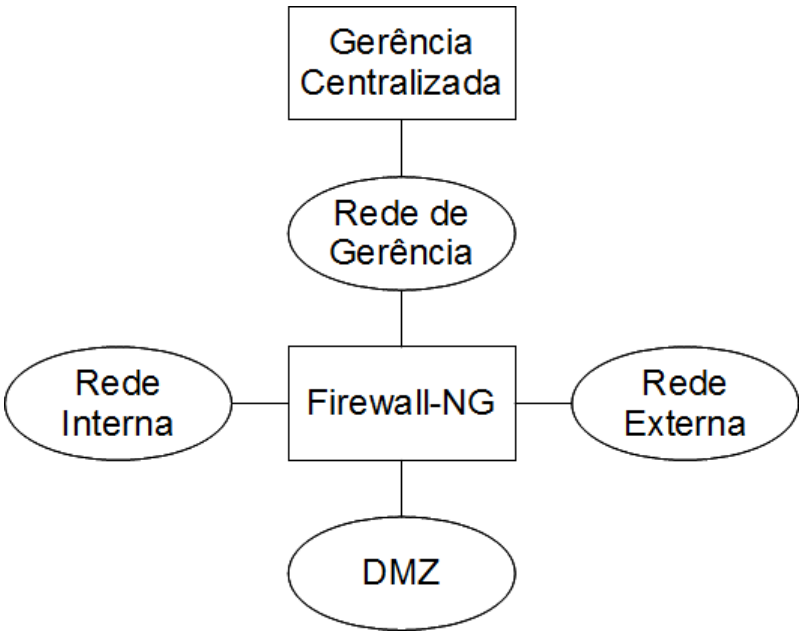
1.4.1. A Licitante Convocada deverá prover equipamentos especializados de geração de tráfego e ameaças, do tipo *appliance*, observado o item 1.1.16 deste anexo.

1.4.2. O conjunto de equipamentos especializados de geração de tráfego e ameaças deverá ser capaz de gerar pelo menos 5.000 (cinco mil) ameaças ou

ataques de tipos variados, stateful e stateless, encapsuladas nos protocolos diversos, incluindo, HTTP, HTTPS, protocolos de email, vídeo conferência, VoIP, FTP e VPN e métodos de ofuscação.

1.4.3. O conjunto de equipamentos especializados de geração de tráfego e ameaças deverá ser capaz de simular pelo menos 1.000 aplicações.

1.4.4. A amostra e demais equipamentos devem ser instalados e configurados de forma a simular uma arquitetura de rede conforme a figura abaixo:



1.4.4.1. O firewall multifuncional e a solução de Gerência Centralizada deverão se comunicar por meio de Rede de Gerência dedicada. O Firewall deverá se conectar à Rede de Gerência por meio de interface dedicada para este fim, conforme o item 2.2 das especificações técnicas presentes no Anexo B do termo de Referência.

1.4.4.2. A Rede Interna deverá possuir clientes, que deverão acessar a Rede Externa por meio de NAT N-1. A quantidade de clientes variam de acordo com o porte do lote.

1.4.4.2.1. Lote 1, pelo menos 50 clientes.
1.4.4.2.2. Lote 2, pelo menos 125 clientes.
1.4.4.2.3. Lote 3, pelo menos 500 clientes.
1.4.4.2.4. Lote 4, pelo menos 2.500 clientes.
1.4.4.2.5. Lote 5, pelo menos 5.000 clientes.

1.4.4.3. A DMZ deverá possuir servidores, que deverão ser acessados pela Rede Externa por meio de NAT 1-1. A quantidade de servidores variam de acordo com o porte do lote.

1.4.4.3.1. Lote 1, pelo menos 5 servidores.
1.4.4.3.2. Lote 2, pelo menos 13 servidores.
1.4.4.3.3. Lote 3, pelo menos 50 servidores.
1.4.4.3.4. Lote 4, pelo menos 250 servidores.
1.4.4.3.5. Lote 5, pelo menos 500 servidores.

1.4.4.4. A Rede Externa deverá possuir clientes, que farão acesso aos servidores da DMZ, e mais servidores, que serão acessados pelos clientes da Rede Interna. A quantidade de clientes e servidores variam de acordo com o porte do lote.

1.4.4.4.1. Lote 1, pelo menos 50 clientes e 5 servidores.
1.4.4.4.2. Lote 2, pelo menos 125 clientes e 13 servidores.
1.4.4.4.3. Lote 3, pelo menos 500 clientes e 50 servidores.
1.4.4.4.4. Lote 4, pelo menos 2.500 clientes e 250 servidores.
1.4.4.4.5. Lote 5, pelo menos 5.000 clientes e 500 servidores.

1.4.4.5. Cada servidor da Rede Externa e da DMZ deve corresponder a pelo menos 1 (uma) regra específica de acesso no Firewall. A quantidade de regras variam de acordo com o porte do lote.

1.4.4.5.1. Lote 1, pelo menos 10 regras.
1.4.4.5.2. Lote 2, pelo menos 25 regras.
1.4.4.5.3. Lote 3, pelo menos 100 regras.
1.4.4.5.4. Lote 4, pelo menos 500 regras.
1.4.4.5.5. Lote 5, pelo menos 1.000 regras.

1.4.5. A amostra deve ser configurada com as funcionalidades de firewall, tal como previstas na especificação técnica Anexo B, contendo identificação de usuários, identificação dos países de origem e destino das comunicações (geolocalização), controle de acesso à Internet (controle de aplicações e filtragem de URL's), sistema de prevenção a intrusão(IPS, Antivírus e Anti-Malware), administração de largura de banda de serviço (QoS), decriptografia e inspeção de tráfego SSL, suporte para conexões VPN IPSec e SSL habilitadas simultaneamente.

1.4.6. A amostra deve ser configurada de forma a realizar a inspeção integral de todos os pacotes de dados, independentemente de seu tamanho ou direção de fluxo, e com todas as assinaturas, listas e demais métodos de controle de acesso e sistema de detecção e prevenção de intrusão habilitados.

1.4.7. A amostra deve ser configurada com seus módulos de sistema de prevenção a intrusão(IPS, Antivirus e Anti-Malware) em modo de detecção.

1.4.8. A amostra deve ser configurada de forma a registrar todos os acessos autorizados ou bloqueados, bem como todas as aplicações e ameaças detectadas pelo Firewall Multifuncional.

1.4.9. A amostra deve ser submetida a um tráfego que corresponde a pelo menos 85% do tamanho especificado para throughput daquele lote, respeitando o perfil de tráfego.

1.4.10. Durante os testes, é vedado habilitar o modo de conservação, ou desligar funcionalidades automaticamente da amostra.

1.4.11. A amostra deve ser submetida à padrão de tráfego de dados, baseado em na metodologia do NSS Labs Metodologia, estudos de perfil de tráfego de órgãos do SISP, adaptações das RFCs 2544, 3511 e diretrizes e políticas de Firewalls do NIST, com a seguinte distribuição:

1.4.11.1. HTTP= 50% (conteúdo variável com imagens e textos, tamanho variável de 100 bytes a 500 Kbytes).

1.4.11.2. HTTPS a ser decriptografado e inspecionado = 30% (conteúdo variável com imagens e textos, tamanho variável de 100 bytes a 500 Kbytes).

1.4.11.3. Outros protocolos=20%, dentre eles protocolos de vídeo conferência, email, VPN e VoIP, etc.

1.4.11.3.1. VPN (IPSec, conteúdo variável com imagens e textos, tamanho variável de 100 bytes a 500 Kbytes).

1.4.11.3.2. Email (POP, SMTP e IMAP com conteúdo variável, incluindo arquivos anexos).

1.4.11.3.3. UDP (distribuição de tamanho: 56% 64 bytes, 17% 512 bytes e 27% 1518 bytes).

1.4.11.3.4. Outros (distribuição de tamanho varíável).

1.4.11.4. As ameaças, ataques e aplicações estarão encapsulados nestes protocolos.

1.4.12. A amostra terá o tamanho dos frames variados a ser definido na ocasião dos testes.

1.4.13. O padrão de tráfego definido no item 1.4.10 deve ser distribuído entre todos os clientes e servidores utilizados nos testes.

1.4.14. Será considerado como taxa de transferência (throughtput) o somatório das saídas (out) das interfaces sob teste.

1.4.15. A amostra deverá ser inicialmente submetida a uma taxa de transferência de 25% do perfil de tráfego do lote que estiver sendo testado por 30 minutos

com o objetivo de coleta de parâmetros que serão utilizados para verificação da performance do equipamento.

1.4.15.1. Serão coletados os parâmetros que indiquem a taxa de transferência, taxa de detecção de ameaças, taxa de detecção de aplicações, latência e variação de latência (jitter) do equipamento.

1.4.16. A amostra será então submetida a uma taxa de transferência do tamanho de 85% do throughput do lote que estiver sendo testado, por 30 minutos e não poderá apresentar prejuízo em sua performance.

1.4.16.1. Serão coletados os parâmetros que indiquem a taxa de transferência, taxa de detecção de ameaças, taxa de detecção de aplicações, latência e variação de latência (jitter) do equipamento.

1.4.17. Será considerado prejuízo na performance do equipamento a ocorrência de quaisquer dos eventos a seguir:

1.4.17.1. Perda de pacotes superior a 3%.

1.4.17.2. Erros irrecuperáveis de transações TCP/layer-7.

1.4.17.3. Obter taxa de detecção de ameaças ou ataques menor que 80%.

1.4.17.4. Valores de latência ou de variação de latência (jitter) acima de 5x (cinco vezes) dos valores coletados no item 1.4.16 deste anexo.

1.4.17.5. Os valores de latência poderão ser comparados com os descritos nos datasheets dos equipamentos testados pelo grupo técnico de apoio ao DEIST/STI para avaliação de desempenho.

1.4.18. A amostra deverá comprovar os itens de conexões simultâneas e novas conexões por segundo das especificações técnicas presentes no Anexo B deste termo por, pelo menos, 5 (cinco) minutos.

1.4.19. Durante a realização dos testes, será avaliada a solução de gerência centralizada, que deve permanecer acessível, possibilitando a modificação e aplicação de políticas de segurança, bem como a visualização dos logs de acesso e de detecção de ameaças e aplicações.

1.4.20. A licitante deve disponibilizar em até 5 (cinco) dias úteis contados da data da finalização dos testes, o relatório com todas as informações e resultados apurados durante os testes.

1.4.21. No relatório deve constar, no mínimo: informações da topologia do ambiente de teste utilizado, arquivos, scripts de configuração, versões de software utilizadas e registros de logs com evidências capturadas. O relatório deve ser fornecido de maneira impressa ou digital.

1.4.22. A equipe técnica do DEIST/STI emitirá no prazo de 5 (cinco) dias úteis após a entrega do relatório dos testes de amostra, o TERMO DE AVALIAÇÃO DE AMOSTRAS. O termo informará se a amostra está ou não de acordo com as especificações técnicas constantes no Anexo B do Termo de Referência.

1.4.23. Caso o TERMO DE AVALIAÇÃO DE AMOSTRAS indique que as amostras estão em total conformidade com as especificações técnicas exigidas, essas serão consideradas homologadas e a licitante será habilitada.

1.4.24. Caso o TERMO DE AVALIAÇÃO DE AMOSTRA indique que as AMOSTRAS não estão em conformidade com as especificações técnicas exigidas, as não conformidades serão listadas e a LICITANTE ofertante do melhor lance poderá ter, a critério do MP, o prazo de 3 (três) dias úteis, não prorrogáveis, a contar da data de emissão do Termo, para proceder aos ajustes necessários na(s) AMOSTRA(S) reprovadas com ressalvas e disponibilizá-las, no mesmo prazo, para a realização de testes complementares, para aferição da correção ou não das inconformidades indicadas.

1.4.25. A Equipe Técnica de apoio ao pregoeiro emitirá, no prazo de até 2 (dois) dias após a entrega da(s) AMOSTRA(S) ajustada(s), novo TERMO DE AVALIAÇÃO DE AMOSTRAS, em que informará se a(s) nova(s) AMOSTRA(s) está (ão) ou não em conformidade com as especificações técnicas exigidas neste Termo de Referência e anexos.

1.4.26. Caso o novo TERMO DE AVALIAÇÃO DE AMOSTRA indique a total conformidade da(s) AMOSTRA(S) ajustada(s) às especificações técnicas exigidas, essa(s) será(ão) considerada(s) homologada(s) e a proposta da LICITANTE será aceita.

1.4.27. Caso o novo TERMO DE AVALIAÇÃO DE AMOSTRA indique a não conformidade da(s) AMOSTRA(s) ajustada(s) às especificações técnicas exigidas, a LICITANTE ofertante do melhor lance será desclassificada e eliminada do processo licitatório

1.4.28. No caso de inabilitação da LICITANTE por não aprovação de AMOSTRA, o pregoeiro convocará a o próximo licitante detentor de proposta válida, obedecida a classificação na etapa de lances, sucessivamente, até que um licitante cumpra os procedimentos previstos

neste Termo de Referência, tendo sua proposta aprovada e a sua habilitação confirmada.