ANEXO I DO EDITAL DO PREGÃO Nº 05/2017

TERMO DE REFERÊNCIA

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 de computadores, 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 e suporte técnico durante o período de garantia com repasse de conhecimento da solução a fim de atender às necessidades dos 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 às 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 ameaças e tentativas de invasões das 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.

Cabe destacar que a presente contratação surgiu da manifestação de interesse dos órgãos do Sistema de Administração de Recurso de Tecnologia da Informação (SISP) em resposta a uma pesquisa realizada entre março e abril de 2015 pelo Núcleo de Contratações de TI (NCTI) e que foi confirmada, posteriormente, numa apresentação da comissão de coordenação do SISP, realizada em julho de 2015. Naquela oportunidade, 15 instituições demonstraram interesse em adquirir elementos de solução de segurança de rede, sendo que 3 delas indicaram que gostariam de compor um grupo de trabalho multi-disciplinar a fim de participar da modelagem e especificação da presente contratação. Ao final, a confirmação da Intenção de Registro de Preços (IRP), que ocorreu em Março de 2017, confirmou a participação de 54 órgãos ou entidades públicas participantes da contratação em tela.

Partindo-se de tais pressupostos, a presente contratação consiste na aquisição de uma solução de segurança integrada que englobe equipamento *firewall* corporativo e multifuncional. Essa solução pode incluir, dentre outras funcionalidades: alta disponibilidade, *anti-malware, anti-spyware,* antivírus, 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 desta contratação compartilhada por meio do mecanismo previsto no sistema de registro de preços (SRP).

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 técnicas e 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 do mercado e dos fornecedores das soluções de segurança de redes.

Para o levantamento das necessidades, qualificação da demanda e definição de parâmetros a fim de modelar a contratação em tela, 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 fizeram menção ao cenário presente nos órgãos, às maiores dificuldades nas soluções de segurança, aos pontos fracos e fortes de modelos de contratação indicados e às possibilidades de melhoria 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 técnicos 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 na modelagem no formato da contratação proposta nesse Termo de Referência com o agrupamento modular das soluções e a formação de lotes, a fim de atender as variadas faixas de necessidades apontadas na pesquisa junto ao SISP, conforme os perfis dos órgãos do SISP.

Em última análise, a contratação da solução de segurança aqui proposta vai além da aquisição de um conjunto de equipamentos. É uma busca por uma solução que melhore a maturidade em segurança de redes dos órgãos envolvidos, aumentando o ganho de escala (típico dos processos conjunto) e permitindo o gerenciamento por equipes técnicas mais reduzidas, uma vez que centraliza a solução de várias funcionalidades em uma 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, atualizaram-se os procedimentos do Sistema de Registro de Preços (SRP) 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, Desenvolvimento 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 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 mesmo 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 expressivos volumes 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 ou existir disponibilidade orçamentária para efetivar a contratação.

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 bem sucedidas com as contratações conjuntas de Ativos de Redes levaram a equipe da CGINF/DESIN/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 DESIN/STI, do grupo de trabalho técnico e da Central de Compras e Contratações - SEGES/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 questionamentos e às impugnações, porventura interpostos.

2.4. 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 e garantir a disponibilidade dos serviços disponibilizados na plataforma digital.

Os três eixos da EGD possuem pontos de atenção em 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 estão discriminados na Planilha de Quantitativos e Preços Máximos, constante no ANEXO A.

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

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 para a sua admissão pela Administração Pública.

5.2. Em função das características 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 mencionadas, foi possível enquadrar a contratação em apreço nos incisos I e III do Art. 3º do Decreto nº 7.892, de 23 janeiro de 2013.

5.3. Ainda conforme o Art. 4º do Decreto nº 7.892, é necessária a realização da Intenção de Registro de Preços - IRP, para verificação da intenção de participação no Registro de Preços, bem como será permitida a adesão para aquisição de mais 100% do quantitativo total da contratação, considerado para este limite o somatório dos quantitativos requeridos pelos órgãos não participantes, por meio de adesão, em consonância com o Art. 22º do Decreto nº 7.892, de 23 janeiro de 2013.

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.

7.4. 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.

7.5. A CONTRATANTE solicitará a instalação dos equipamentos e da solução por meio de uma Ordem de Serviço de Instalação - OSI, que deverá ser cumprida no prazo máximo de até 15 (quinze) dias corridos, a partir da sua emissão.

7.5.1. 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.

7.5.2. 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 TR.

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 TR.

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 TR, 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.

8.2.10.1 A solução a ser entregue pela CONTRATADA deverá ser idêntica àquela submetida como AMOSTRA (série, modelo, acessórios e outros componentes de hardware e software) no Teste de Conformidade, conforme Anexo E.

8.3. Escopo do Serviço de Instalação

8.3.1. A CONTRATADA deverá prover o 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 TR. Não fazendo parte do presente escopo de fornecimento cabeamento e *racks* para interconectar a solução à rede local do órgão CONTRATANTE.

8.3.2. A CONTRATADA deverá prover o 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 quando for o caso. 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 da CONTRATANTE, 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.

8.3.11. 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.

8.3.12. 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*.

8.3.13. 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 aqui presentes. 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 equipamentos 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 TR, 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, bem como da substituição de equipamentos não aceitos, cabendo à CONTRATANTE a emissão de documento fiscal ou equivalente necessário ao transporte do equipamento, quando for o

caso.

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

9.5. 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 Registro de Preços e dos contratos dela decorrentes, 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 da CONTRATANTE no tocante à verificação das especificações técnicas, prestando os esclarecimentos solicitados, atendendo às reclamações, caso ocorram, e prestando toda assistência técnica operacional.

9.8. Sujeitar-se a 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, durante o período de prestação dos serviços;

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 exigido 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 à CONTRATANTE, quando for o caso, a relação nominal dos empregados que adentrarão o órgão para a execução do serviço;

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

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

9.20. 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;

9.21. Instruir seus empregados quanto à necessidade de acatar as recomendações aceitas pela boa técnica, normas e legislação;

9.22. 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;

9.23. Relatar à CONTRATANTE toda e qualquer irregularidade verificada no decorrer da prestação dos serviços;

9.24. 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;

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

9.26. Arcar com os ônus necessários aos fornecimentos descritos neste processo;

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

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

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

9.30. 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.

9.31. 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.

9.32. 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 deste TR.

10.4. Exercer o acompanhamento e a fiscalização dos serviços, por servidor especialmente designado, anotando em registro próprio as falhas detectadas, 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. 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 a IN nº 02/2008 e posteriores alterações.

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

11. DOS NÍVEIS MÍNIMOS DE SERVIÇOS

11.1. Os níveis mínimos de serviço esperados para esta contratação, bem como para os atendimentos aos incidentes/eventos associados estão indicados na 'Tabela 1- Níveis Mínimos de Serviço', cabendo os seguintes detalhamentos:

11.1.1. A classificação da severidade dos incidentes/eventos será determinada pela CONTRATANTE respeitando-se o descrito na 'Tabela 2 - Classificação de Incidentes';

11.1.2. Todos os prazos para a resolução dos incidentes/eventos 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 (Prazo de Resolução)
Tipos 1, 2, 3, 4 e 5	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 ao final destes prazos em cada caso e condicionados à Tabela 3.

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. Exemplo: 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. Exemplo: 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 equipamento) para sanar o problema e restabelecer o funcionamento normal do equipamento, obedecendo ao 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 TR, 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 os 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 escusar de suas responsabilidades quanto à prestação da solução técnica para possíveis falhas ou inconsistências, bem como o auxílio técnico necessário 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*, cabendo à CONTRATANTE a emissão de documento fiscal ou equivalente necessário ao transporte do equipamento, quando for o caso.

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 nova(s) versão(ões) do(s) *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, ou seja, 60 meses a partir do Termo de Recebimento Definitivo estabelecido no item 8.2.10 deste TR.

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 a Ata de Registro de Preço ou o contrato, deixar de entregar documentação exigida neste TR, 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 conforme art. 7º 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 0,33% (zero vírgula trinta e três 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 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;

b4) 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 efetive nos 10 (dez) dias que se seguirem à data da comunicação formal da rejeição ou defeito, independentemente das demais sanções cabíveis;

b5) 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;

b6) multa moratória de 1% (um por cento) sobre o valor total do Contrato, por descumprir ou infringir qualquer das obrigações estabelecidas nos demais itens

referenciados item 9 –DAS OBRIGAÇÕES DA CONTRATADA, estabelecidos neste Termo de Referência, aplicada em dobro na sua reincidência, independentemente das demais sanções cabíveis;

b7) 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. 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;

13.1.3. 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;

13.1.4. Os valores de multas não pagos serão descontados da garantia prestada pela CONTRATADA ou da fatura.

13.1.5. 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;

13.1.6. As penalidades serão obrigatoriamente registradas no SICAF e, no caso de impedimento 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;

13.1.7. 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;

13.1.8. 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, acarretará às 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
Tipo 1, 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 da solução.
			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 da solução, 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 da solução, 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 da solução.
			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 da solução, 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 da solução.
			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 da solução, 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 da solução, 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 uma mesma equipamento solução **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 da solução.
			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 da solução, 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 da solução, 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 da solução.
			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 da solução, 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 da solução, 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 da solução.
			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 da solução, 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 da solução, 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 uma mesma solução 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 da solução. 29) Se o somatório das multas aplicadas com relação às obrigações relativas a uma mesma solução ultrapasse **20**% do seu valor de aquisição, poderá ensejar a rescisão do Contrato, independentemente de aplicação das sanções administrativas cabíveis.

15. DO PAGAMENTO

15.1. O pagamento será realizado no prazo máximo de até trinta dias, corridos, contados a partir da emissão do Termo de Recebimento Definitivo do Objeto, através de ordem bancária, para crédito em banco, agência e conta corrente indicados pela CONTRATADA.

15.2. Havendo erro na apresentação da Nota Fiscal ou dos documentos pertinentes à contratação, ou, ainda, circunstância que impeça a liquidação da despesa, como, por exemplo, obrigação financeira pendente, decorrente de penalidade imposta ou inadimplência, o pagamento ficará sobrestado até que a CONTRATADA providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para a CONTRATANTE.

15.3. Será considerada data do pagamento à CONTRATADA, será realizada consulta ao SICAF para verificar a manutenção das condições de habilitação exigidas no Edital.

15.4. Constatando-se, junto ao SICAF, a situação de irregularidade da CONTRATADA, será providenciada sua advertência, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da CONTRATANTE.

15.5. Não havendo regularização ou sendo a defesa considerada improcedente, a CONTRATANTE deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência da CONTRATADA, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

15.6. Persistindo a irregularidade, a CONTRATANTE deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada à CONTRATADA a ampla defesa.

15.7. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do Contrato, caso a CONTRATADA não regularize sua situação junto ao SICAF.

15.8. Somente por motivo de economicidade, segurança nacional ou outro interesse público de alta relevância, devidamente justificado, em qualquer caso, pela

máxima autoridade da CONTRATANTE, não será rescindido o contrato em execução com a CONTRATADA inadimplente no SICAF.

15.9. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

a) A CONTRATADA regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

15.10. Nos casos de eventuais atrasos de pagamento, desde que a CONTRATADA não tenha concorrido, de alguma forma, para tanto, fica convencionado que a taxa de compensação financeira devida pela CONTRATANTE, entre a data do vencimento e o efetivo adimplemento da parcela, é calculada mediante a aplicação da seguinte fórmula:

EM = I x N x VP, sendo:

EM = Encargos moratórios;

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

VP = Valor da parcela a ser paga.

I = Índice de compensação financeira = 0,00016438, assim apurado:

I =	(6 / 100) / 365	I = 0,00016438 TX = Percentual da taxa anual = 6%

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. Uma mesma licitante poderá participar oferecendo propostas para um ou mais lotes do presente certame, desde que reúna as condições de habilitação necessárias, devendo ofertar preços para todos os itens que compõem o respectivo lote. Ressalta-se que há a possibilidade de cada lote ter um ganhador distinto.

16.3. 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, a fim de dar transparência ao processo e permitir futuras alterações contratuais sem a possibilidade da adoção pela APF de partes obscuras da solução em termos de valores.

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

16.5. 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.

16.6. A licitante deverá apresentar, juntamente com a proposta, o ANEXO D para avaliação do atendimento aos requisitos técnicos e aprovação pelo grupo técnico designado para a contratação que dará apoio ao pregoeiro.

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

16.8. No caso de entender tais documentos como insuficientes para a análise, poderá o pregoeiro, suportado pelo grupo técnico de apoio, solicitar complementação, 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.

16.9. 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, 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 a avaliação da proposta da Licitante mais bem colocada, o pregoeiro solicitará à licitante que apresente um CADERNO DE TESTES, o qual será avaliado e poderá ser aprovado ou não pelo grupo técnico de apoio à contratação nos termos do Anexo E deste TR.

16.12. Caso o CADERNO DE TESTES seja aprovado pelo grupo técnico, o pregoeiro solicitará uma AMOSTRA para realização do Teste de Conformidade da solução de acordo com o descrito no ANEXO E.

16.13 A aprovação da comprovação por escrito da documentação técnica, bem como do CADERNO DE TESTE e das AMOSTRAS pela equipe técnica de apoio ao pregoeiro são condições necessárias para a fase de habilitação da LICITANTE, bem como para 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, de acordo com o pactuado, 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, a instalação e a manutenção/assistência técnica dos equipamentos e *softwares* que compõe a solução, objeto deste TR, 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 possua as especificações compatíveis com esse lote ou superiores	15
Lote 2	*Firewall* Multifuncional	*Firewall* multifuncional de mesmo tamanho de *throughput* que possua as especificações compatíveis com esse lote ou superiores	10
Lote 3	*Firewall* Multifuncional	*Firewall* multifuncional de mesmo tamanho de *throughput* que possua as especificações compatíveis com esse lote ou superiores	10
Lote 4	*Firewall* Multifuncional	*Firewall* multifuncional com tamanho de *throughput* que possua as especificações compatíveis com esse lote ou superior	5
Lote 5	*Firewall* Multifuncional	*Firewall* multifuncional com tamanho de *throughput* que possua as especificações compatíveis com esse 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 TR.

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. Será permitida a adesão para aquisição de mais 100% do quantitativo total da contratação, considerado para este limite o somatório dos quantitativos requeridos pelos órgãos não participantes, por meio de adesão, em consonância com o Art. 22º do Decreto nº 7.892, de 23 janeiro de 2013.

19.3. O(s) contrato(s) terá(ão) vigência de até 12 (meses) meses, a contar da data de sua assinatura. Destacando-se que a garantia da solução e a atualização de *firmwares* e *softwares* deve ser de 60 meses contados a partir do termo de recebimento definitivo.

20. DA FISCALIZAÇÃO

20.1. A CONTRATANTE designará responsável para acompanhar e fiscalizar a execução do contrato, que registrará em relatório 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 TR.

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

Wellington Francisco Pinheiro de Araújo SIAPE: 1775484	Sílvio César da Silva Lima SIAPE: 2475974	Clayton da Costa Paixão SIAPE: 2222250

Brasília, maio de 2017.

Aprovo o presente Termo de Referência, conforme proposto.

Brasília, maio de 2017.

Marcelo Daniel Pagotti

Secretário

ANEXO "A" DO TERMO DE REFERÊNCIA
PLANILHA DE QUANTITATIVOS E PREÇOS UNITÁRIOS MÁXIMOS (QUANTIDADES E PREÇO TOTAL ESTIMADO PARA O LOTE)

Item	Descrição	Quantidade	Valor Unitário (R$)	Valor Total (R$)
Item 1	Firewall multifuncional Tipo 1	694	11.969,59	8.306.895,46
Item 2	Conjunto de funcionalidades IPS/IDS do FW Tipo 1	688	4.136,29	2.845.767,52
Item 3	Conjunto de funcionalidades antivírus e *anti-malware* do FW Tipo 1	691	3.809,30	2.632.226,30
Item 4	Conjunto de funcionalidades para tratamento de conteúdo web do FW Tipo 1	688	3.922,91	2.698.962,08
Item 5	Conjunto de funcionalidades para controle de aplicações e análise profunda do FW Tipo 1	688	4.143,05	2.850.418,40
Item 6	Treinamento oficial até 5 pessoas do FW Tipo 1	128	24.922,59	3.190.091,52
Item 7	Solução de gerência centralizada do FW Tipo 1	240	38.891,41	9.333.938,40
Item 8	Firewall multifuncional Tipo 2	94	29.714,35	2.793.148,90
Item 9	Conjunto de funcionalidades IPS/IDS do FW Tipo 2	92	9.886,63	909.569,96
Item 10	Conjunto de funcionalidades antivírus e *anti-malware* do FW Tipo 2	92	9.254,63	851.425,96
Item 11	Conjunto de funcionalidades para tratamento de conteúdo web do FW Tipo 2	92	9.394,87	864.328,04
Item 12	Conjunto de funcionalidades para controle de aplicações e análise profunda do FW Tipo 2	92	9.886,63	909.569,96
Item 13	Treinamento oficial até 5 pessoas do FW Tipo 2	22	26.512,40	583.272,80
Item 14	Solução de gerência centralizada do FW Tipo 2	20	49.928,42	998.568,40

Item 15	Firewall multifuncional Tipo 3	147	135.115,78	19.862.019,66
Item 16	Conjunto de funcionalidades IPS/IDS do FW Tipo 3	147	27.562,40	4.051.672,80
Item 17	Conjunto de funcionalidades antivírus e *anti-malware* do FW Tipo 3	143	34.842,87	4.982.530,41
Item 18	Conjunto de funcionalidades para tratamento de conteúdo web do FW Tipo 3	141	35.191,91	4.962.059,31
Item 19	Conjunto de funcionalidades para controle de aplicações e análise profunda do FW Tipo 3	141	28.140,31	3.967.783,71
Item 20	Treinamento oficial até 5 pessoas do FW Tipo 3	86	21.146,12	1.818.566,32
Item 21	Solução de gerência centralizada do FW Tipo 3	96	44.751,17	4.296.112,32
Item 22	Firewall multifuncional Tipo 4	54	486.946,02	26.295.085,08
Item 23	Conjunto de funcionalidades IPS/IDS do FW Tipo 4	54	151.153,00	8.162.262,00
Item 24	Conjunto de funcionalidades antivírus e *anti-malware* do FW Tipo 4	54	174.318,57	9.413.202,78
Item 25	Conjunto de funcionalidades para tratamento de conteúdo web do FW Tipo 4	54	147.752,11	7.978.613,94
Item 26	Conjunto de funcionalidades para controle de aplicações e análise profunda do FW Tipo 4	54	151.153,00	8.162.262,00
Item 27	Treinamento oficial até 5 pessoas do FW Tipo 4	39	25.190,83	982.442,37
Item 28	Solução de gerência centralizada do FW Tipo 4	33	84.447,98	2.786.783,34
Item 29	Firewall multifuncional Tipo 5	23	1.105.585,61	25.428.469,03
Item 30	Conjunto de funcionalidades IPS/IDS do FW Tipo 5	23	168.135,94	3.867.126,62
Item 31	Conjunto de funcionalidades antivírus e *anti-malware* do FW Tipo 5	23	183.299,12	4.215.879,76
Item 32	Conjunto de funcionalidades para tratamento de conteúdo web do FW Tipo 5	23	186.980,91	4.300.560,93
Item 33	Conjunto de funcionalidades para controle de aplicações e análise profunda do FW Tipo 5	23	168.135,94	3.867.126,62
Item 34	Treinamento oficial até 5 pessoas do FW Tipo 5	13	26.512,40	344.661,20
Item 35	Solução de gerência centralizada do FW Tipo 5	15	65.159,40	977.391,00
	Valor Total da Contratação:			**R$ 190.490.794,90**

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. Para cada lote adquirido é obrigatória a aquisição do primeiro item (do lote). Essa obrigatoriedade deve ser seguida tanto para órgãos partícipes da ata, quanto para órgãos que façam aquisições como não participantes.

Lote	Item	Descrição	Quantidade
1	**Item 1**	**Firewall multifuncional Tipo 1**	694
	Item 2	Conjunto de funcionalidades IPS/IDS do FW Tipo 1	688
	Item 3	Conjunto de funcionalidades antivírus e *anti-malware* do FW Tipo 1	691
	Item 4	Conjunto de funcionalidades para tratamento de conteúdo web do FW Tipo 1	688
	Item 5	Conjunto de funcionalidades para controle de aplicações e análise profunda do FW Tipo 1	688
	Item 6	Treinamento oficial até 5 pessoas do FW Tipo 1	128
	Item 7	Solução de gerência centralizada do FW Tipo 1	240
2	**Item 8**	**Firewall multifuncional Tipo 2**	94
	Item 9	Conjunto de funcionalidades IPS/IDS do FW Tipo 2	92
	Item 10	Conjunto de funcionalidades antivírus e *anti-malware* do FW Tipo 2	92
	Item 11	Conjunto de funcionalidades para tratamento de conteúdo web do FW Tipo 2	92
	Item 12	Conjunto de funcionalidades para controle de aplicações e análise profunda do FW Tipo 2	92
	Item 13	Treinamento oficial até 5 pessoas do FW Tipo 2	22
	Item 14	Solução de gerência centralizada do FW Tipo 2	20
3	**Item 15**	**Firewall multifuncional Tipo 3**	147
	Item 16	Conjunto de funcionalidades IPS/IDS do FW Tipo 3	147
	Item 17	Conjunto de funcionalidades antivírus e *anti-malware* do FW Tipo 3	143
	Item 18	Conjunto de funcionalidades para tratamento de conteúdo web do FW Tipo 3	141
	Item 19	Conjunto de funcionalidades para controle de aplicações e análise profunda do FW Tipo 3	141
	Item 20	Treinamento oficial até 5 pessoas do FW Tipo 3	86
	Item 21	Solução de gerência centralizada do FW Tipo 3	96
4	**Item 22**	**Firewall multifuncional Tipo 4**	54

	Item 23	Conjunto de funcionalidades IPS/IDS do FW Tipo 4	54
	Item 24	Conjunto de funcionalidades antivírus e *anti-malware* do FW Tipo 4	54
	Item 25	Conjunto de funcionalidades para tratamento de conteúdo web do FW Tipo 4	54
	Item 26	Conjunto de funcionalidades para controle de aplicações e análise profunda do FW Tipo 4	54
	Item 27	Treinamento oficial até 5 pessoas do FW Tipo 4	39
	Item 28	Solução de gerência centralizada do FW Tipo 4	33
5	**Item 29**	**Firewall multifuncional Tipo 5**	23
	Item 30	Conjunto de funcionalidades IPS/IDS do FW Tipo 5	23
	Item 31	Conjunto de funcionalidades antivírus e *anti-malware* do FW Tipo 5	23
	Item 32	Conjunto de funcionalidades para tratamento de conteúdo web do FW Tipo 5	23
	Item 33	Conjunto de funcionalidades para controle de aplicações e análise profunda do FW Tipo 5	23
	Item 34	Treinamento oficial até 5 pessoas do FW Tipo 5	13
	Item 35	Solução de gerência centralizada do FW Tipo 5	15

2. ESPECIFICAÇÕES

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

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

2.1.2. Todos os equipamentos e seus componentes deverão ser novos, sem uso, e 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*, *transceivers*, etc, necessários às suas instalações e operação em rack de 19" padrão EIA-310. No caso dos lotes 1 e 2, firewall multifuncionais de 100 e 250 Mbps, poderá ser fornecido os insumos como bandejas para colocação dos mesmos em racks.

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

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

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

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

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

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

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

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

2.1.6. As licenças de atualização de *software* (*firmware* ou *drivers*) e licenças de atualização de assinaturas deverão ser 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.

2.1.7. Todos os equipamentos devem funcionar 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.

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

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

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

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

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

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

2.1.10.1. Os equipamentos dos lotes 1, 2, 3 e 4 da solução ofertada, não deverão exceder, individualmente, 4 Unidades de Rack, sendo "caixas" únicas, sem empilhamentos.

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

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

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

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

2.1.14. Possuir filtragem de pacote por endereço IP de origem e destino, por 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.

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

2.1.16. Suportar *tags* de VLAN;

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

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

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

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

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

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

2.1.21.2. Suportar e efetuar o download dos arquivos PCAP.

2.1.22. Não deve possuir restrições de licenciamento em relação às características, requisitos e funcionalidades presentes nos subitens do item 2.1, inclusive em relação ao número ou tipo de clientes, usuários, máquinas e endereços IP.

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

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

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

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

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

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

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

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

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

2.1.25. Deve suportar no mínimo NAT 64.

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

2.1.27. Suportar nativamente IPv6;

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

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

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

2.1.30. Possuir tecnologia de *firewall stateful*;

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

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

2.1.33. Suportar sincronização de horário por NTP;

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

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

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

2.1.37. Possuir mecanismo de *anti-spoofing*;

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

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

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

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

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

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

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

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

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

2.1.45.2. Deve permitir a delegação de funções de administração.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.1.52. Deve permitir a criação de túneis VPN IPSec;

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

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

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

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

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

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

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

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

2.1.59. Suportar Certificado Digital X.509 v3;

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

2.1.61. Permitir alteração dos algoritmos criptográficos das VPNs;

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

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

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

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

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

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

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

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

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

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

2.2. Solução de gerência centralizada

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

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

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

a) ser compatíveis com rack padrão 19 polegadas;

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

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

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

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

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

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

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

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

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

2.2.6. Deve permitir a criação de relatórios customizados.

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

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

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

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

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

2.2.12. Deverá manter o histórico de configurações enviadas aos equipamentos e deverá 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, durante ou depois de aplicá-las.

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

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

2.3. Conjunto de funcionalidades IPS/IDS

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

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

2.3.3. Decodificar múltiplos formatos de *Unicode*;

2.3.4. Suportar fragmentação e desfragmentação IP;

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

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

2.3.7. Possuir proteção contra os ataques como, mas não restringindo-se 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, suportando, no mínimo, as técnicas: IP *Packet Fragmentation*, *Stream Segmentation*, RPC *Fragmentation*, URL *Obfuscation*, HTML *Obfuscation*, *Payload Encoding*, FTP *Evasion* e *Layered Evasions*.

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

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

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

2.3.17. Possuir as estratégias de bloqueio e liberação selecionáveis, tanto por conjuntos de 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 com a gerência local e a gerência centralizada da solução.

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

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

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

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

2.4.2. Possuir funcionalidade de varredura contra vírus e *malwares* em tráfego nos seguintes protocolos: HTTPS, HTTP e pelo menos dois dos seguintes: 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*, *e-mail* ou outros meios de alerta;

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 a gerência local e a gerência centralizada da solução.

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

2.5. Conjunto de funcionalidades para tratamento de conteúdo web

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

2.5.2. Permitir a criação de categorias personalizadas;

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

2.5.4. Suportar filtragem e categorização das URLs;

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

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

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

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

2.5.9. Deve ser capaz 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;

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

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

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

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

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

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

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

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

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

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

2.6.2. Deve ser capaz de identificar as aplicações mesmo que não estejam 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 que utilizam comunicação criptografada através de SSL.

2.6.5. Permitir o agrupamento de aplicações em grupos personalizados;

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

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

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

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

2.6.10. Possuir atualização manual e automática de novas assinaturas;

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

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

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

2.7. Treinamento oficial para até 5 pessoas

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

2.7.2. A carga horária do treinamento não poderá ser inferior a 24 horas, sendo cada voucher apto para até 5 pessoas. O treinamento é composto por turmas que

podem ser formadas de um ou mais Vouchers de uma entidade CONTRATANTE, ou ainda, ser uma turma compartilhada por mais de uma entidade CONTRATANTE. Nos dois casos cada turma se limita a no máximo 10 pessoas.

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

2.7.3.1. O local de treinamento deverá possuir todas as facilidades para um perfeito desempenho das atividades, incluindo os recursos áudio 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 (mas não se restringindo a) sala de aula, data show, apostilas, bloco de anotações e caneta para cada treinando.

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

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

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

2.7.8. São produtos esperados de todos os treinamentos:

2.7.8.1. Aulas teóricas e práticas.

2.7.8.2. Material didático contratado e aprovado pela CONTRATANTE.

2.7.8.3. Referências para estudos e pesquisas complementares.

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

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

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

3. DEFINIÇÃO DOS LOTES E ITENS

3.1. LOTE 1 - Item 1: Firewall multifuncional Tipo1

3.1.1. Requisitos específicos:

3.1.1.1. Atender a todos os requisitos do item 2.1;

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

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

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

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

3.1.1.6. Quantidade mínima de 50.000 sessões simultâneas.

3.1.1.7. Quantidade mínima de 5.000 novas sessões por segundo

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

3.2.1. Atender a todos os requisitos do item 2.3.;

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

3.3.1. Atender a todos os requisitos do item 2.4;

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

3.4.1. Atender a todos os requisitos do item 2.5;

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

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

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

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

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

3.7.1. Requisitos específicos:

3.7.1.1. Atender a todos os requisitos do item 2.2

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

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

3.8.1. Requisitos específicos:

3.8.1.1. Atender a todos os requisitos do item 2.1;

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

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

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

3.8.1.5. Quantidade de sessões simultâneas 90.000.

3.8.1.6. Quantidade de novas sessões por segundo 12.000.

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

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

3.9.1. Atender a todos os requisitos do item 2.3;

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

3.10.1. Atender a todos os requisitos do 2.4;

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

3.11.1. Atender a todos os requisitos do item 2.5;

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

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

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

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

3.14. LOTE 2 - item7: Solução de gerência centralizada

3.14.1. Requisitos específicos

3.14.1.1. Atender a todos os requisitos do item 2.2;

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

3.15. LOTE 3 – item 1: Firewall multifuncional Tipo3

3.15.1. Requisitos específicos:

3.15.1.1. Atender a todos os requisitos do 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 e 2.6, ativadas simultaneamente e com inspeção integral de todos os pacotes de dados, independentemente de seu tamanho ou direção de fluxo, levando-se em consideração o perfil de tráfego descrito no ANEXO E.

3.15.1.3. O equipamento deve possuir no mínimo 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 6 (seis) portas 10/100/1000 BASE-T, podendo 1 (uma) delas ser utilizada para a gerência e 4 (quatro) portas 1 GE SFP, com os respectivos *transceivers* 1000 BASE-SX e padrão IEEE 802.3z.

3.15.1.5. Possuir a capacidade mínima de 1 (um) disco rígido ou SSD de 24 GB para armazenamento de logs.

3.15.1.6. Suporte para no mínimo 3 (três) instâncias virtuais.

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. *Throughput* mínimo de 300 Mbps para IPSec VPN.

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

3.16.1. atender a todos os requisitos do item 2.3;

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

3.17.1. Atender a todos os requisitos do item 2.4;

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

3.18.1. Atender a todos os requisitos do item 2.5;

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

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

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

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

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

3.21.1. Requisitos específicos:

3.21.1.1. Atender a todos os requisitos do item 2.2;

3.21.1.2. Possuir capacidade mínima de 1TB para armazenamento de logs e eventos.

3.22. LOTE 4 – **item 1:** Firewall multifuncional Tipo 4

3.22.1. Requisitos específicos:

3.22.1.1. Atender a todos os requisitos do item 2.1;

3.22.1.2. Possuir, no mínimo, o *throughput* de 5 Gbps para todas as funcionalidades dos itens 2.1, 2.2, 2.3, 2.4, 2.5 e 2.6, ativadas simultaneamente e com inspeção integral de todos os pacotes de dados, independentemente de seu tamanho ou direção de fluxo, levando-se em consideração o perfil de tráfego descrito no ANEXO E.

3.22.1.3. 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 BASE-T, podendo 01 (uma) delas ser utilizada para gerência, 4 (quatro) portas 1GE SFP, com os respectivos *transceivers* 1000BASE-SX e padrão IEEE802.3z, e 2 (duas) portas 10GE SFP+ ou XFP, com os respectivos *transceivers* 10GBASE-SR e padrão IEEE802.3ae.

3.22.1.4.1. As portas elétricas podem ser entregues por meio de *transceivers*.

3.22.1.5. Possuir a capacidade mínima de 2 (dois) discos, sendo rígidos ou SSD de 120 GB em RAID 1 para armazenamento de logs.

3.22.1.6. Fontes de alimentações internas redundantes.

3.22.1.7. Ser licenciado para no mínimo 10 instâncias virtuais.

3.22.1.8. Quantidade de sessões simultâneas 2.000.000.

3.22.1.9. Quantidade de novas sessões por segundo 90.000.

3.22.1.10. *Throughput* mínimo de 600 Mbps para IPSec VPN.

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

3.23.1. Atender a todos os requisitos do item 2.3;

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

3.24.1. Requisitos específicos:

3.24.1.1. Atender a todos os requisitos do item 2.4;

3.24.1.2. Possuir suporte para a integração com equipamentos ou serviços com a funcionalidade de APT (*Advanced Persistent Threat*) e *Zero Day*.

3.24.1.2.1. A funcionalidade de APT (Advanced Persistent Threat) e Zero Day deve possuir capacidade de emular (sandbox) ataques em diferentes sistemas operacionais, tais como: Windows XP e Windows 7, assim como documentos do Windows Office. 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.

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

3.25.1. Atender a todos os requisitos do item 2.5;

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

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

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

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

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

3.28.1. Requisitos específicos:

3.28.1.1. Atender a todos os requisitos do item 2.2;

3.28.1.2. Possuir capacidade mínima de 2 TB para armazenamento de logs e eventos.

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

3.29.1. Requisitos específicos:

3.29.1.1. Atender a todos os requisitos do item 2.1;

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

3.29.1.3. 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 6 (seis) portas 10/100/1000 BASE-T, podendo 01 (uma) delas ser utilizada para gerência, 6 (seis) portas 1GE SFP, com os respectivos *transceivers* 1000BASE-SX e padrão IEEE802.3z, e 4 (quatro) portas de 10GE SFP+ ou XFP, com os respectivos *transceivers* 10GBASE-SR e padrão IEEE802.3ae.

3.29.1.4.1. As portas elétricas podem ser entregues por meio de *transceivers*.

3.29.1.5. Possuir a capacidade mínima de 2 (dois) discos, sendo rígidos ou SSD de 240 GB em RAID 1 para armazenamento de logs

3.29.1.6. Fontes de alimentação internas redundantes.

3.29.1.7. Ser licenciado para no mínimo 20 instâncias virtuais.

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. *Throughput* mínimo de 1,5Gbps para IPSec VPN.

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

3.30.1. Atender a todos os requisitos do item 2.3;

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

3.31.1. Requisitos específicos:

3.31.1.1. Atender a todos os requisitos do item 2.4;

3.31.1.2. Possuir suporte para a integração com equipamentos ou serviços com a funcionalidade de APT (*Advanced Persistent Threat*) e *Zero Day*.

3.31.1.2.1. A funcionalidade de APT (Advanced Persistent Threat) e Zero Day devem possuir capacidade de emular (sandbox) ataques em diferentes sistemas operacionais, tais como: Windows XP e Windows 7, assim como documentos do Windows Office. 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. Atender a todos os requisitos do item 2.5;

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

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

3.34. LOTE 5 – item 6: Treinamento oficial para até 5 pessoas

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

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

3.35.1. Requisitos específicos:

3.35.1.1. Atender a todos os requisitos do item 2.2;

3.35.1.2. Possuir capacidade mínima de 4 TB para armazenamento de logs e eventos.

ANEXO "C" DO TERMO DE REFERÊNCIA
PAUTA DE DISTRIBUIÇÃO

			Lote 1						
Estado	Cidade	UASG/Órgão	item 1	item 2	item 3	item 4	item 5	item 6	item 7
PA	Altamira	200111 SUPERINTENDENCIA REG. POL. RODV. FEDERAL PA	1	1	1	1	1	0	1
PA	Ananindeua	200111 SUPERINTENDENCIA REG. POL. RODV. FEDERAL PA	1	1	1	1	1	0	1
SP	Aparecida	200117 SUPERINTENDENCIA REG. POL. RODV. FEDERAL SP	1	1	1	1	1	0	1
SE	Aracajú	195006 CIA DE DESENV. DO VALE DO SAO FRANCISCO DF	1	1	1	1	1	0	1
AL	Arapiraca	152805 CAMPUS ARAPIRACA	1	1	1	1	1	0	0
SP	Arujá	200117 SUPERINTENDENCIA REG. POL. RODV. FEDERAL SP	1	1	1	1	1	0	1
SP	Atibaia	200117 SUPERINTENDENCIA REG. POL. RODV. FEDERAL SP	2	2	2	2	2	0	2
SP	Barra do Turvo	200117 SUPERINTENDENCIA REG. POL. RODV. FEDERAL SP	1	1	1	1	1	0	1
AL	Batalha	158147 INST.FED.DE EDUC.CIENC.E TEC.DE ALAGOAS	1	1	1	1	1	0	0
PA	Belém	200111 SUPERINTENDENCIA REG. POL. RODV. FEDERAL PA	1	1	1	1	1	1	1

MG	Belo Horizonte	158122 INST.FED.DE EDUC.CIENCIA E TECNOLOGIA DE MG	6	6	6	6	6	2	2
MG	Belo Horizonte	195006 CIA DE DESENV. DO VALE DO SAO FRANCISCO DF	1	1	1	1	1	0	1
PA	Benevides	200111 SUPERINTENDENCIA REG. POL. RODV. FEDERAL PA	1	1	1	1	1	0	1
BA	Bom Jesus da Lapa	195006 CIA DE DESENV. DO VALE DO SAO FRANCISCO DF	1	1	1	1	1	0	1
DF	Brasília	170008 MF PROCURADORIA GERAL DA FAZENDA NACIONAL_DF	2	2	2	2	2	1	1
DF	Brasília	195006 CIA DE DESENV. DO VALE DO SAO FRANCISCO DF	0	0	0	0	0	3	0
DF	Brasília	200141 SUPERINTENDENCIA REG. POL. RODV. FEDERAL DF	6	6	6	6	6	6	6
DF	Brasília	201004 MP COORDENACAO GERAL DE AQUISIÇÕES	20	20	20	20	20	1	2
DF	Brasília	201057 SERVIÇO FLORESTAL BRASILEIRO – SFB-DF	10	10	10	10	10	2	2
DF	Brasília	343026 IPHAN INST. PATR. HIST. E ARTISTICO NACIONAL	65	65	65	65	65	1	1
PB	Cabedelo	275068 COMPANHIA BRASILEIRA DE TRENS URBANOS	1	1	1	1	1	0	0
SP	Caçapava	200117 SUPERINTENDENCIA REG. POL. RODV. FEDERAL SP	1	1	1	1	1	0	1
PA	Cachoeira do Pará	200111 SUPERINTENDENCIA REG. POL. RODV. FEDERAL PA	1	1	1	1	1	0	1
SP	Cachoeira Paulista	200117 SUPERINTENDENCIA REG. POL. RODV. FEDERAL SP	1	1	1	1	1	0	1
SP	Cajati	200117 SUPERINTENDENCIA REG. POL. RODV. FEDERAL SP	1	1	1	1	1	0	1
CE	Camocim	158961 INST. FEDERAL DO CEARÁ_CAMPUS CAMOCIM	1	1	1	1	1	1	1
MS	Campo Grande	200128 SUPERINTENDENCIA REG. POL. RODV. FEDERAL MS	30	30	30	30	30	1	1
MT	Campo Novo do Parecis	158492 INST.FED.MATO GROSSO CAMPUS NOVO PARECIS	2	0	2	0	0	1	0
GO	Campos Belos	158124 INST.FED.DE EDUC. CIENCIA E TEC. GOIANO	1	1	1	1	1	1	1
PA	Capanema	200111 SUPERINTENDENCIA REG. POL. RODV. FEDERAL PA	1	1	1	1	1	0	1
PA	Castanhal	200111 SUPERINTENDENCIA REG. POL. RODV. FEDERAL PA	1	1	1	1	1	0	1
GO	Catalão	158124 INST.FED.DE EDUC. CIENCIA E TEC. GOIANO	1	1	1	1	1	1	1
GO	Ceres	158124 INST.FED.DE EDUC. CIENCIA E TEC. GOIANO	1	1	1	1	1	1	1
MG	Contagem	200115 SUPERINTENDENCIA REG. POL. RODV. FEDERAL MG	43	43	43	43	43	9	43
AL	Coruripe	158147 INST.FED.DE EDUC.CIENC.E TEC.DE ALAGOAS	1	1	1	1	1	0	0
GO	Cristalina	158124 INST.FED.DE EDUC. CIENCIA E TEC. GOIANO	1	1	1	1	1	1	1

MT	Cuiabá	200120 SUPERINTENDENCIA REG. POL. RODV. FEDERAL_MT	15	15	15	15	15	1	1
PR	Curitiba	200118 SUPERINTENDENCIA REG. POL. RODV. FEDERAL PR	48	48	48	48	48	1	1
PA	Dom Eliseu	200111 SUPERINTENDENCIA REG. POL. RODV. FEDERAL PA	1	1	1	1	1	0	1
SC	Florianópolis	200125 SUPERINTENDENCIA REG. POL. RODV. FEDERAL SC	40	40	40	40	40	1	1
CE	Fortaleza	200112 SUPERINTENDENCIA REG. POL. RODV. FEDERAL CE	30	30	30	30	30	1	1
GO	Goiânia	200121 SUPERINTENDENCIA REG. POL. RODV. FEDERAL GO	13	10	10	10	10	2	1
SP	Guaiçara	200117 SUPERINTENDENCIA REG. POL. RODV. FEDERAL SP	1	1	1	1	1	0	1
SP	Guarulhos	200117 SUPERINTENDENCIA REG. POL. RODV. FEDERAL SP	3	3	3	3	3	4	3
GO	Hidrolândia	158124 INST.FED.DE EDUC. CIENCIA E TEC. GOIANO	1	1	1	1	1	1	1
GO	Ipameri	158124 INST.FED.DE EDUC. CIENCIA E TEC. GOIANO	1	1	1	1	1	1	1
PA	Ipixuna do Pará	200111 SUPERINTENDENCIA REG. POL. RODV. FEDERAL PA	1	1	1	1	1	0	1
GO	Iporá	158124 INST.FED.DE EDUC. CIENCIA E TEC. GOIANO	1	1	1	1	1	1	1
SP	Itapecerica da Serra	200117 SUPERINTENDENCIA REG. POL. RODV. FEDERAL SP	2	2	2	2	2	0	2
GO	Jataí	160102 41 BATALHAO DE INFANTARIA MOTORIZADO MEX GO	1	1	1	1	1	1	1
PB	João Pessoa	200122 SUPERINTENDENCIA REG. POL. RODV. FEDERAL PB	14	14	14	14	14	1	1
BA	Juazeiro	195006 CIA DE DESENV. DO VALE DO SAO FRANCISCO DF	1	1	1	1	1	0	1
MG	Juiz de Fora	160120 4. DEPOSITO DE SUPRIMENTO	1	1	1	1	1	1	1
SP	Lavrinhas	200117 SUPERINTENDENCIA REG. POL. RODV. FEDERAL SP	1	1	1	1	1	0	1
AP	Macapá	200233 SUPERINTENDENCIA REG. POL. RODV. FEDERAL AP	6	6	6	6	6	1	6
AL	Maceió	158147 INST.FED.DE EDUC.CIENC.E TEC.DE ALAGOAS	2	2	2	2	2	2	1
AL	Maceió	200129 SUPERINTENDENCIA REG. POL. RODV. FEDERAL AL	10	10	10	10	10	1	3
AM	Manaus	200110 SUPERINTENDENCIA REG. POL. RODV. FEDERAL AM	4	4	4	4	4	1	4
PA	Marabá	200111 SUPERINTENDENCIA REG. POL. RODV. FEDERAL PA	3	3	3	3	3	0	3
AL	Maragogi	152815 INSTITUTO FED.DE ALAGOAS CAMPUS MARAGOGI	1	1	1	1	1	0	0
AL	Marechal Deodoro	158380 INST.FED DE ALAGOAS CAMPOS MARECHAL DEODORO	1	1	1	1	1	0	0
SP	Marília	200117 SUPERINTENDENCIA REG. POL. RODV. FEDERAL SP	2	2	2	2	2	0	2

SP	Miracatu	200117 SUPERINTENDENCIA REG. POL. RODV. FEDERAL SP	2	2	2	2	2	0	2
MG	Montes Claros	195006 CIA DE DESENV. DO VALE DO SAO FRANCISCO DF	1	1	1	1	1	0	1
GO	Morrinhos	158124 INST.FED.DE EDUC. CIENCIA E TEC. GOIANO	1	1	1	1	1	1	1
AL	Murici	152803 CAMPUS MURICI INST. FED. EDUC. TEC AL	1	1	1	1	1	0	0
RN	Natal	200123 SUPERINTENDENCIA REG. POL. RODV. FEDERAL RN	15	15	15	15	15	1	5
SP	Ourinhos	200117 SUPERINTENDENCIA REG. POL. RODV. FEDERAL SP	1	1	1	1	1	0	1
TO	Palmas	200139 SUPERINTENDENCIA REG. POL. RODV. FEDERAL TO	8	8	8	8	8	3	2
AL	Penedo	152800 CAMPUS PENEDO_INSTITUTO FED. ED. ALAGOAS	1	1	1	1	1	0	0
AL	Penedo	195006 CIA DE DESENV. DO VALE DO SAO FRANCISCO DF	1	1	1	1	1	0	1
PE	Petrolina	195006 CIA DE DESENV. DO VALE DO SAO FRANCISCO DF	1	1	1	1	1	0	1
AL	Piranhas	152802 CAMPUS PIRANHAS INST. FED. DE EDUC. TEC AL	1	1	1	1	1	0	0
RS	Porto Alegre	200119 SUPERINTENDENCIA REG. POL. RODV. FEDERAL_RS	41	41	41	41	41	1	2
RO	Porto Velho	200131 SUPERINTENDENCIA REG. POL. RODV. FEDERAL RO	12	12	12	12	12	2	12
GO	Posse	158124 INST.FED.DE EDUC. CIENCIA E TEC. GOIANO	1	1	1	1	1	1	1
MG	Pouso Alegre	158137 INST.FED.DE EDUC.CIENC.E TEC.DO SUL DE MG	8	8	8	8	8	2	0
PE	Recife	195006 CIA DE DESENV. DO VALE DO SAO FRANCISCO DF	1	1	1	1	1	0	1
PE	Recife	200113 SUPERINTENDENCIA REG. POL. RODV. FEDERAL PE	20	20	20	20	20	20	20
SP	Registro	200117 SUPERINTENDENCIA REG. POL. RODV. FEDERAL SP	2	2	2	2	2	0	2
AC	Rio Branco	200235 SUPERINTENDENCIA REG. DA POL. RODOV. FED. AC	5	5	5	5	5	5	5
RJ	Rio de Janeiro	113201 SAE CNEN COMIS.NACIONAL DE ENERGIA NUCLEAR_RJ	18	18	18	18	18	2	2
RJ	Rio de Janeiro	153010 MEC CEFET CENT.FED.ED.TEC.CELSO S.FONSECA_RJ	1	1	1	1	1	0	0
RJ	Rio de Janeiro	160311 ESCOLA DE APERFEICOAMENTO DE OFICIAIS_RJ	2	2	2	2	2	2	2
RJ	Rio de Janeiro	200116 SUPERINTENDENCIA REG. POL. RODV. FEDERAL RJ	35	35	35	35	35	1	1
AL	Rio Largo	158147 INST.FED.DE EDUC.CIENC.E TEC.DE ALAGOAS	1	1	1	1	1	0	0
GO	Rio Verde	158124 INST.FED.DE EDUC. CIENCIA E TEC. GOIANO	1	1	1	1	1	1	1
SP	Roseira	200117 SUPERINTENDENCIA REG. POL. RODV. FEDERAL SP	1	1	1	1	1	0	1

PE	Salgueiro	195006 CIA DE DESENV. DO VALE DO SAO FRANCISCO DF	1	1	1	1	1	0	1
BA	Salvador	195006 CIA DE DESENV. DO VALE DO SAO FRANCISCO DF	1	1	1	1	1	0	1
BA	Salvador	200114 SUPERINTENDENCIA REG. POL. RODV. FEDERAL BA	23	23	23	23	23	5	23
PA	Santa Maria do Pará	200111 SUPERINTENDENCIA REG. POL. RODV. FEDERAL PA	1	1	1	1	1	0	1
AL	Santana do Ipanema	152801 CAMPUS SANTANA DO IPANEMA INST. FED. ALAGOAS	1	1	1	1	1	0	0
PA	Santarém	200111 SUPERINTENDENCIA REG. POL. RODV. FEDERAL PA	1	1	1	1	1	0	1
SP	São José do Rio Preto	200117 SUPERINTENDENCIA REG. POL. RODV. FEDERAL SP	2	2	2	2	2	0	2
SP	São José dos Campos	200117 SUPERINTENDENCIA REG. POL. RODV. FEDERAL SP	2	2	2	2	2	0	2
MA	São Luís	195006 CIA DE DESENV. DO VALE DO SAO FRANCISCO DF	1	1	1	1	1	0	1
MA	São Luís	200124 SUPERINTENDENCIA REG. POL. RODV. FEDERAL MA	20	20	20	20	20	20	5
AL	São Miguel dos Campos	152804 CAMPUS SAO MIGUEL DOS CAMPUS	1	1	1	1	1	0	0
SP	São Paulo	275068 COMPANHIA BRASILEIRA DE TRENS URBANOS	1	1	1	1	1	0	0
AL	Satuba	158382 INST.FED.ALAGOAS CAMPUS SATUBA	1	1	1	1	1	0	0
PE	Serra Talhada	158741 INST. FED. CAMPUS SERRA TALHADA	2	2	2	2	2	1	2
MT	Tangará da Serra	158492 INST.FED.MATO GROSSO CAMPUS NOVO PARECIS	1	0	1	0	0	0	0
SP	Taubaté	200117 SUPERINTENDENCIA REG. POL. RODV. FEDERAL SP	1	1	1	1	1	0	1
PI	Teresina	195006 CIA DE DESENV. DO VALE DO SAO FRANCISCO DF	1	1	1	1	1	0	1
PI	Teresina	200127 SUPERINTENDENCIA REG. POL. RODV. FEDERAL_PI	15	15	15	15	15	1	1
GO	Trindade	158124 INST.FED.DE EDUC. CIENCIA E TEC. GOIANO	1	1	1	1	1	1	1
SP	Ubatuba	200117 SUPERINTENDENCIA REG. POL. RODV. FEDERAL SP	2	2	2	2	2	0	2
GO	Urutaí	158124 INST.FED.DE EDUC. CIENCIA E TEC. GOIANO	1	1	1	1	1	1	1
SP	Vargem	200117 SUPERINTENDENCIA REG. POL. RODV. FEDERAL SP	1	1	1	1	1	0	1
AL	Viçosa	158147 INST.FED.DE EDUC.CIENC.E TEC.DE ALAGOAS	1	1	1	1	1	0	0
ES	Vitória	200126 SUPERINTENDENCIA REG. POL. RODV. FEDERAL ES	15	15	15	15	15	3	8
TOTAIS			694	688	691	688	688	128	240

			Lote 2						
Estado	Cidade	UASG/Órgão	item 8	item 9	item 10	item 11	item 12	item 13	item 14
ES	Aracruz	158419 INST.FED.DE ED.CIENC.E TEC.DO ES C.ARACRUZ	1	1	1	1	1	1	1
MG	Belo Horizonte	158122 INST.FED.DE EDUC.CIENCIA E TECNOLOGIA DE MG	12	12	12	12	12	2	2
RR	Boa Vista	200232 SUPERINTENDENCIA REG. POL. RODV. FEDERAL RR	1	1	1	1	1	1	1
DF	Brasília	201004 MP COORDENACAO GERAL DE AQUISIÇÕES	40	40	40	40	40	1	2
DF	Brasília	201057 SERVIÇO FLORESTAL BRASILEIRO – SFB-DF	2	2	2	2	2	2	2
MG	Cuiabá	158494 INST.FED.MATO GROSSO CAMPUS BELA VISTA	1	1	1	1	1	1	1
PB	João Pessoa	153065 MEC_UF UNIVERSIDADE FEDERAL DA PARAIBA PB	6	6	6	6	6	1	1
PB	João Pessoa	275068 COMPANHIA BRASILEIRA DE TRENS URBANOS	2	2	2	2	2	1	1
AL	Maceió	158147 INST.FED.DE EDUC.CIENC.E TEC.DE ALAGOAS	1	0	0	0	0	1	1
AL	Maceió	158381 INST.FED DE ALAGOAS CAMPOS MACEIO	1	1	1	1	1	0	0
AL	Maceió	275068 COMPANHIA BRASILEIRA DE TRENS URBANOS	2	2	2	2	2	0	0
RN	Natal	275068 COMPANHIA BRASILEIRA DE TRENS URBANOS	2	2	2	2	2	0	0
AL	Palmeira dos Índios	158383 INST.FED.DE ALAGOAS CAMPUS PALMEIRA DOS IND	1	1	1	1	1	0	0
MG	Pouso Alegre	158137 INST.FED.DE EDUC.CIENC.E TEC.DO SUL DE MG	1	1	1	1	1	1	0
RJ	Rio de Janeiro	153010 MEC CEFET CENT.FED.ED.TEC.CELSO S.FONSECA_RJ	7	7	7	7	7	2	0
RJ	Rio de Janeiro	160311 ESCOLA DE APERFEICOAMENTO DE OFICIAIS_RJ	2	2	2	2	2	2	2
GO	Rio Verde	158299 INST.FED.GOIANO CAMPUS RIO VERDE	2	2	2	2	2	2	2
BA	Salvador	200114 SUPERINTENDENCIA REG. POL. RODV. FEDERAL BA	1	0	0	0	0	1	1
SE	São Cristóvão	154050 MEC UNIVERSIDADE FEDERAL_SE	4	4	4	4	4	1	1
SP	São José dos Campos	113214 AGÊNCIA NACIONAL DE AVIAÇÃO CIVIL ANAC SP	2	2	2	2	2	0	0
SP	São Paulo	113214 AGÊNCIA NACIONAL DE AVIAÇÃO CIVIL ANAC SP	2	2	2	2	2	1	1
PI	Teresina	158146 INST.FED.DE EDUC.CIENC. E TECNOLOGIA PIAUI	1	1	1	1	1	1	1
TOTAIS			94	92	92	92	92	22	20

	Lote 3

Estado	Cidade	UASG/Órgão	item 15	item 16	item 17	item 18	item 19	item 20	item 21
ES	Alegre	158425 INST.FED.DE ED.CIENC.E TEC.DO ES C.ALEGRE	2	2	2	2	2	1	1
SE	Aracajú	155017 EBSERH HOSPITAL UNIVERSITARIO DE SERGIPE	1	1	1	1	1	1	1
ES	Aracruz	158419 INST.FED.DE ED.CIENC.E TEC.DO ES C.ARACRUZ	1	1	1	1	1	1	1
PA	Belém	200111 SUPERINTENDENCIA REG. POL. RODV. FEDERAL PA	2	2	2	2	2	1	2
PA	Belém	240125 MUSEU PARAENSE EMILIO GOELDI	2	2	2	0	0	1	0
MG	Belo Horizonte	158122 INST.FED.DE EDUC.CIENCIA E TECNOLOGIA DE MG	4	4	4	4	4	2	3
MG	Belo Horizonte	275068 COMPANHIA BRASILEIRA DE TRENS URBANOS	2	2	2	2	2	0	0
SC	Blumenau	158125 INST.FED.DE EDUC. CIENC. E TEC. CATARINENSE	1	1	1	1	1	1	1
RR	Boa Vista	200232 SUPERINTENDENCIA REG. POL. RODV. FEDERAL RR	2	2	2	2	2	2	2
DF	Brasília	113214 AGÊNCIA NACIONAL DE AVIAÇÃO CIVIL ANAC DF	2	2	0	0	0	1	1
DF	Brasília	154040 FUNDAÇÃO UNIVERSIDADE DE BRASÍLIA FUB	4	4	4	4	4	2	1
DF	Brasília	160064 COLEGIO MILITAR DE BRASILIA_MEX_DF	2	2	2	2	2	1	2
DF	Brasília	200005 MJ CGS COORDENACAO GERAL DE LOGISTICA_DF	10	10	10	10	10	1	1
DF	Brasília	200141 SUPERINTENDENCIA REG. POL. RODV. FEDERAL DF	1	1	1	1	1	1	1
DF	Brasília	201004 MP COORDENACAO GERAL DE AQUISIÇOES	4	4	4	4	4	2	2
DF	Brasília	926142 DEPARTAMENTO DE TRÂNSITO DO DISTRITO FEDERAL	2	2	2	2	2	1	1
ES	Cachoeiro do Itapemirim	158418 INST.FED.DE ED.CIENC.E TEC.DO ES C.CACHOEIRO	2	2	2	2	2	1	1
MS	Campo Grande	200128 SUPERINTENDENCIA REG. POL. RODV. FEDERAL MS	2	2	2	2	2	1	1
ES	Campus Nova Venécia	158422 INST.FED.DE ED. CIENC.E TEC.DO ES C.N.VENÉCIA	2	2	2	2	2	1	1
MG	Contagem	200115 SUPERINTENDENCIA REG. POL. RODV. FEDERAL MG	1	1	1	1	1	1	1
MG	Cuiabá	158494 INST.FED.MATO GROSSO CAMPUS BELA VISTA	1	1	1	1	1	1	1
MT	Cuiabá	200120 SUPERINTENDENCIA REG. POL. RODV. FEDERAL_MT	1	1	1	1	1	1	1
PR	Curitiba	153079 UNIVERSIDADE FEDERAL DO PARANÁ – UFPR	5	5	5	5	5	2	1
PR	Curitiba	200118 SUPERINTENDENCIA REG. POL. RODV. FEDERAL PR	2	2	2	2	2	1	1
SC	Florianópolis	200125 SUPERINTENDENCIA REG. POL. RODV. FEDERAL SC	2	2	2	2	2	1	1

CE	Fortaleza	200112 SUPERINTENDENCIA REG. POL. RODV. FEDERAL CE	2	2	2	2	2	1	1
GO	Goiânia	158124 INST.FED.DE EDUC. CIENCIA E TEC. GOIANO	1	1	1	1	1	1	1
GO	Goiânia	200121 SUPERINTENDENCIA REG. POL. RODV. FEDERAL GO	1	1	1	1	1	2	1
ES	Guarapari	158883 INST.FED.DO ESPIRITO SANTO_CAMPUS GUARAPARI	2	2	2	2	2	1	1
ES	Itapina	158424 INST.FED.DO ES CAMPUS ITAPINA	2	2	2	2	2	1	2
PB	João Pessoa	200122 SUPERINTENDENCIA REG. POL. RODV. FEDERAL PB	1	1	1	1	1	1	1
CE	Juazeiro do Norte	158316 INST.FED.DO CEARA CAMPUS JUAZEIRO DO NORTE	3	3	3	3	3	3	3
MG	Juiz de Fora	158414 INST.F.ED.CIENC.E TEC DO SUD.DE MG C.J.FORA	2	2	2	2	2	2	2
ES	Linhares	158420 INST.FED.DE ED.CIENC.E TEC.DO ES_C.LINHARES	2	2	2	2	2	1	1
AP	Macapá	200233 SUPERINTENDENCIA REG. POL. RODV. FEDERAL AP	2	2	2	2	2	1	2
AL	Maceió	158147 INST.FED.DE EDUC.CIENC.E TEC.DE ALAGOAS	1	1	1	1	1	1	1
AL	Maceió	200129 SUPERINTENDENCIA REG. POL. RODV. FEDERAL AL	2	2	2	2	2	2	2
AM	Manaua	200110 SUPERINTENDENCIA REG. POL. RODV. FEDERAL AM	2	2	2	2	2	1	2
ES	Montanha	158884 CAMPUS MONTANHA_IFECT ES	2	2	2	2	2	1	1
RN	Natal	200123 SUPERINTENDENCIA REG. POL. RODV. FEDERAL RN	2	2	2	2	2	2	2
TO	Palmas	200139 SUPERINTENDENCIA REG. POL. RODV. FEDERAL TO	2	2	2	2	2	2	2
RS	Porto Alegre	200119 SUPERINTENDENCIA REG. POL. RODV. FEDERAL_RS	2	2	2	2	2	1	2
RO	Porto Velho	200131 SUPERINTENDENCIA REG. POL. RODV. FEDERAL RO	2	2	2	2	2	2	2
PE	Recife	200113 SUPERINTENDENCIA REG. POL. RODV. FEDERAL PE	2	2	2	2	2	2	2
PE	Recife	275068 COMPANHIA BRASILEIRA DE TRENS URBANOS	2	2	2	2	2	0	0
AC	Rio Branco	200235 SUPERINTENDENCIA REG. DA POL. RODOV. FED. AC	2	2	2	2	2	2	2
RJ	Rio de Janeiro	113201 SAE CNEN COMIS.NACIONAL DE ENERGIA NUCLEAR_RJ	10	10	10	10	10	2	5
RJ	Rio de Janeiro	113214 AGÊNCIA NACIONAL DE AVIAÇÃO CIVIL ANAC RJ	2	2					
RJ	Rio de Janeiro	153010 MEC CEFET CENT.FED.ED.TEC.CELSO S.FONSECA_RJ	2	2	2	2	2	2	1
RJ	Rio de Janeiro	153133 MEC FACULDADE DE ECONOMIA E ADMINISTACAO UFRJ	2	2	2	2	2	2	2
RJ	Rio de Janeiro	160296 COMANDO BRIGADA INFANTARIA PARAQUEDISTA_RJ	1	1	1	1	1	1	1

RJ	Rio de Janeiro	160311 ESCOLA DE APERFEICOAMENTO DE OFICIAIS_RJ	2	2	2	2	2	2	2
RJ	Rio de Janeiro	200116 SUPERINTENDENCIA REG. POL. RODV. FEDERAL RJ	4	4	4	4	4	1	4
RJ	Rio de Janeiro	275068 COMPANHIA BRASILEIRA DE TRENS URBANOS	2	2	2	2	2	1	1
GO	Rio Verde	158299 INST.FED.GOIANO CAMPUS RIO VERDE	1	1	1	1	1	1	1
BA	Salvador	200114 SUPERINTENDENCIA REG. POL. RODV. FEDERAL BA	1	1	1	1	1	1	1
BA	Salvador	254422 CENTRO DE PESQUISAS GONCALO MUNIZ FIOCRUZ	2	2	2	2	2	2	2
ES	Santa Teresa	158426 INST.FED.DE ED.CIENC.E TEC DO ES C.S.TERESA	2	2	2	2	2	1	1
SE	São Cristóvão	154050 MEC UNIVERSIDADE FEDERAL_SE	4	4	4	4	4	1	1
MA	São Luis	200124 SUPERINTENDENCIA REG. POL. RODV. FEDERAL MA	2	2	2	2	2	2	2
SP	São Paulo	200117 SUPERINTENDENCIA REG. POL. RODV. FEDERAL SP	2	2	2	2	2	1	2
PI	Teresina	158146 INST.FED.DE EDUC.CIENC. E TECNOLOGIA PIAUí	1	1	1	1	1	1	1
PI	Teresina	200127 SUPERINTENDENCIA REG. POL. RODV. FEDERAL_PI	2	2	2	2	2	1	1
MG	Viçosa	154051 UNIVERSIDADE FEDERAL DE VICOSA	2	2	2	2	2	1	2
ES	Vila Velha	158427 IFE.CIENC.E TEC.DO ES CAMPUS VILA VELHA	1	1	1	1	1	1	1
ES	Vinda do Novo Imigrante	158429 IFE.CIENC.TEC DO ES C.V.N.DO IMIGRANTE	1	1	1	1	1	1	1
ES	Vitória	200126 SUPERINTENDENCIA REG. POL. RODV. FEDERAL ES	2	2	2	2	2	2	2
TOTAIS			147	147	143	141	141	86	96

			Lote 4						
Estado	Cidade	UASG/ Órgão	item 22	item 23	item 24	item 25	item 26	item 27	item 28
SE	Aracajú	158393 INST.FED.DE ED.CIENC.E TEC.DE SE C.ARACAJU	1	1	1	1	1	1	0
DF	Brasília	113214 AGÊNCIA NACIONAL DE AVIAÇÃO CIVIL ANAC DF	2	2	2	2	2	1	1
DF	Brasília	160070 DEPARTAMENTO GERAL DE PESSOAL MEX_DF	2	2	2	2	2	2	2
DF	Brasília	170531 SUPERINTENDÊNCIA DE ADMINISTRAÇÃO DO MF DF	2	2	2	2	2	1	1
DF	Brasília	195006 CIA DE DESENV. DO VALE DO SAO FRANCISCO DF	2	2	2	2	2	1	2
DF	Brasília	201004 MP COORDENACAO GERAL DE AQUISIÇOES	6	6	6	6	6	2	2

DF	Brasília	343026 IPHAN INST. PATR. HIST. E ARTISTICO NACIONAL	2	2	2	2	2	1	1
DF	Brasília	443033 COORDENAÇAO GERAL DE FINANÇAS_DF	2	2	2	2	2	1	1
SE	Estância	152426 INSTITUTO FEDERAL DE SERGIPE CAMPUS ESTANCIA	1	1	1	1	1	1	0
SC	Florianópolis	200229 COORDENAÇÃO DE ENSINO COEN CGRH PRF MJ	2	2	2	2	2	2	2
SE	Gloria	152420 INSTITUTO FEDERAL DE SERGIPE CAMPUS GLORIA	1	1	1	1	1	1	0
SE	Itabiana	152430 INSTITUTO FEDERAL DE SERGIPE CAMPUS ITABAIANA	1	1	1	1	1	1	0
PB	João Pessoa	153065 MEC_UF UNIVERSIDADE FEDERAL DA PARAIBA PB	2	2	2	2	2	1	1
SE	Lagarto	158394 INST FED.DE SERGIPE CAMPUS LAGARTO SE	1	1	1	1	1	1	0
AM	Manaus	240105 INSTIT.NACIONAL DE PESQUISA DA AMAZONIA_MCT	2	2	2	2	2	2	2
PE	Petrolina	154716 HOSP. ENSINO UNIVASF	2	2	2	2	2	2	2
SE	Propria	154681 IFCT SE CAMPUS PROPRIA	1	1	1	1	1	1	0
RJ	Rio de Janeiro	113214 AGÊNCIA NACIONAL DE AVIAÇÃO CIVIL ANAC RJ	2	2	2	2	2	0	0
RJ	Rio de Janeiro	153010 MEC CEFET CENT.FED.ED.TEC.CELSO S.FONSECA_RJ	2	2	2	2	2	1	1
RJ	Rio de Janeiro	160296 COMANDO BRIGADA INFANTARIA PARAQUEDISTA_RJ	1	1	1	1	1	1	1
RJ	Rio de Janeiro	160298 COMANDO DA 1 REGIAO MILITAR RJ	2	2	2	2	2	2	2
RJ	Rio de Janeiro	160311 ESCOLA DE APERFEICOAMENTO DE OFICIAIS_RJ	2	2	2	2	2	2	2
RJ	Rio de Janeiro	250059 INSTITUTO NACIONAL DE CARDIOLOGIA	2	2	2	2	2	2	2
SE	Santana do Livramento	158134 INST.FED.DE EDUC. CIENC.E TEC.DE SERGIPE	1	1	1	1	1	1	1
SE	São Cristóvão	158392 INST.F.DE ED. CIENC.E TEC.DE SE C.S.CRISTOVÃO	1	1	1	1	1	1	0
SP	São Paulo	113202 COMISSAO NACIONAL DE ENERGIA NUCLEAR	2	2	2	2	2	2	2
RS	Sapucaia do Sul	158339 INST.FED.SUL R.GRANDENSE SAPUCAIA DO SUL	1	1	1	1	1	1	1
PI	Teresina	158146 INST.FED.DE EDUC.CIENC. E TECNOLOGIA PIAUí	1	1	1	1	1	1	1
SE	Tobias Barreto	154679 IFCT SE CAMPUS TOBIAS BARRETO	1	1	1	1	1	1	0
MG	Viçosa	154051 UNIVERSIDADE FEDERAL DE VICOSA	2	2	2	2	2	1	2
ES	Vitória	158416 INST.FED.DE ED.CIENC.E TEC.DO ES_C. VITÓRIA	2	2	2	2	2	1	1
TOTAIS			54	54	54	54	54	39	33

			Lote 5						
Estado	Cidade	UASG/Órgão	item 29	item 30	item 31	item 32	item 33	item 34	item 35
SE	Aracajú	158134 INST.FED.DE EDUC. CIENC.E TEC.DE SERGIPE	1	1	1	1	1	1	1
DF	Brasília	110245 FUNDO DE IMPRENSA NACIONAL – DF	3	3	3	3	3	3	3
DF	Brasília	195006 CIA DE DESENV. DO VALE DO SAO FRANCISCO DF	2	2	2	2	2	1	2
DF	Brasília	200005 MJ CGS COORDENACAO GERAL DE LOGISTICA_DF	4	4	4	4	4	1	1
PR	Curitiba	153079 UNIVERSIDADE FEDERAL DO PARANÁ – UFPR	2	2	2	2	2	1	1
SC	Florianópolis	153163 MEC UNIV. FED. DE SANTA CATARINA SC	2	2	2	2	2	1	1
RJ	Rio de Janeiro	160296 COMANDO BRIGADA INFANTARIA PARAQUEDISTA_RJ	1	1	1	1	1	1	1
RJ	Rio de Janeiro	160311 ESCOLA DE APERFEICOAMENTO DE OFICIAIS_RJ	2	2	2	2	2	2	2
BA	Salvador	153038 UNIVERSIDADE FEDERAL DA BAHIA UFBA	2	2	2	2	2	1	2
SE	São Cristóvão	154050 MEC UNIVERSIDADE FEDERAL_SE	4	4	4	4	4	1	1
TOTAIS			23	23	23	23	23	13	15

ANEXO "D" DO TERMO DE REFERÊNCIA
MODELO DE COMPROVAÇÃO PONTUAL DE ATENDIMENTO À ESPECIFICAÇÃO TÉCNICA

LOTE	ITEM	ITEM	DESCRIÇÃO	PROPOSTA ATENDE? (SIM OU NÃO)	REFERENCIA NA DOCUMENTAÇÃO TÉCNICA	OBSER-VAÇÃO
.	.	.	.	.	.	.
.	.	.	.	.	.	.
.	.	.	.	.	.	.

ANEXO "E" DO TERMO DE REFERÊNCIA
TESTES DE CONFORMIDADE

Definição

O teste de conformidade da amostra visa à aferição da real capacidade técnica dos equipamentos ofertados pela Licitante Convocada. Busca-se comprovar,

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 serão efetuados em todos os itens de hardware e software da solução, em todos os lotes.

2. Disposições gerais

2.1. O Teste de Conformidade deverá ser realizado em laboratório a ser disponibilizado pela Licitante na cidade de Brasília-DF ou em local indicado pelo grupo técnico de apoio ao pregoeiro, na cidade de Brasília-DF. A decisão final sobre a localidade de realização dos testes será tomada pelo referido grupo técnico e informada pelo pregoeiro.

2.2. Após a avaliação da proposta da licitante mais bem colocada, o pregoeiro solicitará o envio do Caderno de Testes, de acordo com o item 16.11 deste Termo de Referência.

2.3. O Teste de Conformidade será feito com base no Caderno de Testes aprovado pelo grupo técnico de apoio ao pregoeiro. Nesse caderno deverão ser incluídos, pelo menos, os testes descritos e na ordem especificada no item 5 deste Anexo.

2.4. O prazo para apresentação do Caderno de Testes será de até 7 dias úteis a partir da solicitação de apresentação feita pelo pregoeiro. Além disso, o grupo técnico 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 deste Termo de Referência.

2.5. Caso o Caderno de Testes seja rejeitado ou necessite de alterações pelo grupo técnico, a Licitante terá um prazo de até 3 dias úteis para a realização das devidas correções e reapresentar o documento para a validação do grupo técnico.

2.6. A validação do Caderno de Testes não pode exceder 2 análises por parte do grupo técnico de apoio.

2.7. Após a aprovação do Caderno de Testes, o pregoeiro solicitará à Licitante uma amostra dos itens do lote da mesma marca e modelo ofertado na proposta, a fim de apurar o atendimento das especificações técnicas constantes no Anexo B, de acordo com o item 16.12 do Termo de Referência e o item 3 deste Anexo.

2.8. A amostra que será utilizada na execução do Teste de Conformidade deverá ser disponibilizada no laboratório em que se realizarão os testes, de acordo com o item 2.2 deste Anexo, no prazo de até 30 dias corridos, contados a partir da solicitação do pregoeiro.

2.8.1. O pregoeiro solicitará à LICITANTE do melhor lance o prazo estimado para atendimento do prazo anterior (até 30 dias corridos) ao estabelecido, a fim de agendar a reabertura do pregão.

2.9. Após o recebimento da amostra no laboratório, a Licitante terá até 5 dias úteis, a partir da solicitação do pregoeiro, para que a amostra, bem como o ambiente, estejam prontos para o início do Teste de Conformidade, atendendo ao item 2.22 deste Anexo.

2.10. Em seguida, o pregoeiro, suportado pelo grupo técnico, definirá a data de início dos testes, ocasião em que comunicará via sistema tal data às licitantes participantes do certame.

2.11. Após iniciado, o Teste de Conformidade deverá seguir o roteiro definido no Caderno de Teste e terá duração máxima de até 5 dias úteis.

2.12. O Teste de Conformidade deverá ser executado em dia útil, de segunda-feira à sexta-feira, das 08:00 horas às 18:00 horas, com previsão de até 2 horas de almoço.

2.13. A Licitante Convocada deverá indicar previamente, em até 2 dias úteis após a solicitação de envio do Caderno de Testes descrita no item 2.3 deste Anexo, 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 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.

2.13.1. Será permitida a substituição de quaisquer dos componentes da Equipe Técnica da Licitante Convocada para os testes, mediante a autorização prévia do pregoeiro.

2.14. Cada uma das demais licitantes participantes do pregão que queira acompanhar o Teste de Conformidade deverá indicar previamente, em até 2 dias úteis após a solicitação de envio do Caderno de Testes descrita no item 2.3 deste Anexo, 1 (um) técnico ou representante legal da licitante participante ou do fabricante da solução participante ofertada, devidamente identificado por meio de vínculo contratual ou procuração, como "Técnico de Acompanhamento da Licitante Participante".

2.14.1. Não será permitida a substituição de qualquer Técnico de Acompanhamento da Licitante Participante sem a autorização prévia do pregoeiro.

2.15. Durante a realização dos testes, não será permitida a comunicação 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 de apoio a contratação.

2.15.1. A não observância da regra de comunicação especificada no item anterior poderá causar o descredenciamento unilateral, de quaisquer dos componentes da Equipe Técnica da Licitante Convocada ou de qualquer Técnico de Acompanhamento da Licitante Participante.

2.15.2. Quaisquer pessoas que venham dificultar o bom andamento dos testes e os trabalhos da equipe técnica responsável pelo acompanhamento de apoio ao pregoeiro poderão ser descredenciadas de forma unilateral e não mais participarão dos Testes de Conformidade.

2.16. O grupo técnico de apoio ao pregoeiro poderá solicitar alteração ou adequação durante o Teste de Conformidade, mesmo com o Caderno de Testes apresentado e aprovado, com a finalidade de dirimir quaisquer dúvidas referentes a itens da especificação técnica.

2.17. A fim de evitar quaisquer vícios nos testes, o grupo técnico de apoio ao pregoeiro, a qualquer momento e mesmo depois da validação do Caderno de Testes, poderá solicitar alterações nas gerações das ameaças, ataques, aplicações, percentuais ajustáveis de tamanho de pacote, políticas, tipos de tráfego, dentre outros, para todos os componentes da solução.

2.18. O Ministério do Planejamento, Desenvolvimento e Gestão, em situações excepcionais e de interesse da Administração Pública, reserva-se o direito de suspender temporariamente a execução do Teste de Conformidade, com a respectiva suspensão dos seus prazos de completa execução.

2.19. Caso uma mesma Licitante seja convocada para realização de testes em mais de um lote, com solução idêntica (*firewall* e gerência centralizada) por ela ofertada, o teste a ser realizado poderá ser o do lote de maior porte, sendo dispensado o teste para o lote de menor porte.

2.20. 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.

2.21 Caso o laboratório de testes seja disponibilizado pela LICITANTE deverá, no mínimo:

i) Contar com área mínima de 40 m² a fim de permitir o acompanhamento adequado dos testes, sem aglomeração de pessoas no espaço do laboratório;

ii) Possuir ar condicionado;

iii) Possuir, pelo menos, 1 projetor e 4 monitores espalhados pelo laboratório, a fim de permitir o acompanhamento dos testes pelo grupo técnico de apoio, pelos técnicos de acompanhamento das licitantes participantes e da equipe técnica da licitante convocada;

iv) Possuir cadeiras para, pelo menos, 25 pessoas;

v) Possuir iluminação adequada;

vi) Possuir identificação em todos os cabos de comunicação;

vii) Prover segurança e controle de acesso à localidade dos testes, a fim de garantir a integridade do ambiente e da solução testada, para que não haja possibilidade de qualquer tipo de adulteração ao processo.

2.22. A solução ofertada, bem como os 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 pregoeiro.

2.22.1. A não observância desse item poderá acarretar o reinício do Teste de Conformidade, não interrompendo a contagem do prazo do item 2.11 deste Anexo E ou mesmo na reprovação da solução ofertada.

2.23. Não caberá ao Ministério do Planejamento, Desenvolvimento e Gestão, sob nenhuma hipótese, o pagamento de nenhum tipo de indenização, em virtude da realização do Teste de Conformidade, seja a solução ofertada aprovada ou reprovada.

2.24. A licitante deve disponibilizar em até 5 dias úteis contados da data da finalização dos testes o Relatório dos Testes da Amostra, o qual deverá conter todas as informações e resultados apurados durante os testes.

2.25. No Relatório dos Testes de Amostra deverá constar, no mínimo: informações da topologia do ambiente de teste utilizado, arquivos, impressões de telas, scripts de configuração, versões de software utilizadas e registros de logs com evidências capturadas e quaisquer informações que a equipe de apoio ao pregoeiro ache pertinente, seguindo a estrutura estabelecida no Caderno de Teste. O relatório deve ser fornecido de maneira impressa e digital. Ou seja, espera-se do relatório a mesma sequência do Caderno de Teste as respectivas comprovações e ou evidências para os itens constante deste documento.

2.26. A equipe técnica de apoio ao pregoeiro emitirá no prazo de 5 dias úteis após a entrega do Relatório dos Testes da Amostra, o TERMO DE AVALIAÇÃO DE AMOSTRA. Tal termo informará se a Amostra foi ou não aprovada no Teste de Conformidade, descrito no item 5 deste anexo. Caso o TERMO DE AVALIAÇÃO DE AMOSTRA indique que a amostra foi aprovada no Teste de Conformidade, essa será considerada homologada e a licitante será habilitada.

2.28. Caso o TERMO DE AVALIAÇÃO DE AMOSTRA indique que a amostra não foi aprovada no Teste de Conformidade, as não conformidades serão listadas e a LICITANTE CONVOCADA terá o prazo de 3 dias úteis, não prorrogáveis, a contar da comunicação do pregoeiro, para realização dos testes complementares.

2.28.1. A licitante deve disponibilizar em até 3 dias úteis contados da data da finalização dos testes complementares o Relatório dos Testes Complementares da Amostra, o qual deverá conter todas as informações e resultados, apurados durante os testes.

2.29. A Equipe Técnica de apoio ao pregoeiro emitirá, no prazo de até 3 (três) dias após a conclusão dos testes complementares, o novo TERMO DE AVALIAÇÃO DE AMOSTRA, que informará se a nova amostra foi ou não aprovada no Teste de Conformidade.

2.29.1. Caso o novo TERMO DE AVALIAÇÃO DE AMOSTRA indique a total conformidade da AMOSTRA, essa será considerada homologada e a proposta da LICITANTE será aceita.

2.29.2. 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.

2.30. A não realização, a realização incompleta ou a não comprovação de quaisquer dos itens do Teste de Conformidade acarretarão na reprovação da solução ofertada e a consequente desclassificação da LICITANTE.

2.31. No caso de inabilitação da LICITANTE por não aprovação de AMOSTRA, o pregoeiro convocará o próximo LICITANTE detentor de proposta válida, obedecida a classificação na etapa de lances, sucessivamente, até que um LICITANTE cumpra integralmente as especificações e os procedimentos previstos neste Termo de Referência.

2.32. A ordem de realização dos testes de conformidade deve obedecer a sequência dos lotes que atendem o maior número de órgãos. No entanto, essa ordem pode ser alterada a critério da Administração Pública.

3. Amostra

3.1. Para o Teste de Conformidade, a LICITANTE Convocada deverá apresentar uma AMOSTRA da solução ofertada, que deverá ser composta por:

(i) 1 (um) equipamento *firewall* multifuncional;

(ii) 1 (uma) solução de gerenciamento centralizado;

(iii) demais equipamentos que compõem a solução apresentada na proposta;

(iv) todas as licenças e *softwares* necessários ao funcionamento da solução;

(v) cabos, conectores, kits de fixação, trilhos, fibras óticas, *patchcords*, *transceivers* e demais acessórios necessários à sua instalação e operação.

3.2. A solução de gerenciamento centralizado deverá ser instalada, executada e acessada em equipamentos providos pela própria Licitante Convocada (servidor de virtualização, desktops, notebooks, etc.), observado o disposto no item 2.20 deste Anexo.

3.3. 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 quaisquer dúvidas, a fim de que possam ser realizados procedimentos de verificação de conformidade com as especificações técnicas constantes deste Termo de Referência.

4. Preparação Inicial

4.1. Todos os componentes da solução ofertada deverão ser, antes de iniciado o Teste de Conformidade, submetidos a procedimento de limpeza e exclusão dos dados de forma a zerar quaisquer configurações.

4.2. A solução ofertada deverá então ser atualizada para a versão mais recente 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 meses de liberação de uso para o mercado, será admitida a utilização da versão imediatamente anterior.

4.3. A versão utilizada do *firmware* deverá ter a comprovação de sua integridade realizada por meio da comparação dos *hashes* da versão de firmware utilizada nos testes e a disponibilizada no sítio oficial do fabricante.

4.3.1. Não serão aceitos firmwares pré-instalados.

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

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

4.4. Toda configuração da amostra deve ser feita item a item, em linha de comando ou interface gráfica, de forma que se permita o acompanhamento inequívoco por parte da equipe técnica.

4.5. Ao final de todo o procedimento de configuração inicial deverá ser realizado backup em DVD ou *pendrive* ou drive externo com a geração de *hash* do(s) arquivo(s), sendo uma cópia entregue ao grupo técnico de apoio ao pregoeiro. Este *backup* poderá ser restaurado no início de cada teste para agilizar os procedimentos.

4.6. Uma vez que a solução ofertada tenha sido atualizada na forma do item 4.5, não será mais permitida nenhuma atualização adicional durante a execução de todo o Teste de Conformidade.

4.7. A LICITANTE Convocada deverá prover equipamentos especializados de geração de tráfego e ameaças, observado o item 2.23 deste Anexo, ou seja, sem custos adicionais aos ofertados.

4.8. O conjunto de equipamentos especializados de geração de tráfego e ameaças, a ser utilizado no testes em comento, deverá ser capaz de gerar, no mínimo, 100 (cem) aplicações e 5.000 (cinco mil) ameaças ou ataques de tipos variados, *stateful* e *stateless*, encapsuladas em protocolos diversos, incluindo HTTP, HTTPS, protocolos de e-mail, vídeo conferência, VoIP, FTP, VPN e métodos de ofuscação.

4.9. Antes da execução dos testes, deverá ser realizada uma aferição do gerador de tráfego da seguinte forma: as portas geradoras e receptoras deverão estar em *loop*, no qual serão gerados os tráfegos com os respectivos percentuais solicitados neste Anexo, bem como as ameaças. A mesma quantidade de tráfego, com as mesmas características, deverá, então, ser equivalente entre as portas geradoras e receptoras. A documentação do processo deverá gerar, como insumos, arquivos do tipo PCAP, estatísticas do gerador ou similares.

4.10. A aferição de *throughput* de tráfego durante os testes deve ter por base os dados gerados e obtidos pelo gerador de tráfego.

5. Teste de Conformidade

Para um melhor entendimento desta seção, são descritas abaixo suas divisões:

(i) Configurações de Testes e Topologia: tem como objetivo, definir um catálogo de configurações da amostra, a topologia e o tráfego para os testes. Os itens desse catálogo serão demandados especificamente no início de cada teste.

(ii) Teste de assertividade: tem como objetivo, mensurar a eficácia das funcionalidades da amostra, em relação às categorizações, os bloqueios e às detecções de ameaças, ataques, URLs e aplicações.

(iii) Teste de desempenho: tem como objetivo, mesurar o desempenho da amostra em consonância com os requisitos técnicos exigidos no anexo "B", em relação à taxa de transferência (*throughtput*) e performance.

(iv) Teste de sessões: tem como objetivo, mensurar o desempenho da amostra em consonância com os requisitos técnicos exigidos no anexo "B", em relação às novas sessões por segundo e sessões simultâneas.

5.1. Configurações de Testes e Topologia

5.1.1. A amostra deverá ser configurada com as funcionalidades de *firewall*, tal como previstas na especificação técnica do Anexo B, contendo identificação de usuários, identificação dos países de origem e destino das comunicações (geolocalização), controle de acesso (controle de aplicações e filtragem de URL's), sistema de detecção/prevenção a intrusão/ataques (IDS/IPS), proteção contra ameaças (Antivírus e *Anti-malware*), administração de largura de banda de serviço (QoS), descriptografia, inspeção de tráfego SSL e suporte para conexões VPN IPSec.

5.1.1.1. Destaca-se que, durante a realização dos testes, a amostra será avaliada com as funcionalidades dos itens 2.1, 2.3, 2.4, 2.5 e 2.6 habilitadas, salvo quando houver indicação explícita contrária neste documento, permitindo sempre que possível inspeção por fluxo.

5.1.2. A amostra deve ser configurada com seus módulos de sistema de detecção/prevenção à intrusão/ataques (IDS/IPS), proteção contra ameaças (Antivírus e *Anti-malware*) e controle de acesso (controle de aplicações e filtragem de URL's) habilitados pelo fabricante para ambientes empresariais ou *enterprise* em modo de detecção. Sendo submetida a:

(i) ataques de, no mínimo, 2.000 (duas mil) assinaturas distintas de IPS/IDS;

(ii) ameaças de, no mínimo 2.000 (duas mil) assinaturas de *malwares* distintas;

(iii) acessos de, no mínimo, 5.000 (cinco mil) sites distintos de internet, distribuídos em, no mínimo, 40 (quarenta) categorias ou subcategorias distintas;

(iv) um mínimo de 100 (cem) aplicações.

5.1.2.1. Os ataques, ameaças, sites e aplicações acima serão previamente apresentados no caderno de teste.

5.1.3. 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.

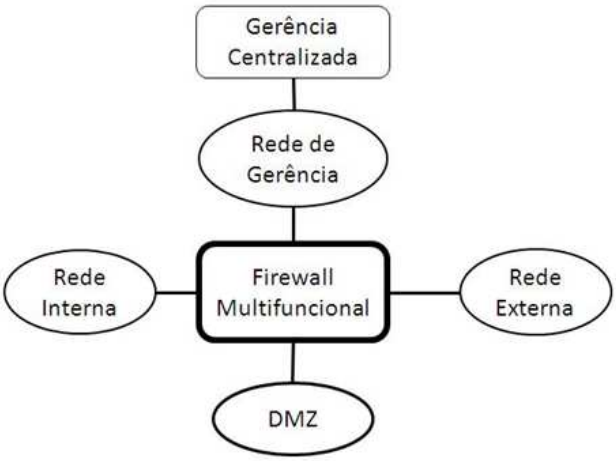
5.1.4. A amostra deve ser configurada de forma a registrar todos os tráfegos autorizados ou bloqueados, bem como todas as aplicações e ameaças detectadas pelo *Firewall* Multifuncional.

5.1.4.1. Os testes serão analisados pelo grupo técnico de apoio ao pregoeiro com base nos dados gerados e obtidos pelo gerador de tráfego, sendo complementado, quando necessário, pelos dados obtidos pela amostra.

5.1.5. Durante a realização dos testes, será avaliada a solução de gerência local e centralizada, que devem permanecer acessíveis, possibilitando a modificação e aplicação de políticas de segurança, bem como a visualização dos logs de acesso e de detecção de ameaças e aplicações, por CLI e/ou por GUI (interface

gráfica) a critério do grupo técnico de apoio ao pregoeiro.

5.1.6. A amostra e demais equipamentos devem ser instalados e configurados de forma a simular uma arquitetura de rede básica conforme a figura abaixo, a ser ajustada e homologada no Caderno de Testes.



5.1.7. 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 utilizada para este fim, conforme o item 2.1.45 das especificações técnicas presentes no Anexo B do Termo de Referência.

5.1.8. A Rede Interna deverá possuir clientes, considerando 1 (um) IP para cada cliente, que deverão acessar a DMZ e a Rede Externa, a qual deverá ser acessada por meio de NAT N-1. A quantidade de clientes varia de acordo com o porte do lote, conforme especificado a seguir:

i) Lote 1, pelo menos 50 clientes.

ii) Lote 2, pelo menos 125 clientes.

iii) Lote 3, pelo menos 500 clientes.

iv) Lote 4, pelo menos 1.500 clientes.

v) Lote 5, pelo menos 2.500 clientes.

5.1.9. A DMZ deverá possuir servidores, considerando 1 IP para cada servidor, que deverão ser acessados pela Rede Externa por meio de NAT 1-1. A quantidade de servidores varia de acordo com o porte do lote, conforme especificado a seguir:

i) Lote 1, pelo menos 5 servidores.

ii) Lote 2, pelo menos 13 servidores.

iii) Lote 3, pelo menos 50 servidores.

iv) Lote 4, pelo menos 200 servidores.

v) Lote 5, pelo menos 400 servidores.

5.1.10. A Rede Externa deverá possuir clientes, considerando 1 IP para cada cliente, que farão acesso aos servidores da DMZ, e mais servidores, que serão acessados pelos clientes da Rede Interna. A quantidade de clientes e servidores varia de acordo com o porte do lote, conforme especificado a seguir:

i) Lote 1, pelo menos 50 clientes e 5 servidores.

ii) Lote 2, pelo menos 125 clientes e 13 servidores.

iii) Lote 3, pelo menos 500 clientes e 50 servidores.

iv) Lote 4, pelo menos 1.500 clientes e 200 servidores.

v) Lote 5, pelo menos 2.500 clientes e 400 servidores.

5.1.11. 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 varia de acordo com o porte do lote. No mínimo 60% dos hits devem ocorrer nas últimas regras, baseando-se na análise *top-down*, conforme especificado a seguir:

i) Lote 1, pelo menos 10 regras.

ii) Lote 2, pelo menos 25 regras.

iii) Lote 3, pelo menos 100 regras.

iv) Lote 4, pelo menos 500 regras.

v) Lote 5, pelo menos 1.000 regras.

5.1.12. A amostra deve ser submetida à padrão de tráfego de dados, baseado na metodologia do NSS Labs, 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 média, permitindo-se variações em até 10%:

5.1.12.1. HTTP = 55% (conteúdo variável com imagens e textos, tamanho variável de 100 bytes a 500 Kbytes, sendo uma reserva de 5% para arquivos com malwares e 1% para ataques).

5.1.12.2. HTTPS a ser descriptografado e inspecionado = 25% (conteúdo variável com imagens e textos, tamanho variável de 100 bytes a 500 Kbytes, sendo

uma reserva de 5% para arquivos com *malware* e 1% para ataques, utilizando-se criptografia AES e SHA – 256 ou superior).

5.1.12.3. Aplicações, outros ataques, outras ameaças e outros protocolos = 20%, a ser acordado com o grupo técnico de apoio ao pregoeiro e homologado no Caderno de Testes.

5.1.12.3.1. 5% VPN (PiSec, conteúdo variável com imagens e textos, tamanho variável de 100 bytes a 500 Kbytes)

5.1.12.3.2. E-mail (POP, SMTP e IMAP com conteúdo variável, incluindo arquivos anexos).

5.1.12.3.3. 5% UDP (distribuição de tamanho: 56% 72 bytes, 17% 512 bytes e 27% 1518 bytes).

5.1.12.3.4. 4% de aplicações (qualquer protocolo e com tamanho variável).

5.1.12.3.5. Outros (distribuição de tamanho variável)

5.2. Teste de Assertividade

5.2.1. Deverá ser utilizada a configuração de testes descritos nos itens 5.1.1 a 5.1.5.

5.2.2. Após as configurações do item acima, deverá ser realizado o *backup* das configurações da Amostra, sendo calculado seu *hash*.

5.2.3. Da distribuição do item 5.1.2, o grupo técnico modificará durante os testes, em até 25%, os ataques, ameaças, sites e aplicações apresentados no caderno de teste.

5.2.4. No teste de assertividade, a solução deverá:

i) Categorizar e bloquear os ataques em, no mínimo, 2.000 (duas mil) assinaturas distintas de IPS/IDS;

ii) Categorizar e bloquear as ameaças em, no mínimo 2.000 (duas mil) assinaturas de *malwares* distintas;

iii) Categorizar e bloquear, pelo menos, 100 (cem) aplicações distintas;

iv) Classificar os acessos em, no mínimo, 5.000 (cinco mil) sites distintos de internet, distribuídos em, no mínimo, 40 (quarenta) categorias ou subcategorias distintas sendo bloqueados 25% deste total escolhidos por categorias específicas definidas pelo grupo técnico de apoio ao pregoeiro no momento do teste.

5.2.5. Serão coletados parâmetros que indiquem o índice de assertividade das funcionalidades dos lotes descritas nos itens 2.1, 2.3, 2.4, 2.5 e 2.6 do anexo B.

5.2.5.1. Serão contabilizados apenas os bloqueios e categorizações de(as) ameaças/ataques/aplicações/URLs corretos(as), devendo, portanto, ser excluídos(as) da contabilização aqueles(as) que correspondem aos falsos positivos (inexistentes, mas bloqueados(as) pela solução) e categorizados como mal formados, não identificados, desconhecidos ou similares.

5.2.5.2. A categorização contabilizada será analisada pelo grupo técnico de apoio ao pregoeiro com base nos dados gerados e obtidos pelo gerador de tráfego, sendo complementado, quando necessário, pelos dados obtidos pela amostra.

5.2.5.3. A auditoria da contabilidade será feita por amostragem

5.2.6. A amostra será considerada aprovada no teste de assertividade se apresentar o valor de acerto de pelo menos 80% para cada funcionalidade testada dos itens 2.1, 2.3, 2.4, 2.5 e 2.6 do anexo B.

5.2.6.1. A referida taxa de 80% (oitenta por cento) significa que de cada 100 ameaças/ataques/aplicações/URLs distintas(os) trafegadas através da solução, esta deverá categorizar e bloquear, de forma assertiva, pelo menos 80 deles(as).

5.2.7. Após a realização do teste de assertividade, o *firewall* da Amostra deverá ter todos os seus contadores zerados e configurações apagadas.

5.3. Teste de Desempenho

5.3.1. Para os testes deverão ser utilizadas todas as configurações de testes e topologia descritas no item 5.1.

5.3.2. Será considerado como taxa de transferência (*throughtput*) o somatório das interfaces de entrada do gerador de tráfego, após passagem do tráfego no equipamento testado.

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

5.3.4. Durante os testes de desempenho minimamente deverão ser gerados(as) as ameaças, ataques, aplicações e URLs, bem como ativadas as assinatura e perfis de antivírus, *anti-malware*, IDS/IPS, aplicações e URLs, em modo de detecção, que foram homologadas no teste de assertividade.

5.3.5. Após os ajustes para os testes, deverá ser realizado o backup das configurações da Amostra, sendo calculado seu *hash*.

5.3.6. As configurações da Amostra devem ser as mesmas, tanto para o item 5.3.7 quanto para o item 5.3.8.

5.3.7. Parametrização: A amostra deverá ser inicialmente submetida a uma taxa de transferência do tamanho de 25% do *throughput* do lote, no padrão de tráfego descrito no item 5.1, sendo testado por 30 (trinta) minutos contínuos e ininterruptos com o objetivo de coleta de parâmetros que serão utilizados para verificação da performance do equipamento. A contagem poderá ser iniciada após o período de estabilização do tráfego.

5.3.7.1. Após a realização da parametrização descrita no *caput*, o *firewall* da Amostra deverá ter todos os seus contadores zerados.

5.3.7.2. Serão coletados os parâmetros que indiquem a taxa de transferência, latência média e variação média de latência (*jitter*) do equipamento, erros absolutos irrecuperáveis de transações TCP/layer-7 e a detecção de ameaças, aplicações, ataques e URLs;

5.3.8. Teste: A amostra deverá ser então submetida a uma taxa de transferência de 85% do *throughput* do lote, no padrão de tráfego do item 5.1, sendo testado, por 30 minutos contínuos e ininterruptos e não poderá apresentar prejuízo em sua performance. A contagem poderá ser iniciada após o período de estabilização do tráfego.

5.3.8.1. O Lote 5, diferentemente dos outros lotes, deverá ter uma amostra submetida a uma taxa de transferência de 80% do respectivo *throughput*, no padrão de tráfego do item 5.1, sendo testado por 30 minutos contínuos e ininterruptos e não poderá apresentar prejuízo em sua performance. A contagem poderá ser iniciada após o período de estabilização do tráfego.

5.3.8.2. Serão coletados os parâmetros que indiquem a taxa de transferência, latência média e variação média de latência (*jitter*) do equipamento, erros absolutos irrecuperáveis de transações TCP/layer-7 e a detecção de ameaças, aplicações, ataques e URLs;

5.3.8.3. Serão comparados os parâmetros coletados nos itens 5.3.7.1 e 5.3.8.2, sendo considerado prejuízo na performance do equipamento a ocorrência de quaisquer dos eventos a seguir:

i) Perda absoluta de pacotes superior a 1%.

ii) Erros absolutos irrecuperáveis de transações TCP/layer-7 superior a 0,5%.

iii) Valores de latência média ou de variação média de latência (*jitter*) acima de 10 x (vezes) dos valores coletados no item 5.3.2 deste anexo.

iv) A não observância de detecções por amostragem de ameaças, ataques, aplicações e URLs presentes no item 5.2.

5.3.8.4. A amostra será considerada aprovada no teste de desempenho se não apresentar os prejuízos na performance, conforme item 5.3.8.3.

5.3.8.5. Após a realização do teste do item 5.3.2, o firewall da Amostra deverá ter todos os seus contadores zerados e configurações apagadas.

5.4. Teste de Sessões

5.4.1. Para a mensuração de novas sessões por segundo e sessões simultâneas, a amostra deverá ser submetida obrigatoriamente a dois testes. Esses testes deverão ser realizados na ordem descrita abaixo, devendo ser a amostra aprovada em no mínimo em um deles.

5.4.2. Primeiro teste

5.4.2.1. Para o teste deverá ser utilizada a configuração de testes descritos nos itens 5.1, 5.3.2 a 5.3.5, sendo a amostra submetida a taxa de *throughput* do item 5.3.8.

5.4.2.2. Mensuração de novas sessões por segundo: para tal aferição, deverá obrigatoriamente ser utilizada a distribuição de tráfego descrita no item 5.1.12 deste anexo, incluindo tráfego *stateless* UDP e VPN.

5.4.2.2.1. A amostra será considerada aprovada se comprovar no mínimo 50% do número de novas sessões por segundo TCP, que é estabelecido no Anexo B por no mínimo 5 minutos contínuos e ininterruptos.

5.4.2.3. Mensuração de sessões simultâneas: para tal aferição, deverá obrigatoriamente ser utilizada a distribuição de tráfego descrita no item 5.1.12 deste anexo.

5.4.2.3.1. A amostra será considerada aprovada na mensuração de novas sessões simultâneas se comprovar o número de sessões simultâneas TCP, que é estabelecido no Anexo B, por no mínimo 5 minutos contínuos e ininterruptos.

5.4.2.4. A mensuração de novas sessões por segundo e a de sessões simultâneas serão realizadas em momentos distintos.

5.4.2.5. A amostra será considerada aprovada no primeiro teste de sessões se for considerada aprovada nas mensurações dos itens 5.4.2.2 e 5.4.2.3.

5.4.2.6. Após a realização do teste do item 5.4.2 deste anexo, o firewall da amostra deverá ter todos os seus contadores zerados e configurações apagadas.

5.4.3. Segundo teste

5.4.3.1. Mensuração de novas sessões por segundo: para tal aferição, deve ser utilizado tráfego HTTP puro e, no mínimo, objeto de 64 bytes, ativando apenas a funcionalidade de firewall *statefull*, não sendo necessário seguir as especificações do item 5.1 e seus subitens.

5.4.3.1.1. A amostra será considerada aprovada se comprovar o número de novas sessões por segundo, que são estabelecidos no Anexo B, por pelo menos, 5 (cinco) minutos contínuos e ininterruptos.

5.4.3.2. Mensuração de sessões simultâneas: para tal aferição, deve ser utilizado tráfego HTTP puro e, no mínimo, objeto de 64 bytes, ativando apenas a funcionalidade de firewall *statefull*, não sendo necessário seguir as especificações do item 5.1 e seus subitens.

5.4.3.2.1. A amostra será considerada aprovada se comprovar o número de sessões simultâneas, que são estabelecidos no Anexo B, por pelo menos, 5 (cinco) minutos contínuos e ininterruptos.

5.4.3.3. As mensurações de novas sessões por segundo e sessões simultâneas serão realizadas em momentos distintos.

5.4.3.4. Ressalta-se que para mensurar novas sessões, cada uma deverá ser estabelecida, minimamente, por meio de *handshake* de três vias (*three-way handshake*).

5.4.3.5. A amostra será considerada aprovada no segundo teste de sessões se for considerada aprovada nas mensurações dos itens 5.4.3.1 e 5.4.3.2.

Documento assinado eletronicamente por **Gilnara Pinto Pereira**, **Analista**, em 04/09/2017, às 14:39.

A autenticidade do documento pode ser conferida no site [https://seimp.planejamento.gov.br/conferir], informando o código verificador **4493342** e o código CRC **E9A0EE27**.