

## **TERMO DE AVALIAÇÃO DA AMOSTRA - LOTE 2 - TESTES COMPLEMENTARES**

**PREGÃO ELETRÔNICO:** Nº 5/2017

**OBJETO:** REGISTRO DE PREÇOS, para eventual aquisição, 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, incluindo 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.

**Lote 2 – LICITANTE:** Teltec Solutions.

### **1. FINALIDADE**

O teste de conformidade da amostra visa à aferição da real capacidade técnica dos equipamentos ofertados pela Licitante Convocada em cumprimento ao disposto nos requisitos constantes da especificação técnica do Anexo B do Termo de Referência do Pregão nº 5/2017, referentes ao Lote 2. Adicionalmente, os testes complementares visam à aferição e esclarecimento dos requisitos listados na conclusão do Termo de Avaliação da Amostra – TAM, após o primeiro período dos testes de conformidade.

Para a avaliação dos testes complementares de conformidade por meio do presente TAM complementar foram levados em consideração o Relatório de Testes Complementares da Amostra apresentado pela empresa LICITANTE, assim como as evidências observadas e coletadas pela equipe técnica durante o período destinado aos testes.

### **2. CONSIDERAÇÕES GERAIS, DA AMOSTRA E DA PREPARAÇÃO INICIAL**

O período destinado à realização dos testes complementares de conformidade do LOTE 2 consistiu no prazo de 24 horas úteis (3 dias úteis) entre os dias 26 e 28 de fevereiro de 2019, das 08:00h às 18:00h, nas dependências do Ministério da Economia (Ministério do Planejamento, Desenvolvimento e Gestão - MP), bloco D situado na quadra 516 Norte, em Brasília-DF.

O ambiente foi aberto e disponibilizado para a empresa antes das 8h da manhã do dia 26/02/2019. Somente às 9h da manhã foi realizada a abertura dos testes, em função do atraso da chegada dos integrantes da empresa Teltec. Iniciado os trabalhos, no dia 26 de fevereiro, foi informado que os testes seriam realizados de acordo com as regras e condições contidas no Anexo E do Termo de Referência. Lembrou-se aos participantes que os testes constituem sessão pública e que, durante a realização dos testes, não deveriam ser realizadas intervenções indevidas das empresas ouvintes ou interessados presentes à sessão pública, bem como questionamentos não deveriam ser realizados durante a sessão, com exceção de esclarecimentos pontuais, uma vez que tais questionamentos deverão ser formalizados e endereçados ao pregoeiro, em momento posterior, em sede de recurso administrativo com as devidas fundamentações.

Reiterou-se à ocasião que, conforme especificado nos itens 2.16 e 2.17 do anexo E do edital PE nº 05/2017, ao grupo técnico de apoio ao pregoeiro é conferida a prerrogativa de, a qualquer tempo durante a realização dos testes, solicitar as alterações, adequações ou informações que julgar necessárias ao esclarecimento de todas as eventuais dúvidas em relação aos testes e itens da especificação técnica. Salientou-se, da mesma forma, a necessidade de se manter o registro e documentação de logs, prints e evidências para a

comprovação do atendimento dos quesitos avaliados nos testes de conformidade, os quais deveriam ser salvos em mídia própria fornecida pelo grupo técnico.

Cabe ressaltar que, devido a limitações de licenciamento do equipamento gerador de tráfego, Spirent Avalanche, os relatórios exportados ficaram com datas anteriores ao dia em que foram gerados. Desta forma, a data de criação dos arquivos foi validada, pela equipe de apoio pregoeiro, através da verificação das propriedades dos arquivos, permitindo a continuidade dos testes, conforme relatado na página 2 do relatório da LICITANTE.

A amostra disponibilizada pela LICITANTE correspondia ao que estava descrito em proposta comercial, a saber: Equipamento firewall ASA 5516-X com Cisco FirePOWER Services, incluindo funcionalidades de Threat Protection, Malware Protection, URL Filtering e Control, além das interfaces de gerenciamento Cisco Firepower Management Center - FMC, Cisco Security Manager - CSM e Cisco Adaptive Security Device Manager - ASDM, conforme apresentado na mesma página 2 do relatório da LICITANTE.

A equipe técnica da LICITANTE restaurou arquivos de backup salvos nos testes anteriores, de forma que pudesse ser garantida a utilização do mesmo firmware durante os testes complementares, conforme apresentado a partir da página 4 do relatório de testes da amostra apresentado pela LICITANTE.

As evidências relacionadas às configurações iniciais, topologia e endereçamentos ficaram registradas entre as páginas 22 e 38 do Relatório de Testes da Amostra, sendo os respectivos prints, arquivos de texto e demais arquivos, como hashes e relatórios do equipamento gerador de tráfego, disponibilizados em mídia da CONTRATANTE.

Dando continuidade aos trabalhos, no primeiro dia de testes a equipe técnica da LICITANTE indicou que iniciaria os testes executando o teste de assertividade da alínea “i) Categorizar e bloquear os ataques em, no mínimo, 2.000 (duas mil) assinaturas distintas de IPS/IDS” do item 5.2.4 do Anexo E.

Da mesma forma que ocorrera no primeiro período de testes, e com o objetivo de otimizar o tempo disponível, a equipe técnica da CONTRATANTE sinalizou que poderiam ser executados paralelamente os testes complementares adicionais que não tivessem relação com os testes de desempenho, pois estes careciam de execução anterior dos testes de assertividade pendentes e respectivas configurações.

Os detalhes a respeito da execução dos testes complementares adicionais são apresentados no item 3.5 a seguir.

### **3. DOS TESTES DE CONFORMIDADE**

#### **3.1) Das Configurações Dos Testes**

Os parâmetros e configurações gerais exigidos entre os itens 5.1.1 e 5.1.5 foram executadas pela equipe técnica da LICITANTE, observadas as características e limitações evidenciadas durante os testes e relatadas neste Termo de Avaliação.

#### **3.2) Dos Testes De Assertividade**

A empresa LICITANTE registrou os resultados dos testes de assertividade a partir da página 38 do Relatório de Testes da Amostra. Após realizar a configuração para execução do primeiro teste de assertividade, foi executado o backup das configurações e o arquivo “asa1.conf.txt”, juntamente com os arquivos “.tar”, foi salvo em mídia disponibilizada pela CONTRATANTE.

A assertividade quanto à alínea “i) Categorizar e bloquear os ataques em, no mínimo, 2.000 (duas mil) assinaturas distintas de IPS/IDS” do item 5.2.4 do Anexo E está evidenciada

entre as páginas 38 e 63 do Relatório dos Testes da Amostra, sendo que, segundo os resultados apresentados pelo equipamento gerador de tráfego, das 3121 tentativas de ataques gerados, 2870 foram identificadas e bloqueadas pelo firewall multifuncional. O Relatório do equipamento gerador de tráfego Spirent, arquivo “IPS\_report.pdf” salvo no diretório “F:\TELTEC-PE52017-LOTE2\Dia 2 - 2019-02-27\Spirent\Assertividade IPS”, apresenta o resultado na página 2, indicando que 91,95% dos ataques injetados na amostra em avaliação foram identificados e bloqueados. O mesmo relatório também foi apresentado pela empresa LICITANTE com o nome de “RTA - Teste de Assertividade IPS-IDS – reteste - Spirent Avalanche.pdf”.

No entanto, **persistiu** a inconsistência identificada em relação aos *logs* apresentados pelo firewall em avaliação. O número de transações registradas, conforme indicado no arquivo “Reteste\_-\_Assertividade\_-\_Ataques\_-\_v2-20190227161706-26206\_1\_Table\_View\_of\_Connection\_Events.csv”, gerado pelo firewall e coletado durante os testes de bancada, foi de **3821**. Contudo, desse total, apenas **1088** apresentam a ação “Block” com a razão “**Intrusion Block**”, o que representa **28,46%** do total. Quando comparado ao número total de tentativas registradas pelo equipamento gerador de tráfego, ou seja, **3121** ataques, as 1088 ações de bloqueio de tentativas de intrusão perfazem **34,86%** de assertividade.

Além disso, dentre os arquivos de logs coletados da amostra, a coluna que descreve a nome das assinaturas/ataques possui apenas **929** valores exclusivos, ou seja, valor **aquém** das 2.000 assinaturas distintas exigidas no teste de conformidade. A contagem desta mesma informação na planilha “RTA - Teste de Assertividade IPS-IDS - reteste.csv”, entregue pela LICITANTE anexa ao Relatório de Testes da Amostra, é de **946** valores distintos. A lista de assinaturas também foi apresentada no relatório da LICITANTE, entre as páginas 38 e 59.

O grupo técnico de apoio ao pregoeiro levantou questionamento à equipe técnica da LICITANTE a respeito do motivo de tal divergência. Foi então informado que a amostra trabalha com duas camadas para prevenção contra ataques de intrusão, mas que a primeira delas não gera evidências das ações de bloqueio tomadas. Diante de tal característica do equipamento, tornou-se clara e inequívoca a impossibilidade de configuração possível ou compatível com o atendimento ao item 5.1.4 do ANEXO E, *in verbis*:

*“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”.*

Adicionalmente, foi solicitado pelo grupo de apoio ao pregoeiro teste de identificação de um mesmo ataque encapsulado tanto em HTTP, quanto em HTTPS. A amostra foi capaz de identificar o ataque nos dois cenários e as evidências foram registradas entre as páginas 61 e 63 do relatório. Também foi exportado arquivo de logs da amostra em avaliação e anexada ao relatório com o nome de “RTA - Teste de Assertividade IPS-IDS - reteste SQL\_injection.csv”. O equipamento gerador de tráfego gerou o arquivo “sql\_report.pdf”, salvo no diretório “F:\TELTEC-PE52017-LOTE2\Dia 2 - 2019-02-27\Spirent\Sql Injection” da mídia disponibilizada pela CONTRATANTE.

O teste complementar quanto à assertividade para “*iii) Categorizar e bloquear, pelo menos, 100 (cem) aplicações distintas*”, com lista idêntica a que fora apresentada em todos os lotes, constituiu de identificação e bloqueio de 40 aplicações elencadas pelo grupo técnico de apoio ao pregoeiro. A empresa LICITANTE registrou os resultados dos testes a partir da

página 63 do seu relatório. Como executado nos demais testes, o grupo de apoio técnico ao pregoeiro indicou que a equipe técnica da LICITANTE poderia apontar, nos logs coletados após execução do primeiro período de testes, em arquivo salvo na mídia da CONTRATANTE, as aplicações que já haviam sido identificadas e bloqueadas através dos testes automatizados com o equipamento gerador de tráfego. As que não fossem encontradas nos logs, deveriam ser objeto de execução de testes pontuais.

Dentre as **40** aplicações, a amostra foi capaz de identificar e bloquear **33** aplicações, perfazendo um total de assertividade de **82,5 %**. Contudo, verificou-se que a amostra **não** possuía granularidade para identificar e bloquear tráfego de vídeo em HTTP, inclusive em sites como Facebook, Instagram e Twitter, o que inviabiliza o controle do consumo de banda por *streaming* de vídeo nestas aplicações, conforme reza o item 2.6.12 do ANEXO B - Especificações Técnicas do instrumento editalício, que reza:

*“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, updates de software, (...)”*

Prosseguindo com os testes pontuais de identificação das aplicações, a amostra também **não** foi capaz de identificar e bloquear as aplicações iCloud e Google Docs. Assim, além da dificuldade supracitada da amostra em identificar, bloquear e restringir aplicações de *streaming* em profundidade e granularidade, o grupo técnico constatou inequívoca desconformidade ao item 2.6.13 do referido anexo, que lista as aplicações mínimas a serem tratadas pela amostra:

*“2.6.13 Identificação, bloqueio e restrição em profundidade e granularidade de aplicações, contemplando, no mínimo: (...), Facebook, (...), **Google Docs**, Instagram, Twitter, LinkedIn, Dropbox, (...)”*

### **3.3) Dos Testes De Desempenho**

O relatório dos testes apresentado pela LICITANTE não apresenta evidências, nem registros a respeito dos testes de desempenho com a funcionalidade de administração de largura de banda (QoS) habilitada nas políticas de firewall. Contudo, foi verificado pelo grupo de apoio técnico ao pregoeiro que a equipe técnica da LICITANTE realizou configuração compatível com políticas de controle de largura de banda (QoS) e executou alteração de configuração de interfaces de forma que fosse disponibilizada, de forma simultânea, as interfaces de gerência local e de gerência centralizada da solução. As configurações das interfaces, NATs e de controle de banda (QoS) ficaram registradas entre as páginas 29 e 38 do relatório da LICITANTE e o backup das configurações foi salvo na pasta “F:\TELTEC-PE52017-LOTE2\Dia 3 - 2019-02-28\backups”, em mídia disponibilizada pela CONTRATANTE.

Entretanto, na mídia utilizada para salvar evidências e arquivos gerados durante os testes, verifica-se apenas os resultados da execução da parametrização, quando é exigida 25% da capacidade indicada para o lote, impossibilitando a comparação de resultados com o teste de desempenho em que é exigida 100% da capacidade para o lote. Em resumo, não foram coletados os parâmetros de 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, **impossibilitando** a execução da comparação exigida no item 5.3.8.3 do Anexo E - Teste de Conformidade dos testes de

desempenho com perfil de administração de largura de banda habilitado e, assim, ateste do desempenho da amostra com os perfis QoS ativados.

### 3.4) Dos Testes De Sessão

Não foram exigidos teste de sessão nos testes complementares.

### 3.5) Dos Testes dos itens adicionais

Conforme indicação do grupo técnico relatada anteriormente, os testes dos itens adicionais relacionados às dúvidas sobre as especificações técnicas solicitadas pelo Anexo B do Edital PE nº 05/2017, apontados no caderno de testes e que não dependiam de configuração da amostra para execução do seu ateste, poderiam ser realizados paralelamente a outros testes, de forma que fosse otimizada a execução dos trabalhos. Os outros itens seriam verificados apenas após a viabilização das configurações necessárias para os testes automatizados de assertividade e desempenho, já que as evidências seriam coletadas utilizando-se tais configurações.

Diante das evidências coletadas, foi constatado que:

i) A amostra atendeu ao disposto no item 2.1.14 quanto ao suporte à *“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”*. A evidência foi registrada nas páginas 75 e 76 do relatório.

ii) Em relação ao item *“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;”* (grifo nosso), a equipe técnica da LICITANTE demonstrou, durante os testes, a integração da solução com uma base de usuários do Microsoft Active Directory. Entretanto, embora a amostra tenha identificado a sessão, não foi capaz de validar o registro de cada usuário associado aos eventos e o campo com a descrição *“User”*, da tabela de eventos da amostra, permanecia com a informação *“Special Identities/unknown”*. O *print* *“Anotação 2019-02-28 170314”*, capturado durante os testes e salvo em mídia da CONTRATANTE, evidencia que a amostra **não** foi capaz de identificar o usuário, estando, portanto, em desconformidade ao item do edital;

Cabe ressaltar que durante o primeiro período de testes a equipe técnica da LICITANTE utilizou um agente instalado em um servidor com o sistema operacional Microsoft Windows para tentar realizar a integração entre a amostra (firewall) e o servidor de diretório de usuários. Na ocasião, a tentativa resultou em falha antes mesmo de a amostra conseguir fazer a leitura da base de usuários. Nos testes complementares, que geraram este novo relatório, a equipe técnica da LICITANTE utilizou um *appliance virtual* hospedado em ambiente VmWare. A equipe técnica de apoio ao pregoeiro chegou à conclusão de que, devido às falhas apresentadas na tentativa de integração da amostra, utilizando-se de recursos diferentes (ora utilizando agente instalado em servidor windows, ora *appliance virtual*), se trata de funcionalidade ainda não estável para uso.

iii) A equipe técnica da LICITANTE, após as primeiras tentativas de configuração que demonstrasse, de forma inequívoca, o atendimento requerido em edital, não demonstrou, até o término do prazo estipulado para os testes complementares, o pleno atendimento do item 2.1.23.3 do Anexo B, a saber: *“Deve prover identificação de forma transparente aos usuários autenticados por single sign on, no mínimo, por meio dos serviços Microsoft Active Directory e RADIUS” (grifo nosso)*. Conforme já citado em item anterior, a amostra autorize a abertura da sessão em regra criada, **não** exibe a identidade do usuário autenticado via estrutura do Active Directory.

iv) A equipe técnica da LICITANTE **não** demonstrou o atendimento do item “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*”, portanto, ficou prejudicada a sua averiguação.

v) A equipe técnica da LICITANTE apresentou telas de configuração nas quais são listadas configurações que buscam o suporte ao item “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*. Porém, dada a limitação a respeito da identificação do usuário e não funcionamento da solução utilizada para integrar a amostra ao AD, conforme já relatado, restou impossibilitada a comprovação inequívoca do item. As evidências foram registradas nas páginas 76, 77 e 78 do relatório da LICITANTE.

vi) Vide texto do termo anterior.

vii) A equipe técnica da LICITANTE **não** demonstrou o atendimento do item “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*”, portanto, ficou prejudicada a sua averiguação.

viii) Vide texto do termo anterior.

ix) Em relação ao item “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)*”, a amostra possui suporte à criação de políticas de controle de uso de largura de banda baseadas em grupos de usuários do AD, observada a limitação para identificar o usuário, já relatada Porém, ficou evidente que a amostra **não** possui capacidade de aplicar o recurso com filtro em aplicações, conforme detalhado na alínea “xvi” a seguir.

Em relação à configuração do recurso de controle de banda (QoS), a equipe técnica da LICITANTE evidenciou, das páginas 36 a 38 do relatório, que a amostra possui campos e telas de configuração nas interfaces Cisco Security Manager - CSM e Cisco Adaptive Security Device Manager - ASDM.

x) A equipe técnica da LICITANTE demonstrou parcialmente o atendimento do item “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*”, uma vez que foi executado teste de autenticação via Microsoft Active Directory, mas a amostra não apresentou a identidade do

usuário. Além disso, havia necessidade, porém não atendida, de se explorar e atestar o funcionamento dos recursos de autenticação com dois fatores, devido às falhas verificadas durante a integração da amostra com o Microsoft Active Directory.

xi) A equipe técnica da LICITANTE **não** demonstrou o atendimento do item “2.3.11. *Permitir filtros de anomalias de tráfego estatístico de flooding, scan e source session limits*”, portanto, ficou prejudicada a sua averiguação.

xii) Vide texto do termo de avaliação anterior.

xiii) Vide texto do termo de avaliação anterior.

xiv) Vide texto do termo de avaliação anterior.

xv) Em relação ao item “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*”, a equipe técnica da LICITANTE demonstrou a capacidade de identificação e bloqueio de aplicações “*independentemente das portas e protocolos utilizados*”. A evidência foi registrada nas páginas 75 e 76 do relatório de testes da amostra apresentado pela LICITANTE.

xvi) Em relação ao item “3.8.1.2. *Possuir, no mínimo, o throughput de inspeção 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*”, sua comprovação plena não foi evidenciada, uma vez que não foi executado completamente o Teste de Desempenho complementar com a funcionalidade de controle de banda (QoS) ativada.

Salienta-se que, em tempo de execução dos testes complementares, com o objetivo de validar o pleno atendimento da funcionalidade de controle de banda (QoS) e respectivos meios de configuração, a equipe técnica de apoio ao pregoeiro constatou que a amostra em análise **não** possui capacidade de executar o controle de banda por aplicação. O método apresentado pela equipe técnica da LICITANTE, executando configuração através da interface de gerenciamento da solução, utiliza-se da criação de assinaturas de forma manual e utilizando expressões regulares, conforme demonstrado nos prints “Anotação 2019-02-28 172243”, “Anotação 2019-02-28 172301” e “Anotação 2019-02-28 172316”, salvos no diretório “F:\TELTEC-PE52017-LOTE2\Dia 3 - 2019-02-28\capturas” da mídia da CONTRATANTE. Tal forma manual de controle inviabiliza sobretudo o tratamento granular e em profundidade de aplicações de streaming (conforme itens 2.6.12 e 2.6.13 do edital), dada a natureza intrinsecamente dinâmica dos tráfegos associados. Tal limitação, portanto evidencia de forma inequívoca que a amostra **não** atende o requisito técnico indicado no item 2.1.48, a saber: “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)*”.

xvii) Vide texto do relatório anterior. De forma complementar, salienta-se que esse parâmetro também carecia de ser novamente observado no teste de desempenho complementar, que não foi executado por completo, conforme já citado.

xviii) Vide texto do termo de avaliação anterior.

xix) Vide texto do termo de avaliação anterior.

xx) Em relação ao item “3.14.1.2. Possuir capacidade mínima de 250 GB para armazenamento de logs e eventos.”, a equipe técnica da LICITANTE demonstrou o atendimento pela solução de gerência centralizada Cisco Firepower Management Center - FMC, em conjunto com a plataforma Cisco Security Manager - CSM, conforme evidência apresentada na página 80 do relatório.

#### **4. CONCLUSÃO**

O grupo técnico de apoio ao pregoeiro, levando em consideração o Relatório de Testes Complementares da Amostra da LICITANTE, bem como os fatos observados, esclarecimentos e evidências coletadas durante a execução dos testes de conformidade, concluiu que a LICITANTE **não** foi capaz de demonstrar o atendimento integral, e de forma inequívoca, dos requisitos do edital de Pregão Eletrônico Nº 5/2017 listados a seguir:

1. Executar e evidenciar o bloqueio de um quantitativo mínimo de 2.000 assinaturas distintas de IPS, com assertividade mínima de 80%, conforme previsto no item 5.2.4 do Anexo E: “i) Categorizar e bloquear os ataques em, no mínimo, 2.000 (duas mil) assinaturas distintas de IPS/IDS”;

2. Identificação e filtragem de *streaming* de vídeo, assim como identificação, bloqueio e restrição em profundidade de aplicações, ambos citados no item 3.2 deste termo de avaliação;

3. Executar teste de desempenho com perfil de administração de largura de banda (QoS) nas 25 políticas criadas no firewall, conforme disposto no item 5.1.1 do Anexo E;

4. Executar e evidenciar os testes complementares conforme observações citadas no item 3.5 acima e alíneas a saber: ii, iii, vii, ix, xi, xv, e observação citada na alínea xvi.

Diante de todo o exposto, o grupo técnico concluiu que a amostra ofertada pela LICITANTE **não** atende aos requisitos técnicos exigidos pelo Edital do PE n.º 5/2017.