Governo do Estado do Rio de Janeiro
Centro de Tecnologia de Informação e Comunicação do Estado do Rio de Janeiro
Vice Presidência de Tecnologia

ESTUDO TÉCNICO PRELIMINAR

SOLUÇÃO NEXT GENERATION FIREWALL (NGFW)

1. DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

1.1. O presente Estudo Técnico Preliminar - ETP reúne o conjunto de informações indicativas e as condições preliminares exigíveis para a aquisição perpétua de solução de firewall, com garantia de 60 meses, contemplando hardware e software, com instalação, configuração e treinamento oficial da solução, com vistas à mitigação e combate de ameaças de segurança cibernética que afetam a rede governo, sob a coordenação da Diretoria de Segurança da Informação - DIRSI.

1.2. O ETP ora apresentado constitui a primeira etapa do Planejamento da Contratação, regido e tendo por base a Lei Federal 14.133/2021 e demais legislação pertinente buscando estabelecer as melhores e mais vantajosas condições de aquisições para atendimento das demandas necessárias ao adequado funcionamento do Centro de Tecnologia de Informação e Comunicação do Estado do Rio de Janeiro - PRODERJ.

1.3. As soluções de Firewall desempenham papel fundamental na manutenção e disponibilidade adequada aos serviços e à continuidade das operações institucionais e corporativas, apoiando as divisões de infraestrutura e de segurança da informação desta Autarquia de forma a manter seus dados integros, seguros e disponíveis.

1.4. **Justificativa**

1.4.1. O PRODERJ, através da Diretoria de Segurança da Informação na forma do Documento de Oficialização de Demanda (66523536), pretende estabelecer em sua infraestrutura de segurança mecanismos de inspeção, detecção e bloqueio de ameaças de forma automatizada e segura, como forma de prevenção contra possíveis incidentes e promoção de aprimoramento dos níveis de segurança dos serviços prestados pelo PRODERJ aos Órgãos da Administração Pública Estadual, protegendo informações sigilosas que transitam na Rede Governo. É fundamental a implementação de uma solução de firewall que atue como uma camada protetiva para o tráfego desses dados.

1.4.2. Saliente-se que esta Autarquia, vinculada à Secretaria de Estado de Transformação Digital, atua como Órgão Gestor da Tecnologia da Informação e Comunicação, no âmbito do Governo do Estado do Rio de Janeiro, na forma do art. 3º, do Decreto Estadual nº 48.997/2024, que altera a estrutura organizacional do Poder Executivo e reestrutura o Sistema Estadual de Tecnologia da Informação e Comunicação - SETIC.

1.4.3. É responsável por sediar, manter e operar a TIC do Estado, ou seja, os sistemas de informações, o desenvolvimento de sistemas, as bases de dados de vários Órgãos estaduais e os diversos equipamentos hospedados no Data Center do Estado. É responsável também por prover serviços de Internet aos Órgãos da administração estadual, tais como correio eletrônico, consultoria, desenvolvimento e hospedagem de páginas, portais, intranets e extranets.

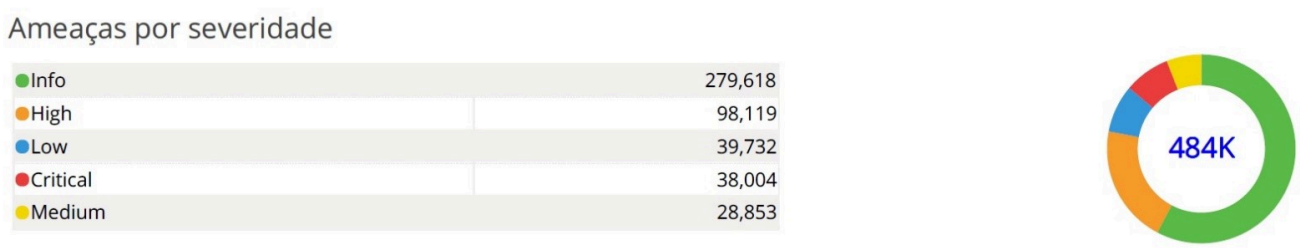
1.4.4. Também tem por competência o Registro de Preços em contratações de bens e serviços relativos à Tecnologia da Informação e Comunicação, para o atendimento das demandas dos demais órgãos da administração direta e indireta da Administração Pública Estadual, conforme o art. 3º, XIII, do Decreto Estadual nº 48.997/2024.

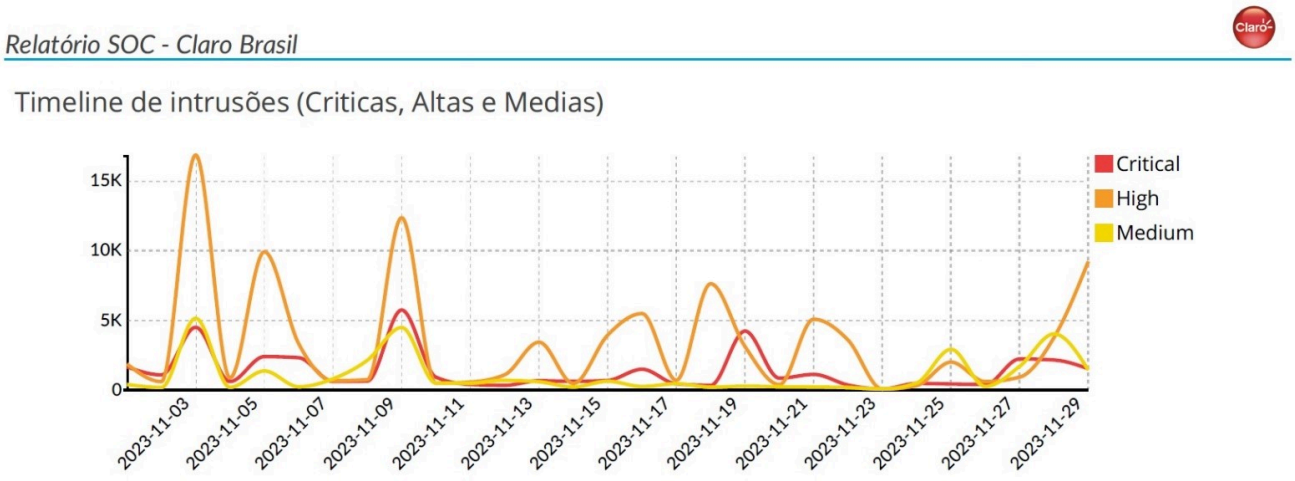
1.4.5. Atualmente o PRODERJ e outros órgãos da Administração Pública Estadual utilizam soluções de firewall corporativo oriundas do contrato de fornecimento de links de internet com a operadora Claro S.A., mediante Ata de Registro de Preços, onde é previsto o fornecimento dos links com segurança de perímetro e SNOC (Security and Network Operation Center). Contudo, a Ata de Registro de Preços do CONECTA-RJ ofertou aos órgãos dois lotes, correspondentes as duas opções para o fornecimento dos links: o "Lote 1" oferecendo links dedicados, incluindo firewall de perímetro. Contudo, a ferramenta opera tão somente sobre os ativos relacionados com o link proveniente daquela contratação. Ademais, esta solução de segurança não é oferecida no "Lote 2".

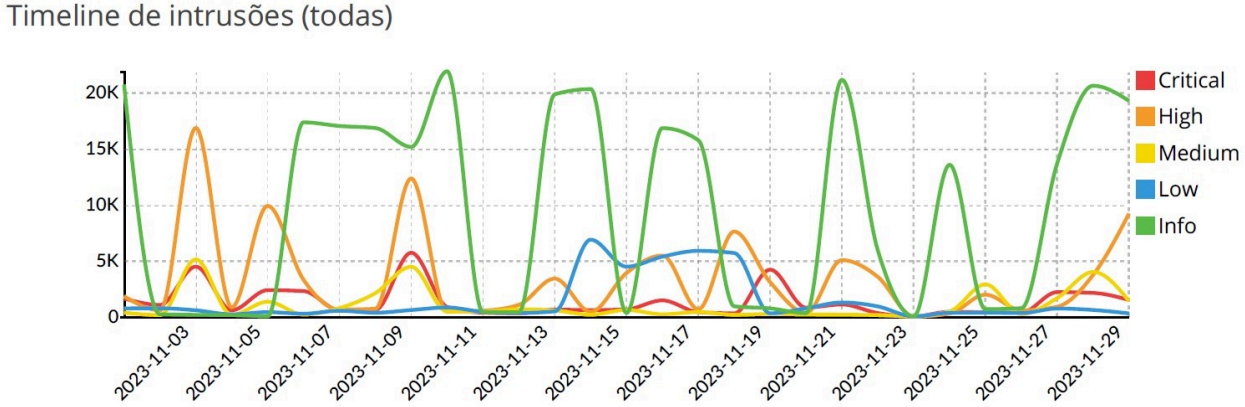
1.4.6. Assim, a presente demanda visa o atendimento aos órgãos que contrataram os links dos "Lotes 1 e 2", e atender ainda os órgãos que não contrataram nenhum dos links ofertados naquele certame, além de ofertar outra possibilidade de aquisição desta ferramenta sem a necessidade de aquisição através somente com a operadora. Fato é que, o fornecimento da solução atrelada à operadora, além de agregar valor nos links, não permitem que um órgão possa adquirir apenas a solução pretendida sem a contratação dos links, além disso cientes de que esses contratos possuem validade, muitas vezes o fim de um contrato de links desse tamanho acaba por impactar sobremaneira já que a troca dos equipamentos geralmente de outras marcas e modelos obriga a uma reconfiguração e consequente perda das configurações que são feitas diariamente e por anos, criando assim retrabalho, descontinuidade, gastos com mão de obra especializada para reconfiguração e prejuízo técnico.

1.4.7. A tarefa de manter a área de TIC sempre alinhada às estratégias do PRODERJ constitui-se desafio permanente. Busca-se garantir em todas as questões relacionadas à infraestrutura de TI, que o foco se mantenha na estratégia e nas necessidades finalísticas da Autarquia. Além desta, existe também a tarefa e obrigação de manter o ambiente tecnológico em alta disponibilidade e de preservar a qualidade dos serviços por ele providos sempre alinhados às estratégias do PRODERJ.

1.4.8. Ante o crescente número de eventos de ataques de agentes malignos vive-se num cenário crítico de segurança cibernética onde os dados institucionais/corporativos estão cada vez mais vulneráveis. Abaixo, relatórios do Centro Integrado de Comando e Controle - CICC, da Polícia Militar do Estado do Rio de Janeiro / PMERJ, referentes ao mês novembro/2023 com estatísticas de ataques de rede ocorridos no período:







1.4.9. Para contribuir na manutenção dos níveis de serviços oferecidos pelo PRODERJ aos demais órgãos e entidades da Administração, bem como se preparar para oferecer novos serviços na vanguarda da tecnologia da informação, é necessário realizar uma reestruturação no fornecimento de ativos de segurança (neste caso, dos firewalls de perímetro).

1.4.10. Ademais, a presente demanda contribuirá para o atendimento da Lei 13.709/2018, Lei Geral de Proteção a Dados (LGPD) que intensifica a obrigatoriedade de proteção e privacidade dos dados dos titulares, no nosso caso, os cidadãos, reforçando a necessidade do PRODERJ, Órgão de Tecnologia do Estado, contratar e fornecer aos demais Órgãos da Administração Pública Estadual, uma solução que possa proteger os ativos de TIC contra os diversos tipos de ameaças existentes no mundo cibernético, conforme se observa no Art. 46 da LGPD, onde consta:

> "Art. 46.Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito."

2. RESULTADOS PRETENDIDOS

A presente demanda visa a mitigação de diversas ameaças de segurança cibernética que afetam a rede governo, bem como obter os seguintes benefícios:

a) Aumentar o nível de proteção das informações trafegadas na rede governo;

b) Proteger contra acesso remoto não autorizado;

c) Permitir uso da internet com maior proteção;

d) Controlar o uso da internet pelos funcionários;

e) Bloquear conteúdo ilegal, imoral e improdutivo;

f) Proteger a rede corporativa contra malwares e outros tipos de ameaças cibernéticas

g) Inibir e impedir a invasão de hackers;

h) Permitir que funcionários remotos acessem a rede VPN de forma segura;

i) Elevar o nível de confiabilidade dos sistemas;

j) Promover compartilhamento seguro dos dados.

3. CONTRATAÇÕES CORRELATAS

Não existe registro de objeto contratado que tenha pertinência por correlação ou por interdependência com o objeto (bens e serviços) deste estudo técnico.

4. INSTRUMENTOS DE PLANEJAMENTO

4.1. Demonstração da previsão da contratação no Plano de Contratações Anual - PCA do órgão ou entidade:

a) ID PCA no PNCP: 42498600000171-0-000053/2024;

b) Data de publicação no PNCP: 02/01/2024;

c) ID do item no PCA: 01 a 05; 07 a 11 e 86 a 90.

4.2. Previsão no PEDTIC (67546441, p 34 e 35) do órgão ou entidade:

a) **Objetivo Estratégico 1 - Prover, manter e atualizar a infraestrutura e as Soluções e Serviços de Tecnologia da Informação e Comunicação**: Prover continuamente a inovação tecnológica para compor e atualizar a infraestrutura, as Soluções e os Serviços de Tecnologia da Informação e Comunicação, atendendo às crescentes demandas da Autarquia e dos Órgãos do Poder Executivo Estadual, visando o desenvolvimento, manutenção, integração e a padronização da TIC do estado (Alinhamento ao PPA 2024-2027 - Programa: 0493 / Ações: 1293 e 1294);

b) **Objetivo Estratégico 2 - Ampliar a capacitação técnica e profissional dos servidores em TIC**: Promover a qualificação exponencial dos servidores por meio da capacitação e participação em eventos que desenvolvam e aprimorem suas competências e a gestão do conhecimento em TIC (Alinhamento ao PPA 2024-2027 - Programa 0493 / Ação 1293);

c) **Objetivo Estratégico 3 - Aprimorar os Processos de TIC**: Promover a melhoria contínua dos processos, métodos e técnicas gerando uma maior efetividade na gestão e no uso dos recursos que fornecem as soluções de TIC (Alinhamento ao PPA 2024-2027 - Programa 0493 / Ação 1294);

d) **Objetivo Estratégico 6 - Garantir os padrões de qualidade dos serviços e soluções de TIC**: Assegurar que os serviços de TIC prestados pelo PRODERJ atendam seus requisitos mínimos, suprindo as expectativas dos órgãos da Administração Pública Direta e Indireta, de modo que contribuam para a agregação de seus valores institucionais e o cumprimento de seus objetivos estratégicos, potencializando sua capacidade de entrega, reforçando a aptidão em produzir, entregar novas soluções e aprimorar as existentes, assim como, o fornecimento de uma infraestrutura inovadora que garantam que os recursos tecnológicos investidos sejam capazes de preservar e promover a segurança, a privacidade, a disponibilidade e a continuidade dos serviços públicos, reduzindo os riscos inerentes aos serviços de TIC (Alinhamento ao PPA 2024-2027 - Programa 0493 / Ações 1293 e 1294).

5. DESCRIÇÃO DOS REQUISITOS DA CONTRATAÇÃO

Visando manter os níveis desta contratação dentro dos padrões adequados, verifica-se a necessidade de estabelecer, no mínimo, as seguintes exigências:

5.1. Requisitos de Negócio

A solução a ser adotada deverá ser capaz de entregar:

5.1.1. Equipamentos do tipo firewall de próxima geração (NGFW), a serem disponibilizados em três diferentes capacidades, bem como os sistemas complementares da solução (gerenciamento, logs e relatórios);

5.1.2. Treinamentos operacionais nas soluções contratadas, voltados para os técnicos da Contratante.

5.1.3. Garantia de 60 meses para todos os componentes da solução, observados os seguintes aspectos:

a) A garantia para os itens de aquisição em modalidade perpétua, por período de 60 meses, costuma ser praxe em licitações para contratações de soluções de TIC, tanto pelo governo federal como pelos demais entes, em que pese significar um aspecto diferencial do produto que, por fugir da condição básica ofertada pelo fornecedor, decerto que interfere em sua precificação e poderá repercutir numa majoração do lance do licitante no momento do pregão.

b) O referido lapso temporal, contudo, se apresenta razoável uma vez que corresponde ao prazo médio de vida útil de uma solução tecnológica, em que os fabricantes amiúde, permanecem ofertando peças de reposição ou mesmo o suporte técnico, por exemplo.

c) Esta garantia visa resguardar o bom funcionamento do inventário de TIC, com soluções de software e hardware em boas condições de forma a preservar o desempenho e a produtividade dos órgãos que venham a contratar o objeto (bens e serviços) ora proposto.

d) Enfim, dentro da mesma lógica do legislador, ao autorizar o poder público para contratações iniciais por prazos de até 5 (cinco) anos, naturalmente com o fim de resguardar a continuidade dos serviços públicos, que aliás, é um princípio da Administração Pública, é que se propõe a garantia de 60 meses para as soluções de TIC a serem adquiridas neste certame.

5.2. Requisitos de Capacitação

5.2.1. A capacitação compreende os serviços de treinamento dos itens nº 05 de todos os lotes.

5.2.2. O treinamento deverá abranger a operação da solução ofertada. Assim, os treinamentos dos itens nº 05 dos lotes, correspondem respectivamente à operacionalização dos itens nº 1 até nº 4 de todos os lotes.

5.2.3. O treinamento será direcionado aos técnicos da CONTRATANTE, deverá ser focado na solução adotada, de forma que haja transferência do conhecimento dos recursos, configurações existentes e sua utilização.

5.2.4. Deverá ser entregue para a contratante a proposta com o conteúdo do treinamento.

5.2.5. A Contratante reserva-se o direito de não aceitar o módulo ministrado, podendo, a seu critério, solicitar a troca de instrutor ou até mesmo repetição do mesmo, caso não seja satisfatório.

5.2.6. Deverá ser ministrado por instrutor capacitado na ferramenta, devendo ser comprovado por meio de certificados ou declaração emitida pelo fabricante.

5.2.7. Deverá ser fornecido pela contratada certificado de capacitação para os participantes do treinamento.

5.2.8. **Objetivo da capacitação**

5.2.8.1. Capacitação do contratante para a operacionalização da ferramenta tecnológica.

5.2.8.2. Formação de facilitadores que possam vir a replicar futuramente o conhecimento no âmbito do órgão contratante.

5.2.9. **Métrica da capacitação**

O treinamento será contratado por aluno (vaga).

5.2.10. **Carga horária da capacitação**

5.2.10.1. Deverá ter carga horária mínima de 40 (quarenta) horas.

5.2.10.2. Deverá iniciar no prazo máximo de até 20 dias úteis contados da emissão da Ordem de Serviço, quando o contratante não especificar prazos no documento.

5.2.10.3. Os treinamentos deverão ser realizados em dias úteis e não poderão exceder o horário comercial.

5.2.11. **Forma de realização da capacitação**

O treinamento será em português, ministrado na modalidade remota, em plataforma virtual disponibilizada pela contratada.

5.2.12. **Materiais didáticos e acessórios da capacitação**

5.2.12.1. É de responsabilidade da contratada todo material audiovisual, didático e eletrônico para a realização dos treinamentos, e quaisquer outras despesas diretas ou indiretas.

5.2.12.2. O material didático será fornecido em português, pela contratada, abordando todos os tópicos do curso.

5.2.13. **Conteúdo programático da capacitação**

5.2.13.1. O treinamento deverá englobar a realização de laboratórios práticos, fornecidos pela CONTRATADA, para configuração e execução de exercícios práticos na mesma versão dos produtos ofertados.

5.2.13.2. O evento abordará no mínimo: o uso da ferramenta, instalação, configuração, operação da ferramenta, gerenciamento, resolução de problemas, e poderá ser gravado para fins de documentação, caso seja de interesse da CONTRATANTE.

5.2.13.3. Deverá contemplar todos os recursos e configurações existentes na solução ofertada.

5.3. Requisitos Legais

a) **Lei Federal nº 14.133/2021**, que trata das normas gerais sobre licitações e contratos administrativos;

b) **Lei Complementar nº 123/2006**, que estabelece normas gerais relativas ao tratamento diferenciado e favorecido a ser dispensado às microempresas e empresas de pequeno porte atualizada;

c) **Decreto Estadual 43.629/2012**, que dispõe s*obre os critérios de sustentabilidade ambiental na aquisição de bens, contratação de serviços e obras pela Administração Pública Estadual Direta e Indireta e dá outras providências;*

d) **Decreto Estadual nº 48.322/2023**, que dispõe sobre o enquadramento dos bens de consumo, adquiridos para suprir as demandas das estruturas da administração pública estadual, nas categorias de qualidade comum e de luxo;

e) **Decreto Estadual nº 48.760/2023**, que implementa o Plano de Contratações Anual - PCA e institui o Sistema PCA RJ, no âmbito da administração pública estadual direta, autárquica e fundacional;

f) **Decreto Estadual nº 48.778/2023**, que regulamenta as licitações pelos critérios de julgamento por menor preço ou por maior desconto, no âmbito da administração pública estadual direta, autárquica e fundacional;

g) **Decreto Estadual 48.816/2023**, que regulamenta a fase preparatória das contratações, de que trata a Lei nº 14.133, de 1º de abril de 2021, no âmbito da administração pública estadual direta, autárquica e fundacional;

h) **Decreto Estadual nº 48.817/2023**, que regulamenta a gestão e a fiscalização das contratações no âmbito da administração pública estadual direta, autárquica e fundacional e dá outras providências;

i) **Decreto Estadual nº 48.843/2023**, que regulamenta o sistema de registro de preços - SRP, no âmbito da administração pública estadual direta, autárquica e fundacional e dá outras providências;

j) **Decreto Estadual nº 48.865/2023**, que regulamenta as licitações pelo critério de julgamento por técnica e preço, no âmbito da administração pública estadual direta, autárquica e fundacional;

k) **Decreto Estadual 48.997/2024**, que dispõe sobre a reestruturação do Sistema Estadual de Tecnologia da Informação e Comunicação - SETIC e estabelece as competências do PRODERJ enquanto órgão de Direção Geral do SETIC/RJ;

l) **Instrução Normativa SLTI/MP nº 94/2022** (a título de boas práticas), que dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC;

m)**Nota técnica SGE TCE-RJ nº 06/2023**, que orienta os jurisdicionados do TCE-RJ acerca da realização do planejamento para aquisição de bens e serviços de Tecnologia da Informação (TI) visando a atender ao princípio da economicidade.

5.4. **Requisitos de Manutenção**

5.4.1. Todas as rotinas para fins de manutenção com vistas ao pleno e adequado funcionamento da solução ao longo da vigência da garantia do produto estarão a cargo da CONTRATADA na forma do Suporte Técnico previsto no subtópico 5.7.3.1. deste documento.

5.4.2. O fornecedor deve disponibilizar ambiente web, número de telefone ou e-mail para abertura de chamados e acompanhamento das soluções e esclarecimentos de dúvidas.

5.4.3. **Requisitos Temporais**

Resguardado o cronograma previsto no subtópico 13.5.1. deste documento, não há outros requisitos temporais a serem considerados.

5.5. **Requisitos de Segurança da Informação e Privacidade**

5.5.1. Caso se faça necessário, para um eventual suporte nas dependências da CONTRATANTE, a CONTRATADA deverá exigir dos seus empregados, o uso obrigatório de uniformes e crachás de identificação.

5.5.2. Caso se faça necessário, para um eventual suporte nas dependências da CONTRATANTE, a CONTRATADA não poderá se utilizar da presente situação para obter qualquer acesso não autorizado às informações de propriedade do CONTRATANTE.

5.5.3. A CONTRATADA não pode obter, capturar, copiar ou transferir qualquer tipo informação de propriedade do CONTRATANTE, sem autorização.

5.5.4. **Da Proteção de Dados Pessoais**

5.5.4.1. As partes (CONTRATANTE e CONTRATADA), no âmbito do quaisquer atividades oriundas da execução deste Estudo Técnico, observarão o regime legal concernente à proteção de dados pessoais, especialmente as diretrizes veiculadas pela Lei nº 13.709 de 14 de agosto de 2018 (LGPD) na realização de qualquer operação que se amolde ao preceito de tratamento de dados pessoais durante a execução do objeto (bens e serviços).

5.5.4.2. A CONTRATADA deverá assinar Termo de Confidencialidade e Sigilo na forma do modelo a ser apresentado como anexo do futuro Termo de Referência.

5.5.4.3. Para atender aos ditames da Lei n° 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), a justificativa da necessidade compatível com as finalidades institucionais, assim como a apresentação de um relatório de impacto à proteção de dados pessoais (art. 5º, XVII, da LGPD) que aborde como serão usadas as tecnologias, deverá ser apresentada:

a) no momento da manifestação de interesse de participação da Intenção de Registro de Preços (IRP) pelos órgãos participantes; e

b) no momento da contratação realizada pelos órgãos não participantes.

5.5.4.4. As partes (CONTRATANTE e CONTRATADA), no âmbito de quaisquer atividades oriundas da execução deste Estudo Técnico, observarão o regime legal concernente à proteção de dados pessoais na realização de qualquer operação que se amolde ao preceito de tratamento de dados pessoais durante a execução do objeto.

5.5.4.5. Considerando a natureza dos dados tratados, pertinentes ao objeto desta contratação, a CONTRATANTE e a CONTRATADA deverão adotar, em relação aos dados pessoais, medidas de segurança, técnicas e administrativas, aptas a proteger os dados e informações de acessos, não autorizados, e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

5.5.4.6. A CONTRATADA deve notificar imediatamente, à CONTRATANTE, a ocorrência de incidente de segurança, relacionado a dados pessoais, por ela tratados, fornecendo informações suficientes para que a CONTRATANTE cumpra quaisquer obrigações de comunicação da ocorrência, à autoridade nacional, e aos titulares dos dados.

5.5.4.7. A CONTRATANTE e a CONTRATADA devem adotar as medidas cabíveis para auxiliar na investigação, mitigação e reparação de cada um dos incidentes de segurança, quando identificada a responsabilização exclusiva, de uma parte e/ou outra.

5.5.4.8. A CONTRATADA, na execução dos serviços de plataforma de serviços digitais, deve auxiliar a CONTRATANTE, na elaboração de relatórios de impacto à proteção de dados pessoais, observado o disposto no artigo 38 da Lei Federal nº 13.709/2018, no âmbito da execução deste objeto.

5.5.4.9. As partes deverão, nomeadamente:

a) Tratar os dados pessoais nos moldes expressamente definidos e em estrita consonância com a finalidade específica delineada pelo CONTROLADOR;

b) Armazenar os dados pessoais apenas durante o período definido pelo CONTROLADOR;

c) Não desviar o tratamento dos dados pessoais da finalidade específica e da hipótese legal legitimadora;

d) Informar imediatamente a outra parte contratante acerca da ocorrência de qualquer incidente que envolva os dados pessoais tratados, assim como prestar toda colaboração necessária para instruir o respectivo Relatório;

e) Assegurar os direitos dos titulares, abrangendo a disponibilidade de canal acessível ao Encarregado pelo tratamento de dados pessoais;

f) Garantir que os respectivos colaboradores ou prestadores de serviços que tenham acesso aos dados pessoais no contexto deste Estudo Técnico cumpram as diretrizes protetivas dos dados pessoais, vinculando-os a um Termo de Confidencialidade.

5.5.4.10. Em se tratando de dados pessoais sensíveis, ambas as partes contratantes, deverão observar as hipóteses legais legitimadoras, nos moldes do Art. 11 da Lei 13.709/18, in verbis:

I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;

II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

a) cumprimento de obrigação legal ou regulatória pelo controlador;

b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;

d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);

e) proteção da vida ou da incolumidade física do titular ou de terceiro;

f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou

g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

5.5.4.11. O compartilhamento de dados deve ser operacionalizado em formato que assegure a necessária segurança da base de dados, como criptografia, anonimização, pseudonimização ou técnicas similares que alcancem idêntico escopo.

5.5.4.12. As partes (CONTRATANTE e CONTRATADA) deverão condicionar a realização das operações de tratamento de dados pessoais à assinatura de Termo de Confidencialidade, cujas cláusulas explicitem as obrigações e responsabilidades pertinentes.

5.5.4.13. O CONTROLADOR e OPERADOR deverão manter o registro das operações de tratamento de dados pessoais que realizarem, assim como estabelecer regras de boas práticas, considerando a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular.

5.5.4.14. O CONTROLADOR e OPERADOR, no âmbito de suas competências, deverão estabelecer regras de boas práticas e de governança que estabeleçam os aspectos procedimentais adequados para o cumprimento das diretrizes normativas, como:

a) as condições de organização;

b) o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares;

c) as normas de segurança;

d) os padrões técnicos;

e) as obrigações específicas para os diversos envolvidos no tratamento; e

f) as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos.

5.5.4.15. É vedada a transferência de dados pessoais, pela CONTRATADA, para fora do território do Brasil sem o prévio consentimento, por escrito, do CONTRATANTE, e demonstração da observância, pela CONTRATADA, da adequada proteção desses dados, cabendo à CONTRATADA o cumprimento de toda a legislação de proteção de dados ou de privacidade de outro (s) país (es) que for aplicável.

5.5.4.16. A responsabilidade pelo cumprimento das diretrizes contempladas na Lei nº 13.709/18, especialmente no tocante ao tratamento de dados pessoais adequados e legítimos, será de responsabilidade do órgão contratante que, ao figurar como agente de tratamento, assumirá as obrigações imputadas na legislação.

5.5.4.17. A CONTRATADA poderá responder por quaisquer danos, perdas ou prejuízos causados a CONTRATANTE, ou a terceiros, decorrentes do descumprimento da Lei Federal nº13.709/2018, não excluindo ou reduzindo essa responsabilidade a fiscalização do CONTRATANTE em seu acompanhamento.

5.5.4.18. A CONTRATADA deve atender à Política de Segurança da Informação instituída pela Instrução Normativa PRODERJ PRE nº 02, de 28 de abril de 2022, e demais normativos correlatos publicados pelo CONTRATANTE.

5.6. **Requisitos Socioambientais**

5.6.1. A contratada deverá promover a correta destinação dos resíduos resultantes da prestação do serviço, tais peças substituídas, embalagens, entre outros, observando a legislação e princípios de responsabilidade socioambiental (Lei nº 12.305/2010).

5.6.2. Deverá ainda obedecer aos critérios previstos no capítulo I do Decreto 43.629/2012, por meio dos artigos 1º e 2º, in verbis:

Art. 1º - As especificações para a aquisição de bens, contratação de serviços e obras por parte dos órgãos e entidades da Administração Pública Estadual Direta e Indireta, a fixação de critérios de julgamento e a execução e fiscalização dos respectivos contratos, observarão critérios de sustentabilidade ambiental, na forma deste Decreto.

Art. 2º - Consideram-se critérios de sustentabilidade ambiental, dentre outros:

I - economia no consumo de água e energia;

II - minimização da geração de resíduos e destinação final ambientalmente adequada dos que forem gerados;

III - racionalização do uso de matérias-primas;

IV - redução da emissão de poluentes;

V - adoção de tecnologias menos agressivas ao meio ambiente;

VI - implementação de medidas que reduzam as emissões de gases de efeito estufa e aumentem os sumidouros;

VII - utilização de produtos de baixa toxicidade;

VIII- utilização de produtos com a origem ambiental sustentável comprovada, quando existir certificação para o produto.

5.7. **Requisitos Tecnológicos:**

5.7.1. **De arquitetura tecnológica**

5.7.1.1. Os requisitos tecnológicos de arquitetura da solução, relacionados aos itens de compra do objeto, encontram-se no Anexo I - Especificações Técnicas do Objeto.

5.7.1.2. Os requisitos tecnológicos relacionados aos itens de serviço (treinamento) do objeto, encontram-se no subtópico 5.2. deste documento.

5.7.2. **De projeto e de implementação**

5.7.2.1. A CONTRATADA deve realizar, nas dependências da CONTRATANTE, antes do início da implantação da solução, uma reunião inicial de projeto (kick-off) em conjunto com as áreas de Segurança da Informação e infraestrutura da Contratada para definir o Plano de Trabalho de instalação e configuração da solução.

5.7.2.2. Após a reunião de kick-off a CONTRATADA deverá produzir e entregar ao CONTRATANTE o Projeto Executivo elaborado com base no quanto acertado ao longo da reunião, contemplando o planejamento, escopo, cronograma, discriminação dos produtos entregáveis, dimensionamento da infraestrutura tecnológica necessária, discriminação da equipe do projeto com perfis e quantitativos mínimos, relatório de controle e tratamento de riscos do projeto e demais artefatos que se façam necessários no entendimento da Contratada.

5.7.2.3. Compreende-se nesta etapa a instalação de equipamentos, sistemas, softwares e aplicativos da CONTRATANTE nos PRODUTOS fornecidos, bem como a migração das configurações existentes na CONTRATANTE para os produtos fornecidos pela CONTRATADA, caso haja viabilidade;

5.7.2.4. A etapa de instalação e configuração deve acontecer de forma gradual e transparente, de acordo com a conveniência da CONTRATANTE.

5.7.2.5. Durante esta etapa, a equipe da CONTRATADA deverá estar presente nos horários de testes, implantação e migração, definidos pela CONTRATANTE.

5.7.2.6. As atividades de instalação e configuração, de acordo com a necessidade, poderão ser executadas em horário comercial, período noturno ou final de semana.

5.7.2.7. Durante a etapa de instalação e configuração, os produtos fornecidos pela CONTRATADA serão colocados em plena operação, em condições reais de produção.

5.7.2.8. A CONTRATADA deverá, com a supervisão e aprovação da CONTRATANTE, planejar e realizar a instalação e configuração dos softwares com total interoperabilidade no ambiente atual da CONTRATANTE, sem impacto no ambiente de produção.

5.7.2.9. Durante a implantação e integração, caso seja necessário, a CONTRATADA deverá realizar, entre outras atividades: instalação de softwares, acompanhamento de migrações de regras e políticas, elaboração e execução de scripts, análise de performance, tunning, resolução de problemas e implementação de segurança.

5.7.2.10. Para instalação e configuração devem ser consideradas as seguintes premissas:

a) Caberá à CONTRATADA a disponibilização de todos os recursos necessários, tais como hardwares, softwares e recursos humanos necessários à instalação das soluções;

b) Caberá à CONTRATADA disponibilização de ferramentas / scripts de retorno imediato ao estado original da estrutura da CONTRATANTE caso a instalação dos produtos / softwares da CONTRATADA apresente falha.

c) A CONTRATADA deverá fornecer todas as licenças necessárias dos PRODUTOS ofertados e dos elementos adicionais que se fizerem necessários à instalação e ao pleno funcionamento do ambiente de produção.

5.7.2.11. O fornecedor deverá submeter previamente, por escrito, à Contratante, para análise e aprovação, quaisquer mudanças nos métodos executivos que fujam às especificações acordadas.

5.7.2.12. O encaminhamento formal das demandas, considerados cada um dos itens do objeto, ocorrerá sempre por meio de emissão de Ordem de Serviço/Fornecimento.

5.7.3. **Do suporte técnico e garantia do produto**

5.7.3.1. **Suporte Técnico**

I - A contratada deverá disponibilizar por meio da Internet uma aplicação WEB para registro dos chamados de suporte técnico através de login e senha fornecida para os usuários autorizados da contratante, em regime de 24x7x365 (vinte e quatro horas por dia durante todos os dias do ano, inclusive sábados, domingos e feriados);

II - A contratante poderá efetuar um número ilimitado de chamados para suporte técnico, durante a vigência da garantia, para suprir suas necessidades com relação a solução adquirida;

III - Considera-se "suporte técnico" a facilidade de comunicação colocada à disposição do CONTRATANTE para a prestação de informações, esclarecimentos ou orientações sobre a utilização, funcionalidades (dicas e atalhos), configuração de softwares/hardwares básicos, aplicativos, sistemas da informação em geral envolvidos na solução objeto da contratação, bem como a intervenção direta nos equipamentos para configurações, instalações e remoções de aplicativos, atualizações de softwares e reparos diversos necessários ao bom funcionamento da solução;

IV - O suporte técnico será acionado sempre que a solução apresentar falha que impeça o seu funcionamento regular e requeira uma intervenção técnica especializada e mesmo a substituição de seus componentes;

V - Durante o atendimento, a contratada poderá analisar a solução, sua atual condição de funcionamento, seus logs de sistema e sugerir mudanças para uma melhor prática de utilização da ferramenta. A equipe técnica do contratante decidirá sobre a aplicação ou não das recomendações;

VI - Cada pessoa cadastrada no sistema como usuário deverá receber identificação e senha que permitam acesso seguro tanto ao sistema, como ao recurso de abertura de chamadas de suporte técnico, de maneira a evitar que pessoas não autorizadas possam acionar o suporte;

VII - O fabricante deverá efetuar a troca de peças ou do equipamento, em que sejam constatadas quaisquer falhas ou defeitos de fabricação. Eventuais substituições de hardware deverão ser realizadas em até 1 (um) dia útil, a partir da constatação da necessidade de substituição do componente de hardware;

VIII - Os prazos de atendimento do suporte técnico da solução devem ter como referência os níveis de severidade, todos informados na tabela abaixo, ficando a contratada sujeita às sanções previstas na lei em caso de descumprimento contratual:

Tabela de Severidades dos Chamados e Prazos de Atendimento / Solução			
Severidade	**Descrição**	**Tempo de 1º contato após abertura do chamado**	**Tempo de Solução**
Urgente	Objeto totalmente inoperante	até 30 minutos	até 2 horas
Importante	Solução parcialmente inoperante – Necessidade de suporte na solução com a necessidade de interrupção de funcionamento da solução	até 1 hora	até 4 horas
Normal	Solução não inoperante, mas com problema de funcionamento – Necessidade de suporte na solução sem a necessidade de interrupção de funcionamento da solução	até 2 horas	até 24 horas
Informação	Solicitações de informações diversas ou dúvidas sobre a solução	até 8 horas	até 48 horas

IX - A severidade do chamado poderá ser reavaliada quando verificado que a mesma foi erroneamente aplicada, passando a contar no momento da reavaliação os novos prazos de atendimento e solução;

X - A cada abertura de chamado CONTRATADA poderá solicitar a prorrogação de quaisquer dos prazos para conclusão de atendimentos de chamados, desde que o faça antes do seu vencimento e devidamente justificado. Caberá à CONTRATANTE aceitar ou não o pedido de prorrogação do prazo.

XI - Todos os prazos para atendimento do suporte começarão a ser contados a partir da abertura do chamado independentemente de este ter sido feito via telefone, e-mail ou website do fornecedor.

5.7.3.2. **Garantia do Produto**

XII - A Garantia do Produto (para os itens 1, 2, 3, 4 de todos os lotes) obedecerá às seguintes regras:

XIII - Considera-se "garantia" a obrigação da CONTRATADA em reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, o objeto do contrato (e quaisquer de seus componentes) em que se verificarem vícios de produto, defeitos ou incorreções, durante o prazo de garantia especificado neste documento;

XIV - A garantia terá duração de 60 (sessenta meses), contados a partir da data do recebimento definitivo do objeto;

XV - A garantia deve obrigatoriamente prover, ao longo de sua duração e sem ônus adicionais para o contratante:

a) Acesso para downloads de patches, drivers, e quaisquer outras atualizações de software necessárias, que devem estar disponíveis no website do fabricante da solução, sem custos adicionais ao Contratante, durante todo o período de garantia.

b) Disponibilizar as revisões dos manuais técnicos e/ou documentação dos equipamentos adquiridos.

5.7.4. **De experiência da equipe que executará os serviços relacionados à solução de TIC e formação da equipe que projetará, implementará e implantará a solução de TIC**

Não se aplica.

5.7.5. **De metodologia de trabalho**

5.7.5.1. São instrumentos formais de comunicação entre a CONTRATANTE e a CONTRATADA:

a) Ordem de Serviço/Fornecimento;

b) Plano de Inserção;

c) Termos de Recebimento;

d) Chamado registrado na Central de Atendimento;

e) Ofícios;

f) Relatórios e Atas de Reunião;

g) E-mail;

h) Demais Termos previstos no instrumento convocatório.

5.7.5.2. A comunicação entre a CONTRATANTE e a CONTRATADA, para fins de encaminhamento de Ordens de Fornecimento/Serviço ou outro documento, ocorrerá sempre por intermédio do preposto, ou seu substituto, designado pela CONTRATADA;

5.7.5.3. A comunicação dos usuários com a Central de Atendimento/Suporte da CONTRATADA poderá ser realizada por meio de abertura de chamado via telefone com registro de protocolo ou utilização de sistema informatizado que permita o registro da demanda.

5.8. **Requisitos Materiais e Humanos**

5.9. Materiais, insumos e acessórios necessários ao perfeito funcionamento da solução deverão ser arcados pela CONTRATADA, sem custos adicionais para a CONTRATANTE.

5.10. Em observação ao entendimento do Enunciado nº 14, item 5 da Procuradoria-Geral do Estado do Rio de Janeiro - PGE/RJ, saliente-se que o objeto da presente contratação, que contempla serviços de treinamento, não prevê o uso de mão de obra residente/dedicada nas dependências do órgão contratante. Adicionalmente registre-se que o objeto também não caracteriza, forma alguma, terceirização de atividade-fim, tendo em vista que se trata de contratação, em regime de compra de equipamentos de tecnologia e respectivos cursos de treinamento, bem como suporte técnico específico do fabricante/fornecedor representante, no âmbito da garantia comum de mercado, que estão diretamente relacionado à atuação de profissionais e especialistas nas soluções contratadas.

5.10.1. **Quantitativo de usuários:**

Não se aplica

5.10.2. **Horário de funcionamento do órgão e horário em que deverão ser prestados os serviços:**

5.10.2.1. Considerada a prestação do Suporte Técnico, o horário de funcionamento do órgão é entre 09hs e 18hs, de segunda a sexta-feira, resguardadas eventuais emergências cuja ocorrência se dê em qualquer horário e dia.

5.10.2.2. O acesso de representante da contratada nas dependências da contratante, deverá ocorrer mediante prévia comunicação entre as partes, por meio dos mecanismos de comunicação definidos neste instrumento.

5.11.3. **Restrições de área, identificando questões de segurança institucional, privacidade, segurança, medicina do trabalho, dentre outras:**

Na forma do subtópico 5.5.4.18 deste documento, no que couber.

5.11.4. **Disposições normativas internas:**

Na forma do subtópico 5.5.4.18. deste documento.

5.11.5. **Instalações, especificando-se a disposição de mobiliário e equipamentos, arquitetura, decoração, dentre outras:**

Não se aplica

5.11.6. **Indicação da relação do material adequado para a execução dos serviços com a respectiva especificação:**

Não se aplica

5.12. **Providências a serem adotadas pela administração previamente à celebração do contrato**

Capacitação de servidores ou de empregados para fiscalização e gestão contratual, não havendo outras providências a serem adotadas que sejam antecedentes e necessárias à celebração do contrato.

5.13. **Fsicalização e Acompanhamento do Contrato**

A execução do contrato será acompanhada e fiscalizada por Comissão de Fiscalização de Contrato, composta por 3 (três) membros da Contratante especialmente designados pela autoridade competente, que será responsável por atestar o pagamento das faturas mediante a conferência de que a CONTRATADA atendeu todos os requisitos do Termo de Referência e do Contrato. A CONTRATADA deverá designar e manter preposto, em suas próprias dependências, que deverá se reportar diretamente à Comissão de Fiscalização de Contrato, para acompanhar e se responsabilizar pela execução do contrato, inclusive pela regularidade técnica e disciplinar da atuação de equipe técnica eventualmente disponibilizada para o cumprimento do objeto (bens e serviços).

5.14. **Acordo de Nível de Serviço**

5.14.1. **Finalidade:** Garantir a qualidade dos Serviços de Treinamentos (item 05 de cada lote).

5.14.2. **Periodicidade:** eventual, ao final do treinamento contratado, para fins de ateste de Nota Fiscal e emissão do Termo de Recebimento Definitivo

5.14.3. **Início da medição:** Imediatamente após a entrega do Relatório de Cumprimento do serviço de treinamento pela Contratada.

5.14.4. **Mecanismo de cálculo:** Os servidores participantes farão avaliação do curso com atribuição de grau, conforme os percentuais indicados abaixo:

a) I (insatisfatório) – 0 a 25%;

b) R (regular) – 25 a 50%;

c) B (bom) – 50 a 75%;

d) MB (muito bom) – 75 a 100%;

5.15. **Sanções**

5.15.1. A Comissão de Fiscalização de Contrato atestará a Nota Fiscal do treinamento realizado, sem aplicação de glosa, se no mínimo 60% das avaliações indicarem os graus B (bom) e/ou MB (muito bom).

5.15.2. A Comissão de Fiscalização de Contrato poderá aplicar alternativamente glosa de 2% sobre o valor da Nota Fiscal se 50% das avaliações indicarem o grau R (regular).

5.15.3. A Comissão de Fiscalização de Contrato poderá aplicar alternativamente glosa de 5% sobre o valor da Nota Fiscal se 50% das avaliações indicarem o grau I (insatisfatório).

5.15.4. Qualquer descumprimento do Acordo de Nível de Serviço poderá implicar as sanções previstas na da Lei de Licitações e Contratos.

5.15.5. Ficam resguardadas todas as sanções administrativas previstas na Lei de Licitações e Contratos.

6. NATUREZA DO OBJETO DA CONTRATAÇÃO

6.1. Os itens que integram o objeto possuem características comuns e usuais encontradas atualmente no mercado de TIC, cujos padrões de desempenho e de qualidade podem ser objetivamente definidos. Portanto, se enquadram como BENS COMUNS ou usuais de mercado.

6.2. O Objeto constitui solução em TIC, parcelado em três lotes que agregam o fornecimento de itens diversos para as soluções de firewall (Lote 1, Lote 2 e Lote 3), observados os seguintes aspectos:

a) Os itens nº 1, 2, 3, 4 (lote 1, lote 2 e lote 3) são medidos em unidades, e correspondem a aquisição de bens (compra);

b) Os itens nº 5 (lote 1, lote 2 e lote 3) são medidos por aluno/vaga, e correspondem a serviços de treinamento a ocorrerem sob demanda.

7. ESTIMATIVAS DAS QUANTIDADES A SEREM CONTRATADAS

7.1. As tabelas abaixo apresentam as quantidades estimadas da solução conforme as demandas do PRODERJ.

7.2. A estimativa das quantidades foi realizada pela Diretoria responsável pela Infraestrutura Tecnológica do PRODERJ, mesma área que, inclusive, será responsável pela operação técnica da solução a ser contratada.

7.3. A quantidade estimada dos appliances e consoles leva em conta a topologia de rede dos dois data centers do PRODERJ, além da necessária duplicidade de equipamentos, já que a redundância deles garantirá a resiliência da solução em caso de falhas. Por exemplo, caso seja necessário implementar firewall em um data center, deverão ser fornecidas ao menos duas unidades (por motivos de Alta Disponibilidade ou ainda Clusterização).

7.4. A quantidade estimada para os treinamentos considerou a capacitação, para os lotes 1 e 2, de um grupo de até 6 (seis) técnicos de cada uma das três áreas técnicas (infraestrutura, sistemas e segurança da informação) e para o lote 3 de um grupo de até 2 (dois) técnicos por área. Tais quantitativos consideraram o grau de relevância, na infraestrutura, das soluções tecnológicas às quais os treinamentos estão relacionados. Considerou ainda eventuais desligamentos de servidores treinados, de forma a viabilizar o treinamento de um outro servidor.

7.5. Não há expectativa de compra pelo PRODERJ para o Lote 3 (Firewall Tipo 3). Não obstante, o item foi concebido para oferta como opção técnica aos outros órgãos partícipes/aderentes do futuro Sistema de Registro de Preços, observadas as suas topologias e infraestruturas tecnológicas.

LOTE 1 - FIREWALL TIPO 1				
Item	**ID SIGA**	**Descrição**	**Métrica**	**Quantidade**
1	168256	APPLIANCE FIREWALL TIPO 1 - INCLUSOS: HARDWARE, LICENCIAMENTO, INSTALAÇÃO, CONFIGURAÇÃO E GARANTIA POR 60 MESES	UN	10
2	172443	CONSOLE DE GERENCIAMENTO CENTRALIZADO PARA O FIREWALL TIPO 1 COM GARANTIA DE 60 MESES	UN	4
3	172442	CONSOLE DE GERENCIAMENTO DE LOGS PARA O FIREWALL TIPO 1 COM GARANTIA DE 60 MESES	UN	4
4	172444	CONSOLE DE RELATORIA CENTRALIZADA PARA O FIREWALL TIPO 1 COM GARANTIA DE 60 MESES	UN	4
5	180944	TREINAMENTO OPERACIONAL PARA A SOLUÇÃO DO LOTE 1	Aluno	18

LOTE 2 - FIREWALL TIPO 2				
Item	**ID SIGA**	**Descrição**	**Métrica**	**Quantidade**
1	168257	APPLIANCE FIREWALL TIPO 2 - INCLUSOS: HARDWARE, LICENCIAMENTO, INSTALAÇÃO, CONFIGURAÇÃO E GARANTIA POR 60 MESES	UN	10
2	180938	CONSOLE DE GERENCIAMENTO CENTRALIZADO PARA O FIREWALL TIPO 2 COM GARANTIA DE 60 MESES	UN	4
3	180940	CONSOLE DE GERENCIAMENTO DE LOGS PARA O FIREWALL TIPO 2 COM GARANTIA DE 60 MESES	UN	4
4	180942	CONSOLE DE RELATORIA CENTRALIZADA PARA O FIREWALL TIPO 2 COM GARANTIA DE 60 MESES	UN	4
5	180945	TREINAMENTO OPERACIONAL PARA A SOLUÇÃO DO LOTE 2	Aluno	18

LOTE 3 - FIREWALL TIPO 3				
Item	**ID SIGA**	**Descrição**	**Métrica**	**Quantidade**
1	168258	APPLIANCE FIREWALL TIPO 3 - INCLUSOS: HARDWARE, LICENCIAMENTO, INSTALAÇÃO, CONFIGURAÇÃO E GARANTIA POR 60 MESES	UN	0
2	180939	CONSOLE DE GERENCIAMENTO CENTRALIZADO PARA O FIREWALL TIPO 3 COM GARANTIA DE 60 MESES	UN	0
3	180941	CONSOLE DE GERENCIAMENTO DE LOGS PARA O FIREWALL TIPO 3 COM GARANTIA DE 60 MESES	UN	0
4	180943	CONSOLE DE RELATORIA CENTRALIZADA PARA O FIREWALL TIPO 3 COM GARANTIA DE 60 MESES	UN	0
5	180946	TREINAMENTO OPERACIONAL PARA A SOLUÇÃO DO LOTE 3	Aluno	0

8. LEVANTAMENTO DE MERCADO

8.1. **Levantamento das Soluções**

Solução 1 - Utilização de ferramenta de Firewall código aberto (open source)

Existem diversas soluções de firewall open source e/ou gratuitas disponíveis no mercado, e algumas delas possibilitam o atendimento a ambientes corporativos de baixa, média e alta complexidade.

- **Vantagens**: No mercado existem soluções open source que oferecem a maioria das funcionalidades disponíveis nas soluções de firewall corporativas, dispondo, inclusive, de suporte técnico da solução na forma de subscrição, de modo a garantir que o Contratante tenha o auxílio do fabricante no sentido de manter a solução em funcionamento por todo o ciclo de vida do software. Soluções open source normalmente possuem diversos fóruns colaborativos na internet, dedicados a resolver questões de implementação, configuração e outros problemas com as ferramentas.

- **Desvantagens**: Embora as soluções open source não apresentem custos financeiros diretos, decorrentes da aquisição de uma solução de firewall corporativo (desconsiderando a opção de suporte pago), existe o custo operacional e até mesmo financeiro do provimento e manutenção da infraestrutura física necessária para que o firewall opere. Em outras palavras, ao utilizar uma solução de firewall open source, a instituição fica responsável pela manutenção e reposição dos componentes de hardware que venham a ser utilizados, e ainda sob risco de não dimensionar adequadamente as capacidades do equipamento para as tarefas a serem desempenhadas. Em cenários open source, não é raro observarmos a instalação do sistema operacional do firewall até mesmo em estações de trabalho, ou seja, em equipamentos completamente inadequados ao processamento do tráfego de rede em ambientes corporativos. Implementações inadequadas de firewall open source podem ocasionar a indisponibilidade de ambientes inteiros, e dispondo apenas de suporte técnico para o software do firewall, o risco de demora no restabelecimento dos serviços é considerável, podendo ainda repercutir em ônus ao poder público.

Solução 2 - Contratação de Firewall em Nuvem (cloud firewall)

Outra possibilidade existente no mercado é a contratação de uma solução de firewall baseada em nuvem, normalmente utilizada para a proteção de infraestruturas hospedadas em nuvens públicas, privadas ou híbridas. Os principais fabricantes do mercado normalmente oferecem a solução no formato “pay-as-you-go", ou seja, com a cobrança seja por hora de uso ou por gigabyte trafegado.

- **Vantagens**: Tais soluções de nuvem permitem uma implementação mais ágil da ferramenta, pois esta não envolve ajustes no data center e outros requisitos de infraestrutura local. Outro benefício seria o da escalabilidade da solução, realizada de maneira simplificada na nuvem, caso necessário.

- **Desvantagens**: Soluções de firewall baseadas em nuvem, via de regra são utilizadas em implementações em nuvem, como é o caso do IaaS (Infrastructure as a Service), modelo onde a contratante mantém seus recursos computacionais em nuvens de terceiros. Considerando o escopo do problema a ser resolvido na presente demanda, que é a segurança do perímetro de rede local, uma solução voltada para infraestrutura em nuvem não seria a melhor escolha tecnológica neste caso.

Solução 3 - Aquisição de firewall em formato appliance

Neste cenário, o fornecimento do firewall ocorreria via aquisição perpétua da solução, composta de hardware especializado, sistemas operacionais, mais o serviço de instalação e configuração inicial. Quanto ao suporte técnico, sua vigência seria então ajustada para ser concomitante ao ciclo de vida da solução. Haveria ainda a oferta de treinamentos operacionais, o que é praxe em contratações de soluções tecnológicas.

- **Vantagens**: Esta terceira hipótese contribuiria para uma estratégia de segurança independente, desvinculando o fornecimento dos firewalls a contratação de links de internet, como ocorre atualmente no Governo do Estado. A aquisição da solução, com suporte vinculado ao tempo de vida da mesma, proporcionaria também os benefícios da continuidade operacional, economia de tempo e mão de obra empregada em renovações contratuais, além da redução da curva de aprendizado ocasionada a cada troca de tecnologia.

- **Desvantagens**: Considerando que em uma nova contratação para solução de firewall, não haveria a indicação de fabricante específico, provavelmente a empresa arrematante forneceria solução de outro fabricante, diferente do que atualmente é empregado no PRODERJ e em outros órgãos, o que, por motivos de incompatibilidade tecnológica, dificultaria a migração de regras, políticas e configurações de firewall atualmente em uso para a nova solução, implicando refazer as configurações de firewall do Contratante.

8.2. **Análise de Projetos Similares**

8.2.1. Pesquisa realizada com base no Portal da Transparência, mantido pela Controladoria Geral da União, bem como nos sítios virtuais dos respectivos órgãos.

8.2.2. Foram identificadas os seguintes procedimentos formalizados por outros Órgãos Públicos, com demandas similares às do objeto a ser contratado:

ÓRGÃO / ENTIDADE		Nº Contrato / Edital	Valor (R$)	Fornecedor	Natureza do Objeto	Período de subscrição / garantia do produto	ANÁLISE DA CONTRATAÇÃO	VANTAGENS	DESVANTAGENS
01	Defensoria Pública da União - DPU	P.E. nº 108/2022 (67541338)	--------	Global Sec. Tecnologia & Informação Eireli	Aquisição perpétua	36 meses	O objeto do lote único trata sobre a aquisição de equipamentos de firewall, disponíveis em três diferentes tamanhos/capacidades. O "firewall tipo 1" do referido processo apresenta inclusive diversas semelhanças técnicas com o nosso também chamado "firewall tipo 1". Quanto aos firewalls tipos 2 e 3 do lote único, além de não envolverem a entrega de hardware, ainda apresentavam capacidades muito abaixo das que foram estipuladas para o presente Estudo	No referido processo, a DPU estabeleceu três diferentes tamanhos/capacidades de equipamentos. O fato de todos eles constarem em um único lote, e portanto, os três tamanhos serem de um mesmo fabricante, viabiliza diversas opções de topologia de rede, que não estariam disponíveis caso os equipamentos fossem de fabricantes distintos.	Entende-se que a definição de somente 36 meses de garantia para os equipamentos adquiridos não traria vantajosidade técnica/econômica, pois no caso de equipamentos NGFW, costuma-se observar como padrão de ciclo de vida de equipamentos de segurança, um prazo de 5 anos (ou 60 meses).
02	Empresa Brasileira de Administração de Petróleo e Gás Natural S.A. - PPSA	P.E. nº 003/2022 (67540862)	------	-------	Aquisição perpétua	60 meses	O objeto deste processo é composto de item único dentro de um lote único. Trata-se da aquisição de equipamentos de firewall, inclusos no valor do equipamento, todos os serviços necessários para o funcionamento da solução, como "instalação", "configuração" e "treinamento". O equipamento descrito no processo apresenta algumas semelhanças com nosso "firewall tipo 3".	O período de garantia de 60 meses é adequado, uma vez que cobre todo o ciclo de vida útil da solução tecnológica.	O fato do serviço de treinamento estar embutido no custo do equipamento não é uma boa estratégia para a oferta da solução no contexto de Sistema de Registro de Preços, onde um partícipe poderá contratar o número exato de treinamento, conforme suas necessidades.
03	Hospital Universitário de Santa Maria - UFSM/EBSH	Contrato nº 030/2023 (67543888) P.E. nº 126/2022 (67541802)	802.379,00	Approach Tecnologia Ltda	Aquisição perpétua	36 meses	O objeto deste processo é composto de item único dentro de um lote único. Trata-se da aquisição de equipamentos de firewall, inclusos no valor do equipamento, todos os serviços necessários para o funcionamento da solução, como "instalação", "configuração" e "treinamento". O equipamento descrito no processo apresenta algumas semelhanças com nosso "firewall tipo 3".	O período de garantia de 60 meses é adequado, uma vez que cobre todo o ciclo de vida útil da solução tecnológica.	O fato do serviço de treinamento estar embutido no custo do equipamento não é uma boa estratégia para a oferta da solução no contexto de Sistema de Registro de Preços, onde um partícipe poderá contratar o número exato de treinamento, conforme suas necessidades.
04	Instituto Federal de Educação, Ciência e Tecnologia de Sergipe - IF-SE	P.E. nº 016/2023 (67542697) Termo de homologação (67545175)	Item 1 677.497,05 Item 2 151.191,84 Item 3 63.824,87 Item 4 36.556,77 Item 5 170.556,80	TLD Teledata Comércio e Serviços Ltda Vtech Comércio, Serviços e Equipamentos de Informática Ltda TLD Teledata Comércio e Serviços Ltda	Aquisição perpétua	60 MESES	O objeto é composto de lote único e 5 itens, todos eles contemplando 5 diferentes tamanhos de firewall. Os custos da instalação, configuração e treinamento estão embutidos no custo do equipamento.	O objeto apresenta várias opções de capacidade para os equipamentos de firewall. Apresenta período de garantia definido para 60 meses.	Não foi solicitado no pregão nenhum tipo de gerenciamento centralizado para os equipamentos, o que prejudica o aspecto da visibilidade de eventos de segurança.
05	Ministério das Comunicações	Contrato nº 122/2022 (67544357) P.E. SRP nº 12/2022 (67543086)	1.300.000,00 (valores unitários discriminados no termo de contrato)	NCT Informática Ltda	Aquisição perpétua	60 MESES	Este objeto compreende um lote único, composto de quatro itens: O primeiro item corresponde ao "Firewall Tipo 3" do presente objeto, o segundo item é uma console de logs, o terceiro um serviço de instalação e o quarto item corresponde ao treinamento operacional.	A aquisição de uma solução de firewall NGFW representa a adição de uma importante camada de segurança cibernética na referida instituição. Apresenta período de garantia definido para 60 meses.	A capacidade especificada para o equipamento do referido pregão está abaixo do necessário para atendimento ao PRODERJ. Para a presente demanda, será necessário ofertar ao menos três opções de capacidade, a fim de cobrir maior número de cenários.
06	Superintendência da Zona Franca de Manaus - SUFRAMA	Contrato nº 04/2023 (67544381) P.E. nº 01/2023 (67542169)	1.854.791,00 (valores unitários discriminados no termo de contrato)	COMDADOS Comércio e Serviços Eletrônicos Ltda	Aquisição perpétua	60 MESES	O objeto deste processo compreende um lote único, composto de sete itens: O primeiro deles corresponde ao "Firewall tipo 3" do presente objeto, o segundo item é o serviço de instalação e configuração do primeiro item, o terceiro é aquisição de appliance de gerenciamento de logs, o quarto item é o treinamento operacional do primeiro item, o quinto item é aquisição de equipamento menos robusto que o do primeiro item, o sexto item instalação e configuração para o equipamento do quinto item, e finalmente o sétimo item, que é a console de gerenciamento centralizado que servirá para os itens 1 e 5.	A SUFRAMA definiu ao menos dois tamanhos de firewall para o atendimento a necessidades distintas, e separou as consoles de gerenciamento e de logs. Apresenta período de garantia definido para 60 meses.	As especificações técnicas para o quinto item estavam ausentes na documentação do referido processo.
07	Superintendência Nacional de Previdência Complementar - PREVIC	Contrato nº 09/2022 (67545917) P.E. nº 04/2022 (67542191)	1.200.000,00 (valores unitários discriminados no termo de contrato)	Approach Tecnologia Ltda	Aquisição perpétua	48 MESES	O objeto deste processo compreende um lote único, composto de três itens: O primeiro corresponde ao "Firewall tipo 3" do presente objeto, o segundo item corresponde ao serviço de instalação e configuração do equipamento, e o terceiro item, abrangendo o treinamento na solução.	A aquisição de uma solução de firewall NGFW representa a adição de uma importante camada de segurança cibernética na referida instituição.	Entende-se que o período definido para a garantia do produto (48 meses) é insuficiente para cobrir todo o ciclo de vida do equipamento adquirido. É desnecessária a composição de um item específico para instalação e configuração.
08	Tribunal de Contas do Estado do Piauí - TCE-PI	Contrato nº 038/2022 (67544682) P.E. nº 019/2022 (67542836)	2.099.000,00 (valores unitários discriminados no termo de contrato)	Approach Tecnologia Ltda	Aquisição perpétua	60 MESES	O objeto compreende um lote com apenas um item, e este corresponde ao "Firewall tipo 2" proposto no objeto apresentado neste Estudo Técnico.	A composição do item único abrange o equipamento, a instalação do mesmo, e todas as demais características necessárias ao pleno funcionamento do equipamento.	Não foi previsto na documentação do referido pregão, nenhum tipo de treinamento de capacitação na solução adquirida.
09	Tribunal Regional Federal 1ª Reg. - TRF1	P.E (SRP) nº 05/2023 (67543631) Resultado Termo de homologação (67544900)	Lote 1 3.906.866,18 (ref. Firewall tipo 1) Lote 2 705.000,00 Lote 3 423.000,00 Lote 4 423.000,00 Lote 5 1.146.000,00	Adistec Brasil Informática Ltda Blockbit Tecnologia Ltda	Aquisição perpétua	60 MESES	Não foi previsto na documentação do referido pregão, nenhum tipo de treinamento de capacitação na solução adquirida.	No processo analisado, o TRF1 optou por disponibilizar várias capacidades de firewall, o que evita desperdícios com superdimensionamento. Apresenta período de garantia definido para 60 meses.	Mesmo oferecendo 6 diferentes opções de capacidades elas eram muito semelhantes entre si, especialmente no que diz respeito ao throughput de proteção, que não apresentou muitas variações significativas nas 6 opções.
10	Universidade Federal da Paraíba - UFP	Contrato nº 014/2022 (67544704) P.E. nº 53/2022 (67543941)	383.900,00 (valores unitários discriminados no termo de contrato)	ARPSIST Serviços de Engenharia Ltda	Aquisição perpétua	36 MESES	O objeto compreende um lote com apenas um item, e este apresenta semelhança ao "Firewall tipo 3" do presente objeto.	A composição do item único abrange o equipamento, a instalação do mesmo, e todas as demais características necessárias ao pleno funcionamento do equipamento.	Não foi previsto na documentação do referido pregão, nenhum tipo de treinamento de capacitação na solução adquirida.
11	Prefeitura Municipal de Itaguaí/RJ	Contrato nº 164/2022 (67545524) P.E. nº 032/2022 (67543220)	1.173.100,00 (valores unitários discriminados no termo de contrato)	Blockbit Tecnologia Ltda	Aquisição perpétua	36 MESES	O objeto compreende um lote único, onde constam 6 itens, sendo os dois primeiros referentes a equipamentos firewall de capacidades distintas, o terceiro item corresponde ao suporte técnico da solução, o quarto item é um serviço de customização da ferramenta, o quinto item é o sistema de gerenciamento centralizado dos equipamentos, finalmente o sexto item contendo módulos de expansão de interfaces de rede.	A Prefeitura definiu ao menos dois tamanhos de firewall para o atendimento a necessidades distintas, e especificou ainda a console de gerenciamento centralizado.	É desnecessária a inclusão do sexto e último item: "Módulo de Interface de rede SFP+", pois bastaria simplesmente definir a quantidade de interfaces nas especificações técnicas, em vez de adquirir mais interfaces de rede em separado.

8.2.3. Consta do portal do Sistema Integrado de Gestão de Aquisições (SIGA-RJ), contratação realizada pelo PRODERJ no ano de 2012, conforme relatório (68186938), com os destaques abaixo informados. Saliente-se que, em razão do extenso lapso temporal desde a referida contratação, ela não foi considerada na tabela acima como referência, uma vez que foram encontrados processos mais recentes, com valores atualizados e com objeto mais próximo do modelo proposto neste estudo

8.2.4. Contrato firmado com a empresa CONTACTA SEGURANÇA EM CONECTIVIDADE LTDA, com vigência entre 05.12.2012 e 04.12.2013, com status de "cancelado", tendo por objeto a "ATUALIZAÇÃO INFRAESTR. FIREWALL", com valor de R$4.290.602,55 (quatro milhões, duzentos e noventa mil, seiscentos e dois reais e cinquenta e cinco centavos).

8.3. **Estimativa Preliminar de Preços**

8.3.1. A estimativa preliminar do valor da contratação, visando uma análise comparativa quanto à viabilidade econômica do tipo de solução escolhida neste estudo técnico, considerou os parâmetros observados nos certames e contratações similares realizadas por outros órgãos da administração pública observados conforme a tabela do subtópico 8.2.2. deste documento.

8.3.2. Saliente-se, em observação do item 8.2 da Nota Técnica nº 6/2023 do Egrégio Tribunal de Contas do Estado do Rio de Janeiro, no que se refere ao art. 8º da Instrução Normativa SEGES/ME nº 65/2021, que não foi localizado, dentre os catálogos de soluções de TIC com condições padronizadas publicados pelo Governo Federal, nenhum referente à solução firewall ou similar que pudesse ser utilizado o preço de referência.

ESTIMATIVA DE PREÇOS PARA AQUISIÇÃO DE SOLUÇÃO DE FIREWALL
Outubro de 2023*

IDENTIFICAÇÃO DA CONTRATAÇÃO	PERÍODO DE GARANTIA	LOTE I - ESTIMATIVA DE PREÇO				
		Item 1 (valor unitário)	Item 2 (valor unitário)	Item 3 (valor unitário)	Item 4 (valor unitário)	Item 5 (valor unitário)
		FIREWALL TIPO 1	CONSOLE DE GERENCIAMENTO CENTRALIZADO	CONSOLE GERENCIAMENTO DE LOGS	CONSOLE DE RELATORIA	TREINAMENTO
Instituto Federal de Educação, Ciência e Tecnologia de Sergipe - IF-SE - P.E. nº 016/2023	60 MESES	R$ 630.072,26	ITENS NÃO SOLICITADOS NO PREGÃO			INCLUSO NO VALOR DO EQUIPAMENTO
Defensoria Pública da União - DPU - P.E. nº 108/2022	36 MESES	R$ 966.000,00	R$ 179.500,00	ITEM NÃO SOLICITADO NO PREGÃO	R$ 179.500,00	R$ 72.000,00**
IDENTIFICAÇÃO DA CONTRATAÇÃO	**PERÍODO DE GARANTIA**	**LOTE II - ESTIMATIVA DE PREÇO**				
		Item 1 (valor unitário)	**Item 2 (valor unitário)**	**Item 3 (valor unitário)**	**Item 4 (valor unitário)**	**Item 5 (valor unitário)**
		FIREWALL TIPO 2	**CONSOLE DE GERENCIAMENTO CENTRALIZADO**	**CONSOLE GERENCIAMENTO DE LOGS**	**CONSOLE DE RELATORIA**	**TREINAMENTO**
Tribunal de Contas do Estado do Piauí - TCE-PI - P.E nº 19/2022	60 MESES	R$ 1.049.500,00	ITENS NÃO SOLICITADOS NO PREGÃO			ITEM NÃO SOLICITADO NO PREGÃO
Tribunal Regional Federal 1ª Reg. - TRF1 - P.E nº 05/2023	60 MESES	R$ 1.499.209,32	R$ 185.381,73			R$ 17.476,93**
Tribunal Regional Federal 1ª Reg. - TRF1 - P.E nº 05/2023	60 MESES	R$ 966.788,81	R$ 185.381,73			R$ 17.476,93**
Tribunal Regional Federal 1ª Reg. - TRF1 - P.E nº 05/2023	60 MESES	R$ 662.000,00	ITENS NÃO SOLICITADOS NO PREGÃO			R$ 22.000,00**
Prefeitura Municipal de Itaguaí/RJ - P.E. nº 032/2022	36 MESES	R$ 249.225,00	R$ 160.000,00		ITEM NÃO SOLICITADO NO PREGÃO	ITEM NÃO SOLICITADO NO PREGÃO
IDENTIFICAÇÃO DA CONTRATAÇÃO	**PERÍODO DE GARANTIA**	**LOTE III - ESTIMATIVA DE PREÇO**				
		Item 1 (valor unitário)	**Item 2 (valor unitário)**	**Item 3 (valor unitário)**	**Item 4 (valor unitário)**	**Item 5 (valor unitário)**
		FIREWALL TIPO 3	**CONSOLE DE GERENCIAMENTO CENTRALIZADO**	**CONSOLE GERENCIAMENTO DE LOGS**	**CONSOLE DE RELATORIA**	**TREINAMENTO**
Empresa Brasileira de Administração de Petróleo e Gás Natural S.A. - PPSA - P.E. nº 003/2022	60 MESES	R$ 222.000,00	ITENS NÃO SOLICITADOS NO PREGÃO			INCLUSO NO VALOR DO EQUIPAMENTO
Instituto Federal de Educação, Ciência e Tecnologia de Sergipe - IF-SE - P.E. nº 016/2023	60 MESES	R$ 140.608,41	ITENS NÃO SOLICITADOS NO PREGÃO			INCLUSO NO VALOR DO EQUIPAMENTO
Ministério das Comunicações - P. E. SRP nº 12/2022	60 MESES	R$ 560.000,00	R$ 75.000,00			R$ 25.000,00**
Superintendência da Zona Franca de Manaus - SUFRAMA - P.E nº 001/2023	60 MESES	R$ 278.471,00	R$ 408.800,00	R$ 138.467,00		R$ 5.520,00**
Tribunal Regional Federal 1ª Reg. - TRF1 - P.E nº 05/2023	60 MESES	R$ 390.000,00	ITENS NÃO SOLICITADOS NO PREGÃO			R$ 10.500,00**
Tribunal Regional Federal 1ª Reg. - TRF1 - P.E nº 05/2023	60 MESES	R$ 390.000,00	ITENS NÃO SOLICITADOS NO PREGÃO			R$ 7.000,00**
Tribunal Regional Federal 1ª Reg. - TRF1 - P.E nº 05/2023	60 MESES	R$ 540.000,00	ITENS NÃO SOLICITADOS NO PREGÃO			R$ 10.500,00**
Superintendência Nacional de Previdência Complementar - PREVIC - P.E nº 004/2022	48 MESES	R$ 555.000,00	ITENS NÃO SOLICITADOS NO PREGÃO			R$ 40.000,00**
Hospital Universitário de Santa Maria - UFSM/EBSH - P.E. nº 126/2022	36 MESES	R$ 403.386,00	ITENS NÃO SOLICITADOS NO PREGÃO			R$ 12.993,00
Conselho Regional de Medicina do RS - CREMERS - P.E. nº 012/2022	36 MESES	R$ 159.600,00	ITENS NÃO SOLICITADOS NO PREGÃO			INCLUSO NO VALOR DO EQUIPAMENTO
Universidade Federal da Paraíba - UFP - P.E nº 53/2022	36 MESES	R$ 95.975,00	ITENS NÃO SOLICITADOS NO PREGÃO			ITEM NÃO SOLICITADO NO PREGÃO
Prefeitura Municipal de Itaguaí/RJ - P.E. nº 032/2022	36 MESES	R$ 110.850,00	R$ 160.000,00		ITEM NÃO SOLICITADO NO PREGÃO	ITEM NÃO SOLICITADO NO PREGÃO

* Na pesquisa realizada no "Painel de Preços do Governo Federal", foi utilizado como parâmetro o filtro "Ano da Compra: 2022 e 2023", pois foi necessário expandir a busca para o ano anterior, a fim de obtermos ao menos três valores para cada item. Os preços que constam na tabela são referentes a equipamentos semelhantes aos deste Estudo.

** Valor referente a uma turma.

8.4. **Avaliação Comparativa (Benchmarking)**

Observado o perfil técnico de soluções ofertadas no mercado, verifica-se que todas as soluções possuem características bem similares e atendem a maioria dos requisitos mínimos esperados na solução ora em estudo. Na tabela abaixo foram consideradas as características mais relevantes de um software "NG-AV" (Next-Generation Antivírus), tendo como base somente os fabricantes líderes. As informações são oriundas dos datasheets de cada solução, disponíveis nos websites oficiais dos respectivos fabricantes.

FUNCIONALIDADE	FABRICANTE / SOLUÇÃO			
	Palo Alto	Checkpoint	Fortinet	Blockbit
IPS	SIM	SIM	SIM	SIM
IDS	SIM	SIM	SIM	SIM
GEOPROTECTION	SIM	SIM	SIM	SIM

ANTI MALWARE	SIM	SIM	SIM	SIM
APPLICATION CONTROL	SIM	SIM	SIM	SIM
WEB FILTER	SIM	SIM	SIM	SIM
VPN (site-to-site e client-to-site)	SIM	SIM	SIM	SIM
ZERO DAY THREAT PREVENTION	SIM	SIM	SIM	NÃO
ANTI-BOT	SIM	SIM	SIM	SIM
ANTI-SPAM	SIM	SIM	SIM	SIM

9. JUSTIFICATIVA DA SOLUÇÃO ESCOLHIDA

Considerando os cenários das soluções apresentadas no tópico 8 deste documento, verificam-se inviáveis para a presente contratação:

9.1. Solução 1: Ainda que sirvam bem para resolver situações de emergência, as soluções open source, via de regra, não são as mais adequadas para implementação em ambientes corporativos, pois o suporte técnico estaria disponível somente para os componentes de software da solução, ou seja, quaisquer problemas relativos a hardware não seriam de responsabilidade da contratada, o que não seria adequado para as necessidades de negócio, que exigem responsabilização e pronto restabelecimento em caso de falhas.

9.2. Solução 2: Não obstante o grande entusiasmo do mercado com as soluções em nuvem, o que permanece evidente em nosso contexto da Administração Pública Estadual, é que os órgãos ainda mantêm seus ativos e serviços críticos em infraestruturas locais, ou ainda, encontram-se em um processo relativamente lento de migração para a nuvem híbrida do próprio PRODERJ. Desta forma, as soluções on premises foram priorizadas neste Estudo, já que a maior parte do tráfego da rede Governo passa pela infraestrutura da Autarquia. Levando em conta a crescente migração de data centers locais para nuvens, é provável que, dentro em breve, seja necessária a elaboração de estudo técnico específico, abordando a viabilidade de contratação para a referida solução de segurança em nuvem.

9.3. Isto posto, a "Solução 3 - Aquisição de firewall em formato appliance" é a mais adequada para o atendimento da demanda atual, que é a de proteção ao perímetro local de rede. A aquisição dos equipamentos suprirá adequadamente a questão do suporte ao hardware e software pelo tempo de vida útil da solução, enquanto a passagem de conhecimento ocorrerá por conta dos treinamentos. Levando em conta o atual contexto de dependência tecnológica do PRODERJ e demais órgãos em relação ao contrato do CONECTA-RJ, e considerando também a compatibilidade observada entre a "Solução 3" e o Sistema de Registro de Preços, o presente estudo técnico propõe a oferta de firewall em 3 (três) capacidades ou "tamanhos" diferentes, proporcionando um melhor ajuste às necessidades dos demais órgãos.

9.4. Quanto à definição do período de garantia do produto, observa-se nos projetos similares observados, que algumas instituições previram garantia de 60 meses, outras optaram por definir 36 meses. Conforme se observa na tabela abaixo, onde está considerado o valor médio observado nas licitações e contratações de referência, verifica-se que a contratação por 60 meses mostrou-se mais vantajosa nos cenários de firewall tipos 1 e 3. Tais projeções devem ser confirmadas na ocasião da pesquisa de preços, realizada pelo setor competente.

COMPARATIVO DE PREÇOS - 36 X 60 MESES		
Firewall Tipo 1	**Preço Unitário (valor médio)**	**Preço Anual (fracionado pela quantidade de anos)**
60 meses	R$ 630.072,26	R$ 126.014,45
36 meses	R$ 966.000,00	R$ 322.000,00
Firewall Tipo 2	**Preço Unitário (valor médio)**	**Preço Anual (fracionado pela quantidade de anos)**
60 meses	R$ 1.044.374,53	R$ 208.874,91
36 meses	R$ 249.225,00	R$ 83.075,00
Firewall Tipo 3	**Preço Unitário (valor médio)**	**Preço Anual (fracionado pela quantidade de anos)**
60 meses	R$ 360,154,20	R$ 72.030,84
36 meses	R$ 219.653,67	R$ 73.217,89

10. ESTIMATIVA PRELIMINAR DO VALOR DA CONTRATAÇÃO

Tendo por referência o menor preço verificado nas licitações e contratações de referência, listadas no subtópico 8.2.2. deste estudo, a estimativa preliminar para uma futura contratação do objeto ora proposto é o apresentado na tabela abaixo:

Solução	Menor Preço Unitário (R$)	Estimativa Anual (fracionado pela quantidade de anos em R$)
Firewall tipo 1	**630.072,26**	126.014,45
Firewall tipo 2	**662.000,00**	132.400,00
Firewall tipo 3	**140.608,41**	28.121,68

11. DESCRIÇÃO DA SOLUÇÃO DE TI COMO UM TODO

Contratação de empresa do ramo de Tecnologia da Informação para o fornecimento de solução de firewall, com garantia de 60 meses, contemplando hardware e software, com instalação e configuração para os novos equipamentos, nas dependências do contratante e curso de treinamento oficial da solução.

12. JUSTIFICATIVAS PARA O PARCELAMENTO OU NÃO DA CONTRATAÇÃO

12.1. Tendo em vista o incentivo a competitividade no certame, optou-se por separar os três diferentes "tamanhos" de equipamentos de firewall e incluí-los em três diferentes grupos/lotes, adicionando a cada um deles seus respectivos itens agregados e opcionais, de forma a resguardar que as soluções de cada lote sejam oriundas de um mesmo fabricante, pois não seria necessária a compatibilização tecnológica entre os três lotes, bastando apenas que os itens de cada lote sejam compatíveis com os outros itens dentro daquele mesmo lote. Com o parcelamento do objeto conforme descrito neste documento, pretende-se compatibilizar o Estudo Técnico com as determinações do Enunciado nº 45 da Douta PGE-RJ.

12.2. O objeto foi concebido de modo a proporcionar aos órgãos participantes/aderentes a opção de contratação modular dos itens, não sendo necessária portanto, a contratação da totalidade dos mesmos, nem mesmo dentro de cada lote, e ao invés disso, a contratação daqueles itens e quantidades que atendam às necessidades específicas, na forma da Intenção no Registro de Preços (IRP) registrada pelos órgãos partícipes para o certame, consideradas as suas estruturas e especificidades de topografia e infraestrutura.

12.3. O objeto ora pretendido se configura em uma solução de TI composta por mais de um item e disposta em três lotes distintos. A aquisição dos itens da solução de firewall, bem como a execução dos treinamentos, têm por objetivo o melhor cumprimento dos requisitos técnicos e tecnológicos da solução, para a entrega das funcionalidades requisitadas pelo PRODERJ.

12.4. O agrupamento dos itens correspondentes à solução de firewall justifica-se por conta da diversidade em infraestruturas tecnológicas nos órgãos da Administração Pública Estadual. Por exemplo, os itens 1, que estão distribuídos respectivamente nos Lotes I, II e III, tratam sobre firewalls com as mesmas funcionalidades, mas foram concebidos em três diferentes lotes, uma vez que deveriam ser ofertados aos órgãos, equipamentos com diferentes capacidades, no que diz respeito aos tipos, quantidades e throughput de interfaces, número de conexões VPN simultâneas, etc.

12.5. Optou-se por agrupar os três "tamanhos" de firewall em lotes distintos, para que fosse possível aos órgãos participantes escolherem as especificações e capacidades de equipamentos de acordo com suas necessidades, e ao mesmo tempo, garantir a interoperabilidade entre as soluções presentes dentro de cada lote, pois a referida interoperabilidade será fundamental em várias topologias de rede (clusterização e alta disponibilidade, por exemplo), e ainda facilitará o gerenciamento, replicação de regras e atualização dos equipamentos. Além disso, tal escolha deve proporcionar maior competitividade por conta da separação do objeto em lotes distintos, possibilitando que diversos fabricantes participem do certame.

12.6. O modelo de contratação ora pretendido permite a preservação do funcionamento integrado (dentro de cada lote), não comprometendo a funcionalidade de toda a solução, tendo em vista que o fornecimento, a instalação, a configuração, suporte técnico e o treinamento das soluções serão executados pelos fornecedores representantes dos fabricantes em cada um dos lotes. Desta forma, há uma redução do risco de perda, interrupção ou queda do funcionamento da solução e consequente indisponibilidade do serviço de TI, por conta de uma possível divisão de responsabilidades entre diferentes fornecedores.

12.7. Assim, entende-se que é fundamental para a pretensa contratação, e necessário para o alcance dos objetivos técnicos e estratégicos para os quais este projeto foi desenvolvido, que todos os itens ora propostos sejam adquiridos/contratados de forma agrupada, por exemplo, se o órgão participante escolher a solução de firewall do Lote I, ele poderá adicionar outros itens opcionais daquele mesmo lote, porém seria inviável a composição com itens de lotes diferentes.

12.8. Justifica-se, portanto, o agrupamento dos itens da contratação com vista ao melhor aproveitamento das práticas de mercado adotadas pelos fabricantes das soluções e melhor gerenciamento do contrato.

12.9. Conforme Acórdão nº 861/2013 - TCU - Plenário - é lícito os agrupamentos em lotes de itens a serem adquiridos por meio de pregão, desde que possuam mesma natureza e que guardem relação entre si. Tal entendimento corrobora com a solução de TI, objeto da contratação em tela, que sugere essa indivisibilidade dentro de cada lote, em razão da natureza dos itens que a compõem.

12.10. Segundo o Acórdão nº 5.260/2011 – TCU – 1ª câmara, de 06/07/2011, "Inexiste ilegalidade na realização de pregão com previsão de adjudicação por lotes, e não por itens, desde que os lotes sejam integrados por itens de uma mesma natureza e que guardem correlação entre si". Os lotes propostos nesse documento estabelecem três agrupamentos de soluções de mesma natureza, que guardam correlação entre si, seja por similaridade técnica ou de tecnologia, bem como de aplicabilidade em busca de soluções únicas, sem causar qualquer prejuízo à competitividade.

12.11. O agrupamento também encontra amparo na jurisprudência do Tribunal de Contas da União, conforme se observa na Súmula 247 - TCU/2007. "É obrigatória a admissão da adjudicação por item e não por preço global, nos editais das licitações para a contratação de obras, serviços, compras e alienações, cujo objeto seja divisível, desde que não haja prejuízo para o conjunto ou complexo ou perda de economia de escala, tendo em vista o objetivo de propiciar a ampla participação de licitantes que, embora não dispondo de capacidade para a execução, fornecimento ou aquisição da totalidade do objeto, possam fazê-lo com relação a itens ou unidades autônomas, devendo as exigências de habilitação adequar-se a essa divisibilidade." (grifos nossos).

12.12. Em suma, a opção pelo fornecimento por grupos de itens leva em conta a modalidade de contratação pretendida e os benefícios associados. Tal agrupamento não compromete a competitividade do certame, uma vez que várias empresas, que atuam no mercado, apresentam condições para cotar os itens pretendidos para futura contratação, apresentados neste estudo.

13. CONDIÇÕES GERAIS DA CONTRATAÇÃO

13.1. **Modelo de execução do contrato**

13.1.1. Para os 05 de todos os lotes, o regime de execução do é o de empreitada por preço unitário.

13.1.3. Saliente-se que, para os itens 01, 02, 03 e 04 de todos os lotes, enquanto bens de aquisição, a forma de fornecimento é a de entrega imediata e integral.

13.2. **Forma de adjudicação do objeto**

13.2.1. A forma de adjudicação do objeto será **MENOR PREÇO** por lote.

13.2.2. Para se obter o menor preço por lote deverão ser negociados os valores individualizados de cada item que o compõe, buscando também o menor preço unitário, tendo em vista que os itens se encontram agrupados em lotes distintos, meramente em razão da compatibilidade técnica/operacional intrínseca dentro de cada um dos lotes.

13.3. **Dotação orçamentária**

Fica dispensada a indicação de prévia dotação orçamentária no sistema de registro de preços, uma vez que será exigida tão somente quando da efetivação da respectiva contratação.

13.4. **Forma e prazo de pagamento**

13.4.1. O pagamento ocorrerá nas formas abaixo:

a) Para os itens de compra (os de nº 01, 02, 03 e 04 de todos os Lotes) o pagamento é à vista;

b) Para itens de serviço de treinamento (nº 05 de todos os Lotes) o pagamento é à vista, sob demanda.

13.4.2. O CONTRATANTE deverá pagar o preço ao CONTRATADO na conta-corrente de titularidade do CONTRATADO a ser indicada, junto à instituição financeira contratada pelo Estado do Rio de Janeiro.

13.4.3. No caso de o CONTRATADO estar estabelecido em localidade que não possua agência da instituição financeira contratada pelo Estado do Rio de Janeiro ou, caso verificada pelo CONTRATANTE a impossibilidade de o CONTRATADO, em razão de negativa expressa da instituição financeira contratada pelo Estado do Rio de Janeiro, abrir ou manter conta-corrente naquela instituição financeira, o pagamento poderá ser feito mediante crédito em conta-corrente de outra instituição financeira. Nesse caso, eventuais ônus financeiros e/ou contratuais adicionais serão suportados exclusivamente pelo CONTRATADO.

13.4.4. A emissão da Nota Fiscal ou Fatura será precedida do recebimento definitivo do objeto ou de cada parcela, mediante atestação, que não poderá ser realizada pelo ordenador de despesas, conforme disposto neste instrumento e/ou no Termo de Referência, bem ainda no artigo 140, II, alínea "b", da Lei nº 14.133/2021 e arts. 20 e 22, XXIII, do Decreto nº 48817/2023.

13.4.5. Quando houver glosa parcial do objeto, o CONTRATANTE deverá comunicar ao CONTRATADO para que emita Nota Fiscal ou Fatura com o valor exato dimensionado.

13.4.6. O CONTRATADO deverá encaminhar a Nota Fiscal ou Fatura para o endereço indicado pelo CONTRATANTE.

13.4.7. Uma vez recebidos os documentos mencionados neste tópico, o órgão competente deverá realizar consulta ao SICAF para verificar:

a) A manutenção das condições de habilitação exigidas pelo instrumento convocatório;

b) Se o CONTRATADO foi penalizado com as sanções de declaração de inidoneidade ou impedimento de licitar e contratar com o poder público, observadas as abrangências de aplicação; e

c) Eventuais ocorrências impeditivas indiretas, hipótese na qual o gestor deverá verificar se houve fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas.

13.4.8. Constatando-se a situação de irregularidade do CONTRATADO, será providenciada sua notificação, por escrito, para que, no prazo de 15 (quinze) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa e especifique provas que pretende produzir. O prazo poderá ser prorrogado uma vez, por igual período, a critério do CONTRATANTE.

13.4.9. Não havendo regularização ou sendo a defesa considerada improcedente, o CONTRATANTE deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência do CONTRATADO, 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.

13.4.10. Persistindo a irregularidade, o CONTRATANTE deverá adotar as medidas necessárias à rescisão do Contrato nos autos do processo administrativo correspondente, assegurada ao CONTRATADO a ampla defesa.

13.4.11. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do Contrato, caso o CONTRATADO não regularize sua situação, ressalvado o disposto no art. 121, § 3º, da Lei nº 14.133, de 2021, no art. 29 do Decreto nº 48.817, de 2023, e no Termo de Referência.

13.4.12. O pagamento será efetuado no prazo máximo de até 30 (trinta) dias, contados do recebimento da Nota Fiscal ou Fatura.

13.4.13. Havendo erro na apresentação da Nota Fiscal ou Fatura, ou circunstância que impeça a liquidação da despesa, o pagamento ficará sobrestado até que o CONTRATADO providencie as medidas saneadoras. Nessa hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para o CONTRATANTE.

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

13.4.15. Independentemente do percentual de tributo inserido na planilha, no pagamento serão retidos na fonte os percentuais estabelecidos na legislação vigente.

13.4.16. O CONTRATADO regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123/2006, 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 nº 123/2006.

13.4.17. Os pagamentos eventualmente realizados com atraso, desde que não decorram de ato ou fato atribuível ao CONTRATADO, sofrerão a incidência de atualização monetária e juros de mora pelo Índice de Custos de Tecnologia da Informação – ICTI (vide subtópico 13.8.5), calculado pro rata die, e aqueles pagos em prazo inferior ao estabelecido no instrumento convocatório serão feitos mediante desconto de 0,5% (um meio por cento) ao mês, calculado pro rata die.

13.5. **Forma e prazo de fornecimento / entrega**

13.5.1. O cronograma para entrega do objeto, contado em dias úteis, será conforme a tabela abaixo:

Prazo	Marco para contagem do prazo	Atividades	Responsável
1	Publicação do extrato do contrato no Portal Nacional de Compras Públicas - PNCP	Emissão da "Ordem de Fornecimento"	Contratante
15	Publicação do extrato do contrato no PNCP	Realização da Reunião Kick-Off prevista no subtópico 5.7.2. deste documento	Contratante e Contratada
10	Emissão da "Ordem de Fornecimento"	Entrega dos itens de compra (hardware + software + licença padrão)	Contratada
35	Reunião kick-off	Instalação completa da solução de firewall (incluindo configurações, regras, políticas, etc.)	Contratada
20	Emissão da Ordem de Serviço (sob demanda)	Início do treinamento da solução	Contratada
2	Entrega do Relatório de Cumprimento do Objeto previsto no subtópico 13.9.1.1 deste documento	Emissão do Termo de Recebimento Provisório	Contratante
20	Emissão do Termo de Recebimento Provisório	Emissão do Termo de Recebimento Definitivo / autorização para emissão de Nota Fiscal ou fatura, resguardadas as disposições do subtópico 13.9.1.5. deste documento.	Contratante

13.5.2. O objeto em sua totalidade é composto por equipamentos e seus respectivos treinamentos. A entrega dos itens nº 1, 2, 3, 4 de todos os lotes, será através da disponibilização dos equipamentos no ambiente da contratada devidamente instalados e configurados. Já a execução dos itens nº 5 de todos os lotes (cursos de treinamento) acontecerá através do portal de treinamentos da contratada ou que esta venha a viabilizar.

13.6. **Endereço de entrega**

13.6.1. A entrega do objeto, considerados todos os itens de compra componentes dos lotes, bem como eventuais atendimentos presenciais de suporte técnico, será realizada no endereço indicado pela Contratante.

13.6.2. No caso do PRODERJ, a entrega ocorrerá em um dos três endereços mencionados no tópico 14.2.4. deste documento.

13.6.3. O acesso de representante da CONTRATADA nas dependências da CONTRATANTE, deverá ocorrer mediante prévia comunicação entre as partes, por meio dos mecanismos de comunicação definidos neste instrumento.

13.6.4. A entrega dos serviços de treinamento ocorrerá conforme as disposições do subtópico 5.2. (Requisitos de Capacitação) deste documento.

13.7. **Vigência contratual (minuta padrão PGE)**

13.7.1. O prazo de vigência será de:

a) 180 (cento e oitenta) dias para os itens de compra (os de nº 01, 02, 03 e 04 dos Lotes), contados da data da divulgação no Portal Nacional de Contratações Públicas, vedada a prorrogação.

b) 12 (doze) meses para os itens de serviço de treinamento (nº 05 dos Lotes), contados da data da divulgação no Portal Nacional de Contratações Públicas, vedada a prorrogação, salvo quando obrigatória nos termos da Lei nº 14.133/2021.

13.8. **Reajuste de preços**

13.8.1. Os preços contratados serão reajustados após o interregno de 1 (um) ano, mediante solicitação do CONTRATADO.

13.8.2. O interregno mínimo de 1 (um) para o primeiro reajuste será contado da data do orçamento estimado.

13.8.3. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir do fato gerador que deu ensejo ao último reajuste.

13.8.4. Os preços iniciais serão reajustados, mediante a aplicação, pela CONTRATANTE, do Índice de Custos de Tecnologia da Informação – ICTI, mantido pela Fundação Instituto de Pesquisa Econômica Aplicada - IPEA.

13.8.5. No caso de atraso ou não divulgação do(s) índice(s) de reajustamento, a CONTRATANTE pagará ao CONTRATADO a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja(m) divulgado(s) o(s) índice(s) definitivo(s).

13.8.6. Fica o CONTRATADO obrigado a apresentar memória de cálculo referente ao reajustamento de preços do valor remanescente, sempre que este ocorrer, sendo adotado na aferição final o índice definitivo.

13.8.7. Caso o índice estabelecido para o reajustamento venha a ser extinto ou de qualquer forma não possa mais ser utilizado, será(ão) adotado(s), em substituição, o(s) que vier(em) a ser determinado(s) pela legislação então em vigor.

13.8.8. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.

13.8.9. O pedido de reajuste deverá ser formulado durante a vigência do contrato e antes de eventual prorrogação contratual, sob pena de preclusão.

13.8.10. Os efeitos financeiros do pedido de reajuste serão contados:

a) da data-base prevista no contrato, desde que requerido o reajuste no prazo de 60 (sessenta) dias da data de publicação do índice ajustado contratualmente;

c) a partir da data do requerimento do CONTRATADO, caso o pedido seja formulado após o prazo fixado na alínea a, acima, o que não acarretará a alteração do marco para cômputo da anualidade do reajustamento, já adotado no edital e no contrato.

13.8.11. Caso, na data de eventual prorrogação contratual, ainda não tenha sido divulgado o índice de reajuste, deverá, a requerimento do CONTRATADO, ser inserida cláusula no termo aditivo de prorrogação para resguardar o direito futuro do CONTRATADO, a ser exercido tão logo se disponha dos valores reajustados, sob pena de preclusão.

13.8.12. A extinção do contrato não configurará óbice para o deferimento do reajuste solicitado tempestivamente, hipótese em que será concedido por meio de termo indenizatório.

13.8.13. O reajuste será realizado por apostilamento, se esta for a única alteração contratual a ser realizada.

13.8.14. O reajuste de preços não interfere no direito das partes de solicitar, a qualquer momento, a manutenção do equilíbrio econômico dos contratos com base no disposto no art. 124, inciso II, alínea "d", da Lei n.º 14.133/2021.

13.9. **Critérios de recebimento e aceitação do objeto**

13.9.1. O **recebimento provisório** do objeto, nos termos do art. 140, incisos I e II da Lei Federal nº 14.133/21, será realizado pela Comissão de Fiscalização do Contrato da CONTRATANTE na forma abaixo indicada:

I - Para os bens de aquisição (itens 1 a 4 dos Lotes 1, 2 e 3) o recebimento é sumário;

II - Para os serviços de treinamento (item 5 dos Lotes 1, 2 e 3) o recebimento ocorrerá mediante termo, no prazo máximo de 2 (dois) dias úteis;

III - Para todos os itens previstos nos lotes do objeto, a CONTRATADA deverá no ato de entrega provisória dos bens e/ou serviços contratados, entregar Relatório de Cumprimento do Objeto na forma do modelo constante do Anexo VI deste documento, o qual deverá acompanhar ainda:

a) Para os bens previstos nos itens 1 de cada lote: dados para acionamento dos serviços de suporte ou garantia, documentos oficiais do fabricante e documentação do produto (manuais, prospectos etc..);

b) Para bens previstos nos itens 2, 3 e 4 de todos os lotes: documentação que comprove o licenciamento das soluções contratadas, tais como número de séries, chaves, dados para acionamento dos serviços de suporte, documentos oficiais do fabricante e documentação do produto e disponibilização das soluções;

c) Para os serviços de treinamento previstos nos itens 5 de todos os lotes: certificados dos alunos treinados.

13.9.1.1. A CONTRATADA deverá elaborar um Relatório de Cumprimento do Objeto (modelo no Anexo VI deste documento) a ser entregue à Comissão de Fiscalização de Contrato quando da entrega do bem ou serviço, para a análise antes da emissão do Termo de Recebimento Provisório. No caso dos itens de compra (itens 1, 2, 3 e 4 de todos os lotes) o relatório deverá ser entregue no momento do recebimento sumário correspondente ao momento da efetiva entrega dos bens.O relatório deve contemplar todas as etapas e procedimentos realizados, eventuais problemas verificados e qualquer fato relevante sobre a execução do objeto contratual (bens e serviços). O relatório deverá estar acompanhado, conforme item ou etapa entregue, das seguintes informações e/ou documentos:

a) Para os itens 1 de todos os lotes: dados para acionamento dos serviços de suporte ou garantia, documentos oficiais do fabricante e documentação do produto (manuais, prospectos etc..);

b) Para os itens 2, 3 e 4 de todos os lotes: documentação que comprove o licenciamento das soluções contratadas, tais como número de séries, chaves, dados para acionamento dos serviços de suporte, documentos oficiais do fabricante e documentação do produto e disponibilização das soluções;

c) Para os itens 5 de todos os lotes: certificados dos alunos treinados.

13.9.1.2. Após a emissão do Termo de Recebimento Provisório, a CONTRATANTE, por meio de sua Comissão de Fiscalização de Contrato, analisará a documentação entregue e poderá fazer inspeções ou promover diligências internas quanto às etapas executadas para a entrega do objeto (bens e serviços), com a finalidade de verificar a adequação no cumprimento do objeto (bens e serviços) pela contratada, bem como verificar a necessidade de arremates, retoques e revisões finais que eventualmente se fizerem necessários.

13.9.1.3. A CONTRATADA fica obrigada a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas o objeto (bens e serviços) em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados, cabendo à fiscalização não proceder ao Termo de Recebimento Definitivo até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas na fase do recebimento provisório.

13.9.1.4. Recebidos provisoriamente os bens e/ou serviços, a Comissão de Fiscalização do Contrato avaliará as características de cada item, identificando eventuais problemas.

13.9.1.5. Os bens e/ou serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, devendo ser substituídos no prazo de XX (XXXX) dias, a contar da notificação da CONTRATADA, às suas custas, sem prejuízo da aplicação das penalidades.

13.9.1.6. Se, após o recebimento provisório, constatar-se que o objeto foi executado em desacordo com o especificado, com defeito ou incompleto, a Comissão de Fiscalização do Contrato notificará por escrito a CONTRATADA, interrompendo-se os prazos de recebimento e pagamento até que sanada a irregularidade.

13.9.1.7. Estando em conformidade, será efetuado o recebimento definitivo.

13.9.2. O **recebimento definitivo** do objeto será efetuado pela Comissão de Fiscalização do Contrato, nos termos do art.140, incisos I e II da Lei Federal nº 14.133/2021, no prazo máximo de 20 (vinte) dias úteis, depois de verificada a conformidade das quantidades e especificações com aquelas contratadas e consignadas no Termo de Referência.

13.9.2.1. Com o recebimento definitivo, que concretiza o ateste do cumprimento do objeto (bens e serviços) contratado, a CONTRATANTE comunicará à CONTRATADA para que, em até 5 dias, emita a Nota Fiscal ou Fatura.

13.9.2.2. A Comissão de Fiscalização de Contrato, sob pena de responsabilidade administrativa, anotará em registro próprio as ocorrências relativas à execução do contrato, determinando o que for necessário à regularização das faltas ou defeitos observados. No que exceder à sua competência, comunicará o fato à autoridade superior, em 10 (dez) dias, para ratificação.

13.9.2.3. A CONTRATADA declarará, antecipadamente, aceitar todas as condições, métodos e processos de inspeção, verificação e controle adotados pela fiscalização, obrigando-se a lhes fornecer todos os dados, elementos, explicações, esclarecimentos e comunicações de que este necessitar e que forem julgados necessários ao desempenho de suas atividades.

13.9.2.4. A instituição e a atuação da fiscalização do objeto (bens e serviços) do contrato não exclui ou atenua a responsabilidade da CONTRATADA, nem a exime de manter fiscalização própria.

13.10. **Participação de empresas em regime de consórcio (minuta padrão PGE)**

13.10.1. É vedada a participação de pessoas jurídicas reunidas em consórcio.

13.10.2. A vedação se dá em razão das características específicas da solução a ser contratada, que não pressupõe multiplicidade ou heterogeneidade de atividades empresariais distintas, nem envolve questões de alta complexidade ou de relevante vulto, em que empresas, isoladamente, não teriam condições de suprir os requisitos de habilitação do edital.

13.10.3. Entende-se que os itens a serem contratados não exigem empresas de diferentes segmentos e/ou capacidades reunidas para atuarem na execução do objeto proposto.

13.10.4. Ademais, a gestão compartilhada poderá gerar vícios ou lacunas no fluxo dos processos de atendimento. A cadeia de responsabilidades entre as empresas será maior que se o objeto estiver sob responsabilidade de uma única empresa, ainda que operacionalizado por meio de atuação conjunta com outras empresas.

13.10.5. Mesmo a garantia produzida como consequência da aquisição é resultado de equipes, técnicas e procedimento complementar, não havendo benefício ou necessidade de segmentação para a realização do objeto proposto, além de repercutir em vários canais de atendimento de eventuais chamados técnicos, gerando uma morosidade no atendimento e ocasionando o não cumprimento dos itens expostos no edital.

13.10.6. A ausência de consórcio não trará prejuízos à competitividade do certame, visto que, em regra, a formação de consórcios é admitida quando o objeto a ser licitado envolve questões de alta complexidade ou de relevante vulto, em que empresas, isoladamente, não teriam condições de suprir os requisitos de habilitação do edital. Nestes casos, a Administração, com vistas a aumentar o número de participantes, admite a formação de consórcio.

13.10.7. Tendo em vista que é prerrogativa do Poder Público, na condição de CONTRATANTE, a escolha da participação ou não de empresas constituídas sob a forma de consórcio, com as devidas justificativas, conforme a literalidade do texto da Lei nº o 14.133, art 15 e seus incisos e parágrafos, pelos motivos já expostos, conclui-se que a vedação de constituição de empresas em consórcio, para o caso concreto, é o que melhor atende o interesse público, por prestigiar os princípios da competitividade, economicidade e moralidade.

13.10.8. Por fim, a vedação da participação de empresas reunidas em regime de consórcio visa exatamente afastar a restrição à competição, na medida em que a reunião de empresas que, individualmente, poderiam fornecer os equipamentos, reduziria o número de licitantes e poderia, eventualmente, proporcionar a formação de conluios/cartéis para manipular os preços nas licitações.

13.11. **Possibilidade de participação de cooperativas**

Não será admitida a participação de cooperativa de trabalho, qualquer que seja a sua forma de constituição, já que o objeto principal trata de compra de bens de aquisição perpétua e, no caso dos itens secundários de treinamento, há vínculo de subordinação direta entre o empregado e a empresa contratada para a prestação dos serviços.

13.12. **Análise da possibilidade de subcontratação**

13.13. Não será admitida a subcontratação, sub-rogação, cessão ou transferência no todo ou em parte, em razão da composição do objeto, distribuído em lotes compostos por itens de aquisição perpétua, de natureza indivisível.

13.14. Saliente-se que, em caso do item de treinamento ser ministrado pelo mesmo fabricante da solução ofertada pela contratada ou com uso de sua plataforma, isso não configura subcontratação, sub-rogação, cessão ou transferência, uma vez que compõe a mesma solução a mesma.

13.15. **Exigência de garantia contratual**

13.15.1. O Contrato conta com garantia de execução, nos moldes do artigo 96 da Lei nº 14.133/2021, correspondente a 5% (cinco por cento) de seu valor anual.

13.15.3. O referido percentual, resguardada a discricionariedade prevista no acima citado art. 96, caput e o teto estabelecido no caput do art. 98 do mesmo diploma legal, considera a natureza do objeto (bens e serviços), enquanto ferramenta estratégica de caráter tecnológico de relevância para as atividades do órgão contratante em razão das exigências trazidas pela nova legislação quanto ao tratamento de dados pessoais.

13.16.4. O CONTRATADO poderá optar pelas seguintes modalidades de garantia:

a) caução em dinheiro ou em títulos da dívida pública;

c) seguro-garantia;

e) fiança bancária; e

g) título de capitalização custeado por pagamento único, com resgate pelo valor total.

13.16.6. Caso o prazo de vigência do contrato seja inferior a um ano, a garantia aqui prevista será calculada sobre o valor total do Contrato.

13.16.7. A garantia, qualquer que seja a modalidade apresentada pelo vencedor do certame, deverá contemplar a cobertura para os seguintes eventos:

a) Prejuízos advindos do não cumprimento do contrato;

c) Multas punitivas aplicadas pela fiscalização à contratada;

e) Prejuízos diretos causados à CONTRATANTE decorrentes de culpa ou dolo durante a execução do contrato;

g) Obrigações previdenciárias e trabalhistas não honradas pela Contratada.

13.17.8. Caso o valor do contrato seja alterado, de acordo com o art. 124 da Lei Federal n.º 14.133/2021 a garantia deverá ser complementada, no prazo de 72 horas, para que seja mantido o percentual de 5 % do valor do Contrato.

13.17.9. Nos casos em que valores de multa venham a ser descontados da garantia, seu valor original será recomposto no prazo de 72 horas, sob pena de rescisão administrativa do contrato.

13.18.10. Demais termos relacionados a garantia contratual serão previstos no edital e no contrato.

13.19. **Qualificação Técnica**

13.19.1. Para fins de comprovação de qualificação técnica deverão ser apresentados Atestado(s) fornecido(s) por pessoas jurídicas de direito público ou privado, que comprovem a experiência e aptidão de desempenho de atividade pertinente e compatível com o objeto da licitação, na forma do artigo 67, § 2º, da Lei Federal nº 14.133/2021 que indiquem nome, função, endereço de contato do(s) atestador(es), ou qualquer outro meio para eventual contato pelo órgão licitante.

13.19.2. Um único atestado é suficiente para a demonstração da experiência anterior do licitante em relação a execução do objeto licitado, sendo possível o somatório de atestados de períodos concomitantes para comprovar a sua capacidade técnica.

13.19.3. O(s) atestado(s) deverão demonstrar o cumprimento de um quantitativo mínimo de 30% (trinta por cento) do volume estimado para os itens: 1 de todos os lotes, os quais correspondem às respectivas parcelas de maior relevância ou de valor significativo para o objeto deste certame.

13.19.4. A motivação para os itens necessários à comprovação de aptidão técnica, bem como o percentual acima referido, se dá em virtude realização do certame via Sistema de Registro de Preços com demanda em larga escala, para atendimento de inúmeros órgãos da Administração. Portanto, se faz razoável a verificação de que o futuro prestador do serviço tem capacidade de atendimento compatível com a criticidade do projeto, mitigando riscos à disponibilidade dos serviços do Governo, bem como diante da importância do objeto a ser contratado, que tem relação direta com a segurança institucional dos órgãos e secretarias do estado.

14. PROVA DE CONCEITO

14.1. **Objetivo**

Será exigido do LICITANTE classificado em primeiro lugar Prova de Conceito para a demonstração de que a solução ofertada é compatível com as exigências técnicas necessárias e prescritas para este objeto (itens de compra), conforme os roteiro apresentados nos Anexos II, III e IV deste documento, respectivamente correspondentes aos lotes 1, 2 e 3.

14.2. **Prazos e condições**

14.2.1. O referido LICITANTE será convocado no prazo máximo de até 10 (dez) dias úteis, a contar da aprovação da sua documentação de habilitação, para uma reunião (que poderá ocorrer em plataforma virtual), onde serão definidas as providências preparatórias do ambiente de teste. Nessa reunião o LICITANTE deverá informar os requisitos necessários para a instalação do ambiente de teste a serem disponibilizados pelo PRODERJ conforme entendimento durante a reunião. Entende-se por "requisitos necessários":

a) Disponibilização de máquinas virtuais e/ou estações de trabalho, projetor e link de internet;

b) Criação de VLAN's e/ou disponibilização de endereços IP;

c) Criação de usuários no AD e/ou modificações de regras de firewall, IPS, etc;

d) Disponibilização de periféricos, tais como: cabos, switches e outros componentes semelhantes não mencionados.

14.2.2. Nesta reunião o LICITANTE deverá, sob pena de desclassificação, entregar os documentos da(s) solução(ões) que permitam comprovar o atendimento aos requisitos técnicos constantes do Anexo I deste documento, apresentando no mínimo:

a) ID do requisito;

b) Descrição do requisito;

c) Nome do produto ofertado (modelo, marca e fabricante);

d) Nome do documento de referência onde é possível verificar evidência do atendimento do requisito;

e) Página do documento referência onde é possível verificar evidência do atendimento do requisito;

f) Outras informações necessárias.

14.2.3. Até o prazo de 5 dias úteis após a realização da reunião preparatória, será divulgada a equipe técnica que avaliará a solução durante a sessão da prova.

14.2.4. O teste será realizado no ambiente do PRODERJ, em um dos endereços abaixo mencionados a ser definido na reunião acima preparatória acima referida:

a) Data Center – Universidade do Estado do Rio de Janeiro (UERJ). End.: R. São Francisco Xavier 524, 2º andar, bloco "F", Maracanã, Rio de Janeiro – RJ, CEP: 20550-013;

b) Data Center – Centro Integrado de Comando e Controle (CICC). End.: Rua Carmo Neto s/nº, Cidade Nova, Rio de Janeiro – RJ - CEP 20210-051; ou

c) Sede – Centro de Tecnologia da Informação e Comunicação do Governo do Estado do Rio de Janeiro (PRODERJ). End.: R. da Conceição 69, 24º e 25º andar, Centro, Rio de Janeiro – RJ CEP 20051-011

14.2.5. Admite-se, alternativamente, o uso de ambiente virtual do próprio LICITANTE ou do fabricante, para a comprovação das funcionalidades da solução ofertada, caso seja acordado na reunião preparatória. Nesta hipótese, o LICITANTE deverá disponibilizar o link de acesso ao acompanhamento da sessão virtual de demonstração até 3 (três) dias úteis antes da realização da sessão, para que o mesmo possa ser repassado em tempo hábil a todos os que acompanharão a sessão.

14.2.6. Em caso de não comparecimento à reunião (por problema único e exclusivo do LICITANTE) a prova acontecerá no ambiente padrão de teste do PRODERJ, em um dos endereços acima citados, sendo vedado ao LICITANTE reivindicar qualquer adaptação na infraestrutura oferecida.

14.2.7. O PRODERJ, por meio da Comissão Permanente de Licitação (Pregoeiro), dará publicidade, através do chat de mensagens do SIGA-RJ, da data de realização do teste que deverá ocorrer no prazo de 10 (dez) dias úteis após a realização da reunião preparatória. O referido prazo poderá ser prorrogado por igual período, mediante requisição fundamentada do LICITANTE.

14.2.8. Se o teste for realizado em ambiente do PRODERJ, o LICITANTE terá até as 17h do último dia útil anterior ao da realização do mesmo para providenciar a instalação do ambiente nas condições definidas na reunião.

14.2.9. A prova será realizada entre 10:00 e 18:00 horas (horário de Brasília), com intervalo de 1 hora para almoço, e poderá durar de 1 a 5 dias úteis.

14.3. **Possibilidade e forma de participação dos interessados**

Os outros licitantes que tenham participado da etapa competitiva e demais interessados que desejem acompanhar a sessão, poderão indicar um representante para acompanhamento, devendo para tanto enviar para o e-mail da Comissão Permanente de Licitação (cdl@proderj.rj.gov.br) até as 16hs do último dia útil que antecede a sessão de teste. No e-mail deverão constar: dados da empresa interessada (nome e contato), de seu representante (nome e contato) para o devido credenciamento.

14.4. **Roteiro e critérios de avaliação**

14.4.1. No dia de realização do teste, o LICITANTE, bem como os demais interessados em acompanhar, deverão chegar ao local indicado com antecedência mínima de 30 minutos.

14.4.2. A equipe técnica do PRODERJ considerará apto o sistema que atender aos requisitos conforme descritos no respectivo Roteiro para Prova de Conceito (Anexos II, III e IV), do futuro Termo de Referência, onde cada item deverá ser preenchido, observados os critérios "atende" ou "não atende".

14.4.3. Durante a prova poderá ser feito questionamento, exclusivamente pelos representantes do PRODERJ à proponente, permitindo a verificação dos requisitos estabelecidos.

14.4.4. Após a prova será emitido, via Sistema Eletrônico de Informações, relatório descrevendo os testes realizados e a conclusão sobre a aprovação da proposta ou desclassificação bem como eventuais ocorrências ou manifestações de quaisquer dos presentes na sessão.

14.4.5. Para a solução ser considerada apta para ser contratada pela Administração, todos os requisitos de software que constam no presente estudo e seu anexo de especificações técnicas, deverão ser considerados ATENDIDOS.

14.4.6. Será desclassificada a licitante que for convocada para a prova de conceito e não demonstrar a compatibilidade de seu produto conforme as especificações técnicas exigidas ou não comparecer no dia marcado sob qualquer pretexto.

14.4.7. Em caso de desclassificação na prova de conceito deverá ser convocada o próximo licitante na ordem de classificação, resguardadas todas as condições e prazos previstos neste tópico.

14.5. **Responsabilidades**

14.5.1. Os custos para a demonstração da solução são de responsabilidade do LICITANTE e em hipótese alguma caberá qualquer tipo de indenização.

14.5.2. O LICITANTE deverá disponibilizar ao menos 01 (um) técnico que se responsabilizará pela instalação do software da solução, caso o teste seja realizado utilizando a infraestrutura do PRODERJ.

14.5.3. A disponibilização de equipamentos, sistemas, demais materiais e/ou acessórios necessários ao ambiente de demonstração durante a prova não informados pelo LICITANTE na reunião preparatória citada no subtópico 14.2.1 são de inteira responsabilidade do LICITANTE.

14.5.4. Ficará sob responsabilidade do PRODERJ o resguardo dos itens eventualmente entregues pelo licitante para a avaliação na prova de conceito, devendo restituí-los ao final nas condições recebidas, resguardados eventuais consumos decorrentes da realização da prova.

15. ANÁLISE DE RISCO DE SOBREPOSIÇÃO DO OBJETO

Observado o quanto informado no tópico 3 (contratações correlatas), não há risco de sobreposição.

16. DA TRANSIÇÃO E DO ENCERRAMENTO DO CONTRATO

Não se aplica, uma vez que se trata de contratação de compra e não há transição entre fornecedores.

17. ESTRATÉGIA DE INDEPENDÊNCIA EM RELAÇÃO À CONTRATADA / PLANO DE SUSTENTAÇÃO

17.1. O contrato é de compra de solução tecnológica contemplando curso de capacitação para a operacionalização da ferramenta, viabilizando transferência de conhecimento. Não se aplica o risco de rescisão ou interrupção antecipada no funcionamento dos produtos. Portanto, não se aplica a existência de um plano de sustentação.

17.3. A substituição de um firewall em uso por outro equipamento novo requer alguma antecipação, planejamento logístico, adaptação de regras e validação por testes, ou seja, não é uma operação simples, ainda que bastante usual. Via de regra, a Contratante deve certificar-se de que o novo equipamento esteja pronto para substituir o antigo.

18. POSICIONAMENTO CONCLUSIVO

18.1. O presente Estudo Técnico Preliminar (ETP), bem como os seus anexos, consideram a necessidade de contratação do objeto (bens e serviços), os requisitos técnicos, legais, ambientais e os do próprio negócio, o mercado em que o objeto se encontra inserido, bem como os demais requisitos necessários para a caracterização e quantificação da demanda identificada, bem como o processo de escolha da solução que melhor se adequa à Instituição nesta oportunidade. São considerados ainda os requisitos ambientais e os aspectos legais, cabendo ressaltar que os riscos envolvidos são administráveis e os custos previstos são compatíveis e se caracterizam pela economicidade.

18.2. Desta forma, entende-se ser VIÁVEL a contratação em comento, e, visando dar início à implementação do objeto aqui delineado, recomenda-se a elaboração de Termo de Referência com base no presente estudo e o encaminhamento para o setor competente para o prosseguimento do feito.

19. ANEXOS

Abaixo, estão listados os documentos anexos cujas disposições estão em plena concordância com este documento principal do qual correspondem a parte integrante e indissociável:

I - Especificações Técnicas do Objeto (75937120);
II - Roteiro para Prova de Conceito - Firewall Tipo 1 (75935971);
III - Roteiro para Prova de Conceito - Firewall Tipo 2 (75936978);
IV - Roteiro para Prova de Conceito - Firewall Tipo 3 (75936561);
V - Mapa de Riscos (75942352);
VI - Modelo de Relatório de Cumprimento do Objeto (75942000);
VII - Orientação para preenchimento da Intenção no Registro de Preços - IRP (75942064).

20. CLASSIFICAÇÃO DESTE DOCUMENTO QUANTO AO GRAU E PRAZO DE SIGILO

Observadas as disposições da Lei Federal nº 12.527/2011 e do Decreto Estadual nº 46.475/2018, que tratam do direito e das restrições de acesso às informações sob guarda do poder público, fica registrado que o presente documento, assim como os seus anexos, são de acesso PÚBLICO.

21. ASSINATURA DOS MEMBROS DA EQUIPE RESPONSÁVEL PELO ESTUDO

Manuelito de Sousa Reis Junior Responsável pela demanda Gerente de Riscos e Ameaças ID nº 4406953-7	Isabela Rebouças Costa Analista de Sistemas ID nº 4349659-8	Rosana Alves de Andrade Analista de Sistemas Gerente de Proteção de Dados e Sistemas ID nº 4347470-5	Fabio Ivo Analista de Rede / Telecom ID nº 5143032-0	Charles Monteiro Guimarães Diretor de Patrimônio e Logística ID nº 4432892-3

Rio de Janeiro, 04 de junho de 2024

Documento assinado eletronicamente por **Isabela Rebouças Costa**, **Analista de Sistemas**, em 06/06/2024, às 16:04, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Manuelito de Sousa Reis Junior**, **Gerente**, em 06/06/2024, às 16:23, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Monique Goncalves Paz**, **Diretora**, em 06/06/2024, às 16:28, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Rosana Alves de Andrade**, **Analista de Sistemas**, em 06/06/2024, às 16:52, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Charles Monteiro Guimarães**, **Diretor**, em 06/06/2024, às 17:22, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Fabio Ivo**, **Assistente**, em 06/06/2024, às 17:24, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Cristina da Silva Barros Drongitis**, **Assessora Chefe**, em 26/08/2024, às 12:51, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

A autenticidade deste documento pode ser conferida no site http://sei.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **75936299** e o código CRC **DC439813**.

Rua da Conceição, 69, 24º Andar / 25º Andar - Bairro Centro, Rio de Janeiro/RJ, CEP 20051-011
Telefone:

ANEXO I DO ESTUDO TÉCNICO PRELIMINAR

ESPECIFICAÇÕES TÉCNICAS DO OBJETO

1. OBJETO

I - Os lotes com os itens componentes do objeto se encontram descritos na tabela do subtópico 7.5. do Estudo Técnico Preliminar.

II - Este anexo deve ser interpretado conforme as disposições do Estudo Técnico Preliminar (75936299) do qual é parte integrante e indissociável.

1.1. Características Gerais das Soluções de Firewall dos Lotes 1, 2 e 3

1.1.1. Arquitetura

1.1.1.1. As soluções de Firewall presentes nos Lotes 1, 2 e 3 do objeto são compostas por equipamentos do tipo appliance, o software complementar para gerenciamento, logs e relatórios, bem como os treinamentos operacionais para as distintas soluções presentes nos Lotes 1, 2 e 3.

1.1.1.2. O firewall gerenciado, especificado no Lote 1, deve ser capaz de encaminhar pacotes para serem analisados por um sistema e/ou equipamento concentrador.

1.1.1.3. O firewall gerenciado, especificado no Lote 2, deve ser capaz de encaminhar pacotes para serem analisados por um sistema e/ou equipamento concentrador.

1.1.1.4. O firewall gerenciado, especificado no Lote 3, deve ser capaz de encaminhar pacotes para serem analisados por um sistema e/ou equipamento concentrador.

1.1.2. Licenciamento

1.1.2.1. **Licença Padrão**

I - Entende-se por Licença Padrão a licença de uso do fabricante em caráter permanente e perpétuo para todas as funcionalidades e quantidades mencionadas neste documento, com exceção aos itens relacionados à Atualização de Assinaturas de Proteção.

II - Entende-se por Atualização de Assinaturas de Proteção todas as funcionalidades, manuais ou automatizadas, necessárias para manter a solução em seu nível de identificação e proteção mais atualizado, tais como: atualização de assinaturas de prevenção de intrusão, assinaturas de identificação de vírus, assinaturas de identificação de aplicações, listas de classificação de URLs, listas de geolocalização, listas de endereços IPs utilizados por botnets, listas de endereços IPs de reputação duvidosa etc.

III - Todos os equipamentos firewall devem possuir esta licença ativada.

1.1.2.2. **Licença de Atualização de Segurança**

I - Entende-se por Licença de Atualização de Segurança a licença de uso do fabricante que permita a utilização das funcionalidades e quantidades mencionadas neste documento para os itens relacionados à Atualização de Assinaturas de Proteção (subtópico 1.1.2.1.).

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

III - As Licenças de Atualização de Segurança devem ter prazo de vigência de 60 (sessenta) meses, contados a partir da aplicação destas nos produtos.

1.1.3. Hardware

1.1.3.1. Deve ser fornecido em formato appliance físico.

1.1.3.2. Deve ser novo, sem uso, entregue em perfeito estado de funcionamento, sem marcas, amassados, arranhões ou outros problemas físicos, acondicionados em suas embalagens originais.

1.1.3.3. Nenhum dos equipamentos fornecidos pode estar em modo End of Life, End of Sale e End of Support no dia do Pregão Eletrônico.

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

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

1.1.3.6. Deve possuir, no mínimo, 1 (uma) interface Ethernet dedicada para gerenciamento.

1.1.3.7. O plano de gerenciamento da solução deve ser apartado do plano de dados, com recursos de CPU, memória e interface de rede dedicados para esta função;

1.1.3.8. Deve ser fornecido em sua capacidade máxima de processamento, memória e armazenamento interno.

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

1.1.4. Funcionalidades Básicas

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

1.1.4.2. Deve suportar o envio de notificações via e-mail, SNMP traps e mensagens de log.

1.1.4.3. Deve permitir o acesso ao equipamento via SSH e interface web HTTPS.

1.1.4.4. A comunicação entre a estação de trabalho do administrador e o firewall deve ser autenticada e criptografada.

1.1.4.5. Deve informar a utilização dos recursos de CPU, memória e atividade de rede.

1.1.4.6. 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.

1.1.4.7. Deve possuir a funcionalidade de exportação automática dos logs para servidor syslog e para a solução de gerenciamento de logs.

1.1.4.8. Desejável possuir plano de gerenciamento segregado do plano de dados, inclusive com CPU e interfaces dedicadas.

1.1.4.9. Deve permitir a importação, criação e edição de regras SNORT.

1.1.4.10. Os Firewalls de segurança físico ou virtualizados, devem possuir processamento dedicado no equipamento de segurança para funções e ações de Gerenciamento, mesmo que o equipamento esteja com alto processamento de CPU. Assim evitando a falta de acesso do administrador para qualquer mitigação de problema e aplicação de política para solução de problemas. Entre as funções, deve suportar no mínimo: acesso SSH, acesso WEB, alterações de política, comunicação SNMP; 1.6. Console de Gerenciamento centralizado.

1.1.4.11. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7.

1.1.5. **Rede**

1.1.5.1. Deve suportar os protocolos IPv4 e IPv6.

1.1.5.2. Deve suportar VLAN no padrão 802.1q.

1.1.5.3. Deve suportar Jumbo Frames.

1.1.5.4. Deve suportar sub interfaces Ethernet lógicas.

1.1.5.5. Deve suportar o protocolo NTP.

1.1.5.6. Deve implementar mecanismo de conversão de endereços NAT (Network Address Translation), de forma a possibilitar a realização de NAT estático (1-1), dinâmico (N-1), NAT pool (N-N) e NAT condicional (possibilitando que um endereço tenha mais de um NAT dependendo da origem, destino ou porta).

1.1.5.7. Deve permitir o registro de eventos de NAT com as informações de endereço interno, endereço público, data e hora do evento, portas de origem e destino.

1.1.5.8. Deve suportar tradução de porta (PAT).

1.1.5.9. Deve suportar as funcionalidades de roteamento estático e dinâmico em IPv4 e IPv6.

1.1.5.10. Deve suportar os protocolos RIP, OSPF v2, OSPF v3 e BGP v4.

1.1.5.11. Deve suportar os protocolos IGMP v2, IGMP v3, PIM-SM.

1.1.5.12. Deve suportar Virtual Routing Redundancy Protocol (VRRP) ou equivalente.

1.1.5.13. Deve suportar os protocolos SNMP v2 e SNMP v3.

1.1.5.14. Deve permitir monitorar, via SNMP, falhas de hardware, uso de recursos por número elevado de sessões, número de túneis estabelecidos na VPN, CPU, memória, status do cluster de Alta Disponibilidade e estatísticas de uso das interfaces de rede.

1.1.5.15. Deve suportar Policy Based Routing (PBR), possibilitando políticas de roteamento condicionado ao endereço IP de origem, endereço IP de destino e porta de comunicação.

1.1.5.16. Deve suportar no mínimo as seguintes funcionalidades em IPv6: SLAAC (address auto configuration), NAT64, Identificação de usuários a partir do LDAP/AD, Captive Portal, IPv6 over IPv4 IPSec, Regras de proteção contra DoS (Denial of Service), De-criptografia SSL e SSH, PBF (Policy Based Forwarding), QoS, DHCPv6 Relay, IPSEc, Ativo/Ativo, Ativo/Passivo, SNMP, NTP, SYSLOG, DNS, Neighbor Discovery (ND), Recursive DNS Server (RDNSS).

1.1.6. **Autenticação e Identificação de Usuários**

1.1.6.1. Deve promover a integração com serviços de diretório LDAP e Active Directory, baseados em caracteres da língua portuguesa, para a identificação, autenticação, autorização e registro de eventos de acessos ou ameaças.

1.1.6.2. Deve identificar de forma transparente os usuários autenticados por meio de serviço de diretório LDAP ou Active Directory.

1.1.6.3. Não será permitida a utilização de agentes instalados nos servidores LDAP, Active Directory, proxies internos e equipamentos dos usuários, nem configuração adicional no navegador.

1.1.6.4. Não será permitida a interceptação ou espelhamento do tráfego destinado aos servidores LDAP, Active Directory e proxies internos.

1.1.6.5. Deve possuir portal de autenticação (captive portal) para a identificação e autenticação de usuários não registrados ou não reconhecidos.

1.1.6.6. O portal de autenticação deve ser capaz de identificar e autenticar usuários cadastrados em serviço de diretório LDAP e Active Directory.

1.1.6.7. Deve permitir a criação de políticas de segurança baseadas em usuários e grupos de usuários pertencentes a um diretório LDAP ou ao Active Directory.

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

1.1.6.9. Deve registrar os eventos dos usuários em tempo real, sem a utilização de processos em lote (batches) ou processos de correlação após a ocorrência do evento em questão.

1.1.6.10. 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.

1.1.6.11. Desejável possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em servidores acessados remotamente, mesmo que não sejam servidores Windows.

1.1.6.12. Desejável identificar usuários através de leitura do campo x-fowarded-for, populando nos logs do firewall o endereço IP, bem como o usuário de rede responsável pelo acesso.

1.1.7. **Geolocalização**

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

1.1.7.2. Deve identificar, no mínimo, 180 países.

1.1.7.3. Deve armazenar as listas de geolocalização no próprio equipamento.

1.1.7.4. 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.

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

1.1.8. **VPN**

1.1.8.1. Deve suportar VPN site-to-site em topologia Full Meshed (todos os gateways possuem links específicos para todos os demais gateways) e Estrela (gateways satélites se comunicam somente com um único gateway central).

1.1.8.2. Deve suportar criptografia 3DES, AES-128, AES-256.

1.1.8.3. Deve suportar integridade de dados com MD5, SHA-1 e SHA-256.

1.1.8.4. Deve suportar o protocolo IKE, fases I e II.

1.1.8.5. Deve suportar os algoritmos RSA e Dif ie-He lman groups 1, 2, 5 e 14.

1.1.8.6. Deve suportar Certificado Digital X.509.

1.1.8.7. Deve suportar NAT-T (NAT Transversal).

1.1.8.8. Deve permitir a criação de túneis VPN SSL/TLS e IPSec.

1.1.8.9. Deve suportar VPN IPSec client-to-site (acesso remoto).

1.1.8.10. Deve possuir cliente próprio para instalação nos dispositivos móveis dos usuários, sem custo adicional.

1.1.8.11. Deve permitir que o usuário realize a conexão VPN por meio de cliente instalado nos sistemas operacionais: Windows, Mac OS ou Linux do seu equipamento ou então por meio de interface web do tipo portal.

1.1.8.12. Caso o acesso seja feito por meio da interface Web, deverá ser compatível com, no mínimo, as versões atualizadas dos seguintes navegadores: Microsoft Edge, Mozilla Firefox e Google Chrome.

1.1.8.13. Deve suportar atribuição de endereço IP nos clientes remotos de VPN.

1.1.8.14. Deve suportar atribuição de DNS nos clientes remotos de VPN.

1.1.8.15. Deve suportar, no mínimo, os protocolos de roteamento estático e dinâmico OSPF e BGP.

1.1.8.16. O túnel IPSec VPN do cliente ao gateway (client-to-site) deve fornecer uma solução de autenticação única (single-sign-on) aos usuários, integrando-se com as ferramentas de Windows login.

1.1.8.17. O túnel IPSec VPN client-to-site deve também possuir autenticação em fator duplo (2FA) aos usuários.

1.1.8.18. Deve permitir criar políticas por usuário e grupos para tráfego de VPN client-to-site.

1.1.8.19. Deve suportar autoridade certificadora integrada ao gateway VPN ou à solução de gerenciamento centralizado.

1.1.8.20. Deve promover a integração com diretórios LDAP e Active Directory para a autenticação de usuários de VPN e regras de acesso.

1.1.8.21. Deve suportar os métodos de autenticação de VPN: usuário e senha de base interna do próprio equipamento, usuário e senha de diretório LDAP, usuário e senha do Active Directory, certificação digital por meio de certificados emitidos por autoridade certificadora integrada ao equipamento ou à solução de gerenciamento centralizado, certificação digital por meio de certificados emitidos por autoridade certificadora integrada ao Active Directory, certificação digital por meio de certificados emitidos por autoridade certificadora no padrão ICP-Brasil.

1.1.8.22. Deve suportar a integração com autoridades certificadoras de terceiros que possam gerar certificados no formato PKCS#12.

1.1.8.23. Deve suportar a solicitação de emissão de certificados a uma autoridade certificadora de confiança (enro lment) via SCEP (Simple Certificate Enro lment Protocol) ou CSR (Certificate Signing Requests).

1.1.8.24. Deve suportar a leitura e verificação de CRLs (Certification Revogation Lists).

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

1.1.8.26. Deve possuir mecanismos de checagem de conformidade do dispositivo remoto.

1.1.8.27. A checagem de conformidade deve permitir verificar, no mínimo, as seguintes informações no cliente remoto: sistema operacional e patches instalados, antivírus e versão instalada, firewall no host.

1.1.9. **Qualidade de Serviço (QoS)**

1.1.9.1. Deve permitir o controle de políticas de uso com base nas aplicações: permitir, negar, agendar, inspecionar e controlar o uso da largura de banda que utilizam cada aplicação ou usuário.

1.1.9.2. Deve suportar a criação de políticas de controle de uso de largura de bandas baseadas em: porta ou protocolo, endereço IP de origem ou destino, usuário ou grupo de usuários, aplicações (por exemplo, Youtube e WhatsApp).

1.1.9.3. Deve suportar a priorização em tempo real de protocolos de voz (VoIP) como H.323, SIP.

1.1.9.4. Deve suportar a marcação de pacotes Dif Serv.

1.1.9.5. Deve permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário.

1.1.10. **Balanceamento de Links**

1.1.10.1. Deve implementar balanceamento de links utilizando as seguintes métricas e critérios para a escolha do caminho: aplicações, jitter, latência e perda de pacotes, permitindo que administradores configurem os valores de tais parâmetros para definir por qual interface certo tipo de tráfego será enviado.

1.1.10.2. Caso o item acima não seja atendido em sua totalidade, será aceita composição com outro equipamento, do tipo appliance físico, desde que a configuração seja realizada através da interface de gerenciamento do firewall e da Solução de Gerenciamento Centralizada, sem nenhum ônus para a Contratante, garantindo o pleno atendimento das métricas e critérios para a escolha do caminho, segundo o item acima.

1.1.10.3. O appliance físico do item anterior deve possuir throughput igual ou superior à discriminada no throughput das “funcionalidades de Filtro de Pacotes, IPS, Filtro de Conteúdo e Proteção contra Malwares habilitadas simultaneamente” do respectivo firewall.

1.1.10.4. O appliance físico do item anterior deve possuir os mesmos requisitos de fontes de alimentação e de afixação em rack, quando exigidos, do respectivo firewall.

1.1.10.5. Os valores dos parâmetros jitter e latência devem poder ser configurados em unidade mínima de milissegundos (ms).

1.1.10.6. A interface virtual de balanceamento deve suportar agregar no mínimo 4 (quatro) interfaces, podendo ser do tipo: física, sub interface e VPN.

1.1.10.7. Deve suportar balanceamento de link por hash do IP de origem e destino.

1.1.10.8. Deve suportar balanceamento de link por peso. Nesta opção deve ser possível definir o peso de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, 4 (quatro) links WAN.

1.1.10.9. Deve permitir a configuração da funcionalidade de balanceamento em qualquer interface WAN, seja ela MPLS, Internet, 4G/LTE etc.

1.1.10.10. Deve possuir roteamento baseado em políticas e múltiplas saídas (e tipos de saídas) WANs.

1.1.10.11. Deve permitir a configuração de failover entre links principais e secundários, caso os links utilizados ultrapassem os limites previamente definidos de jitter, latência e perda de pacotes. Estes limites podem ser configurados para forçar o failover caso apenas um ou todos os limites sejam atingidos simultaneamente.

1.1.10.12. Deve suportar a configuração de regras que permita o failback imediato.

1.1.10.13. Deve ser compatível com a solução de VPN, permitindo que suas características e análises sejam realizadas nas VPNs, assim como em links WAN.

1.1.10.14. Deve ser compatível com VPNs montadas em interfaces virtuais com roteamento dinâmico.

1.1.10.15. Deve realizar o gerenciamento de tráfego por tipo de aplicação.

1.1.10.16. Deve selecionar o melhor caminho baseado em tipo de tráfego e do host de origem.

1.1.10.17. Deve suportar o monitoramento de link com ping e TCP echo.

1.1.10.18. Deve suportar o monitoramento de links VPN (interfaces virtuais).

1.1.10.19. Deve permitir a exportação de informações via netflow.

1.1.11. **Recursos de Segurança**

1.1.11.1. Deve possuir, no mínimo, funcionalidades Anti-Vírus, Anti-Bot, Anti-Malware, AntiSpyware, Sistema de Prevenção de Intrusão (IPS), Filtro de Conteúdo Web, Controle de Aplicação, Prevenção de Perdas de Dados (DLP). E sistemas de prevenção de ameaças de ZeroDay;

1.1.11.2. Deve suportar o funcionamento nos modos snif er (para inspeção de tráfego gerado por uma porta de rede espelhada), layer-2, layer-3, de forma simultânea em uma única instância de firewall;

1.1.11.3. Deve aplicar novas políticas de segurança sem provocar indisponibilidade de serviço ou descontinuidade das conexões ativas;

1.1.11.4. Deve possuir capacidade de melhoria e análise das regras atuais, baseadas em camada 3 e 4 (porta/protocolo), indicando como a referida regra deverá ser configurada em camada 7 (aplicação);

1.1.11.5. O fluxo de análise de regras legadas deve permitir a visualização de quais aplicações estão em uso. Caso não possua essa funcionalidade, será permitida a integração com ferramentas que executam esta função;

1.1.11.6. Deve suportar as atualizações automáticas das bases de assinaturas utilizadas na identificação de vírus, intrusões (IPS) e aplicações sem a necessidade de intervenção manual pelo administrador, sem perda das conexões ativas e sem reinicialização do equipamento.

1.1.11.7. Deve suportar as atualizações automáticas das listas de geolocalização e das listas e categorias de URLs sem a necessidade de intervenção manual pelo administrador, sem perda das conexões ativas e sem reinicialização do equipamento;

1.1.11.8. Deve possuir proteção contra ataques, no mínimo, dos tipos: IP Spoofing, Negação de Serviço (DoS e DDoS), SYN Flood Attack, ICMP Flood Attack e UDP Flood Attack, Buffer Overflow, Port Scanning, Man-in-the-Middle;

1.1.11.9. Deve identificar, decriptografar e analisar o tráfego SSL tanto em conexões de entrada (inbound) quanto de saída (outbound), com suporte a HTTP/2 e TLS 1.2 e 1.3;

1.1.11.10. Deve permitir a decriptografia da área útil do pacote de dados (payload) para fins de controle de acesso à Internet e proteção contra ameaças;

1.1.11.11. Deve permitir a diferenciação de conexões pessoais (bancos, shopping etc) e conexões não pessoais por meio de classificação automática;

1.1.11.12. Deve possuir funcionalidade de backup e restore da configuração e das políticas de segurança através do carregamento de arquivo de configuração previamente salvo;

1.1.11.13. Deve armazenar os backups localmente, ou na solução de gerenciamento centralizado, e permitir que sejam transferidos para equipamentos externos por meio dos protocolos FTP ou SCP;

1.1.11.14. Deve possuir a capacidade de identificar ataques de Advanced Persistent Threat (APT) ou Zero-Day;

1.1.11.15. Deve possuir a capacidade de emular um ambiente operacional isolado e seguro (Sandbox), na nuvem do fabricante, para execução e observação de código malicioso, sem a utilização de assinaturas, com base na atividade, como, por exemplo, operações de arquivo, alterações de registro e sistema etc;

1.1.11.16. O equipamento do Lote 1 deve suportar a análise em, pelo menos, dois dos seguintes sistemas operacionais: Windows, Linux, MacOS e Android. Os equipamentos dos Lotes 2 e 3 devem suportar a análise em, pelo menos, um dos sistemas citados;

1.1.11.17. Deve suportar a análise dos tipos de arquivos: documentos Microsoft Office, dll, exe, pdf, gzip, tar, zip;

1.1.11.18. Deve suportar a análise dos protocolos HTTP/HTTPS, FTP e SMTP;

1.1.11.19. Desejável que a análise de links em sandbox seja capaz de classificar sites falsos na categoria de phishing e atualizar a base de filtro de URL da solução;

1.1.11.20. Para ameaças trafegadas em protocolo SMTP e POP3, é desejável que a solução seja capaz de mostrar nos relatórios o remetente, destinatário e assunto dos e-mails, permitindo identificação ágil do usuário vítima do ataque;

1.1.11.21. Deve permitir visualizar os resultados das análises de malwares de dia zero nos diferentes sistemas operacionais suportados;

1.1.11.22. Deve permitir informar ao fabricante quanto a suspeita de ocorrências de falso-positivo e falso- negativo na análise de malwares de dia zero;

1.1.11.23. Deve atualizar a base com assinaturas para bloqueio dos malwares identificados em sandbox de maneira automática, com frequência de pelo menos 30 minutos;

1.1.11.24. Desejável permitir o envio para análise em sandbox de malwares bloqueados pelo antivírus;

1.1.11.25. Para ameaças trafegadas em protocolo SMTP e POP3, a solução deve ter a capacidade de mostrar nos relatórios o remetente, destinatário e assunto dos e-mails permitindo identificação ágil do usuário vítima do ataque;

1.1.11.26. O sistema de análise “In Cloud” ou local deve prover informações sobre as ações do Malware na máquina infectada, informações sobre quais aplicações são utilizadas para causar/propagar a infecção, detectar aplicações não confiáveis utilizadas pelo Malware, gerar assinaturas de Antivírus e Anti-spyware automaticamente, definir URLs não confiáveis utilizadas pelo novo Malware e prover informações sobre o usuário infectado (seu endereço IP e seu login de rede);

1.1.11.27. Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos java (.jar e class), Android APKs MacOS (mach-O, DMG e PKG), Linux (ELF), RAR e 7-ZIP no ambiente de sandbox;

1.1.11.28. A solução deve analisar os arquivos do tipo malware em ambiente sandbox para baremetal, a fim de evitar técnicas de evasão;

1.1.11.29. A solução deve possuir a capacidade de analisar em sand-box os links (http e https) presentes no corpo de e-mails trafegados em SMTP e POP3.

1.1.12. **Filtro de Pacotes**

1.1.12.1. Não deve possuir restrições ao número de máquinas ou usuários protegidos.

1.1.12.2. Deve informar o número de sessões simultâneas.

1.1.12.3. Deve suportar a implementação tanto em modo transparente (layer-2) quanto em modo gateway (layer-3).

1.1.12.4. Deve suportar Statefull Packet Inspection de tráfego IPv4 e IPv6.

1.1.12.5. Deve suportar controle de acesso para serviços e protocolos pré-definidos, bem como possibilitar a adição de novos serviços e protocolos.

1.1.12.6. Deve suportar os protocolos H.323, SIP.

1.1.12.7. Deve implementar mecanismo de proteção contra ataques de falsificação de endereços IP (anti-spoofing).

1.1.12.8. Deve implementar mecanismo de captura de pacotes, de forma manual ou automática, quando uma ameaça for detectada.

1.1.12.9. Deve identificar os usuários para qualquer protocolo ou aplicação baseada em TCP, UDP e ICMP.

1.1.12.10. Deve suportar a utilização simultânea de políticas de segurança em IPv4 e IPv6.

1.1.12.11. Deve suportar a implementação de políticas de segurança baseadas em: portas, protocolos, usuários, grupos de usuários, endereços IP, redes CIDR/VLSM, horário ou período de tempo, e suas combinações.

1.1.12.12. Deve suportar a consulta a fontes externas de endereços IP, domínios e URL’s podendo ser adicionados nas políticas de firewall para bloqueio ou permissão do tráfego.

1.1.12.13. Desejável possuir mecanismos de otimização de regras. De forma que com base na análise de tráfego o sistema automaticamente faça sugestões e melhorias nas regras existentes.

1.1.12.14. Deve suportar granularidade nas políticas de IPS, antivírus e anti-spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens.

1.1.13. **Filtro de Conteúdo**

1.1.13.1. Deve prover o controle e proteção de acesso à Internet por meio do reconhecimento de aplicações, independente de porta e protocolo, e da classificação de URLs.

1.1.13.2. Deve ser capaz de identificar aplicações, independentemente das portas e protocolos, bem como das técnicas de evasão utilizadas.

1.1.13.3. Deve ser capaz de identificar se as aplicações estão utilizando sua porta padrão.

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

1.1.13.5. Deve ser capaz de identificar aplicações criptografadas usando SSL.

1.1.13.6. Deve ser capaz de identificar um mínimo de 1.400 (mil e quatrocentas) aplicações, incluindo, mas não se limitando a: 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.

1.1.13.7. Deve ser capaz de identificar, no mínimo, as seguintes aplicações: Bittorrent, Youtube, Livestream, Skype, Viber, WhatsApp, Snapchat, Facebook, Facebook Messenger, Instagram, Twitter, Linkedin, Dropbox, Google Drive, One Drive, Logmein, Teamviewer, MS-RDP, VNC, Ultrasurf, TOR, Webex.

1.1.13.8. Deve armazenar a base de assinaturas no próprio equipamento.

1.1.13.9. Deve classificar as aplicações em categorias.

1.1.13.10. Deve permitir o agrupamento de aplicações em grupos personalizados.

1.1.13.11. Deve identificar os usuários que estão utilizando as aplicações.

1.1.13.12. Deve permitir o bloqueio de aplicações que não estejam utilizando suas portas padrão.

1.1.13.13. Deve suportar a implementação de políticas de segurança baseadas em: aplicações, categorias de aplicações, endereço IP de origem ou destino, rede CIDR/VLSM de origem ou destino, usuário ou grupo de usuários, horário ou período de tempo, e suas combinações.

1.1.13.14. Deve proteger contra o roubo de credenciais, usuários e senhas identificadas através da integração com Active Directory submetidos em sites não corporativos. Deve ainda permitir criação de regra onde usuários do Active Directory só possam enviar informações de login para sites autorizados na solução;

1.1.13.15. Deve permitir bloquear o acesso do usuário caso o mesmo tente fazer o envio de suas credenciais em sites classificados como phishing pelo filtro de URL da solução;

1.1.13.16. Deve permitir a utilização ou bloqueio individualizado das aplicações, como BitTorrent e Skype, para determinados usuários ou grupos de usuários.

1.1.13.17. Deve permitir o registro de todos os fluxos autorizados/bloqueados das aplicações, incluindo o usuário identificado.

1.1.13.18. Deve permitir o controle de uso de banda de download ou upload utilizada pelas aplicações (traffic shaping) baseado em: endereço IP ou rede CIDR/VLSM de origem ou destino, usuário ou grupo de usuários, horário ou período de tempo, e suas combinações.

1.1.13.19. Deve ser capaz de efetuar a classificação de conteúdo de páginas web em HTTP e HTTPS, baseado em listas de categoria.

1.1.13.20. 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, 60 (sessenta) categorias ou subcategorias pré-definidas ou suas semelhantes: conteúdo adulto, chat, drogas ilegais, jogos de azar, jogos, pirataria, proxy remoto, redes sociais, streaming media, violência, pornografia, racismo, malware.

1.1.13.21. Deve permitir a inclusão de URLs customizadas por política (whitelist).

1.1.13.22. Deve armazenar as listas de categoria no próprio equipamento.

1.1.13.23. Deve identificar os usuários que estão acessando as páginas web.

1.1.13.24. Deve suportar a implementação de políticas de segurança baseadas em: URLs, categorias de URLs, endereço IP de origem ou destino, rede CIDR/VLSM de origem ou destino, usuário ou grupo de usuários, horário ou período de tempo, e suas combinações.

1.1.13.25. Deve alertar o usuário quando uma URL for bloqueada, por meio de página de bloqueio que possa ser customizada, e que informe, no mínimo, o motivo do bloqueio e a categoria na qual a URL foi classificada.

1.1.13.26. Deve permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado, informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão "Continuar" para possibilitar o usuário continuar acessando o site).

1.1.13.27. Deve permitir registrar todos os acessos autorizados ou bloqueados às páginas web, incluindo sua classificação e o usuário identificado.

1.1.13.28. Desejável permitir habilitar aplicações SaaS apenas no modo corporativo e bloqueá-las quando usadas no modo pessoal.

1.1.13.29. Desejável identificar o uso de táticas evasivas, ou seja, ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas.

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

1.1.13.31. Deve permitir bloquear o acesso a sites de busca (Google, Bing, Yahoo), caso a opção Safe Search esteja desabilitada.

1.1.13.32. Deve suportar base ou cache de URL's local no appliance, evitando delay de comunicação/validação das URL's.

1.1.13.33. Desejável que a categorização de URL's analise a URL ao menos até o nível de diretório.

1.1.13.34. Desejável que a solução proteja contra o roubo de credenciais, usuários e senhas identificadas através da integração com Active Directory submetidos em sites não corporativos. Desejável ainda que permita a criação de regras onde usuários do Active Directory só possam enviar informações de login para sites autorizados.

1.1.13.35. Deve prover análise em tempo real de páginas maliciosas e dessa forma permitir a proteção em tempo real antes mesmo da atualização das bases de dados de URLs. Caso o fabricante não possua esta funcionalidade em sua plataforma será permitida a composição da solução, sem ônus a este órgão.

1.1.14. **Prevenção de Intrusão (IPS)**

1.1.14.1. Deve possuir tecnologia de detecção e prevenção de ataques e intrusões baseada em assinatura.

1.1.14.2. Deve possuir, no mínimo, um conjunto de 10.000 (dez mil) assinaturas de detecção e prevenção de ataques.

1.1.14.3. Deve detectar protocolos independentemente da porta utilizada, identificando aplicações conhecidas em portas não-padrão.

1.1.14.4. Deve possuir, no mínimo, os seguintes mecanismos de detecção e prevenção: assinaturas de vulnerabilidades e exploits, assinaturas de ataques, validação de protocolos, detecção de anomalias, IP defragmentation, remontagem de pacotes TCP, nível de severidade do ataque.

1.1.14.5. Deve ser capaz de inspecionar tráfego criptografado usando SSL.

1.1.14.6. Deve ser capaz de inspecionar integralmente todos os pacotes de dados, independentemente de seus tamanhos.

1.1.14.7. Deve identificar os usuários relacionados aos eventos de intrusão.

1.1.14.8. Deve identificar os usuários relacionados aos eventos de bloqueio.

1.1.14.9. Deve permitir a criação de políticas de segurança que alertem, sem bloquear, sobre a ocorrência de um determinado ataque ou ameaça.

1.1.14.10. Deve permitir a criação de políticas de segurança que bloqueiem uma determinada ameaça.

1.1.14.11. Deve permitir a criação de políticas de segurança que bloqueiem um determinado ataque por meio de uma ação de DROP/RESET.

1.1.14.12. Deve permitir registrar todos os eventos de IPS, incluindo o usuário identificado.

1.1.14.13. Deve identificar e bloquear a comunicação com botnets.

1.1.14.14. Deve bloquear malwares e spywares.

1.1.14.15. Deve inspecionar e bloquear vírus nos seguintes tipos de tráfego, no mínimo: HTTP, HTTPS, SMTP, POP3, FTP e SMB.

1.1.14.16. Deve suportar proteção contra vírus em conteúdo HTML e javascrip, software espião (spyware) e worms.

1.1.14.17. Deve suportar a inspeção de vírus em arquivos comprimidos utilizando o algoritmo deflate (zip, gzip etc).

1.1.14.18. Deve suportar bloqueio de download de pelo menos 45 tipos de arquivos.

1.1.14.19. Deve armazenar as bases de assinaturas no próprio equipamento.

1.1.14.20. Deve possuir a capacidade de detectar e prevenir contra ameaças em tráfego HTTP/2.

1.1.15. **Instalação e Configuração da Solução (para os itens 1, 2, 3 e 4 dos Lotes 1, 2 e 3)**

As especificações de Instalação e Configuração das soluções de Firewall encontram-se no subtópico 5.7.2. do Estudo Técnico Preliminar.

1.1.16. **Garantia do Produto (Para os itens 1, 2, 3 e 4 dos Lotes 1, 2 e 3)**

As especificações de Garantia dos produtos adquiridos encontram-se no subtópico 5.7.3. do Estudo Técnico Preliminar.

1.2. **Características Gerais das Consoles dos Lotes 1, 2 e 3**

1.2.1. **Console de Gerenciamento Centralizado**

1.2.1.1. Deve ser fornecida em appliance virtual, compatível VMware vSphere ESXi 6.0 ou superior, ou baseado em software, compatível com Windows Server 2012 R2 ou superior, ou em appliance físico com suporte à fixação em bastidor (rack) padrãoEIA-310 com largura de 19' (dezenove polegadas) e altura de até duas unidades de rack (2U), acompanhado de todos os acessórios necessários (cabos, suportes, gavetas, braços, trilhos etc).

1.2.1.2. Deve ser acessada via interface web ou através de um software cliente, com interface gráfica, instalado no Windows ou Linux.

1.2.1.3. Deve estar licenciada em caráter permanente/perpétuo para todas as funcionalidades e quantidades mencionadas.

1.2.1.4. Deve permitir o gerenciamento centralizado dos equipamentos de firewall sejam eles virtuais ou físicos em uma mesma console, permitindo os seguintes requisitos:

I - Coleta de logs;

II - Análise de logs;

III - Gerenciamento de firewalls;

IV - Correlação de logs.

1.2.1.5. Deve estar licenciada e permitir a gerência centralizada de, no mínimo, 15 equipamentos.

1.2.1.6. Deve estar licenciada para o limite máximo de usuários, objetos, regras de segurança, NAT e endereços IP suportados pela solução.

1.2.1.7. As comunicações entre a CGC e os firewalls e entre a CGC e as estações dos administradores do sistema devem ser criptografadas e autenticadas.

1.2.1.8. Deve ser capaz de realizar todas as configurações nos firewalls descritas nesta ata.

1.2.1.9. Deve possibilitar a aplicação simultânea de configurações em todos os firewalls gerenciados pela solução.

1.2.1.10. Deve permitir a criação e distribuição de políticas de segurança de forma centralizada, suportando organização hierárquica de regras.

1.2.1.11. Deve suportar, por meio da interface gráfica de gerenciamento, a criação e administração de políticas de filtro de pacotes, prevenção de intrusão, controle de aplicação, filtragem de URLs, monitoração de logs, debugging, troubleshooting e captura de pacotes.

1.2.1.12. Deve ser capaz de gerenciar os firewa ls em unidades remotas, fora da rede local.

1.2.1.13. Deve permitir a autenticação dos administradores através de contas locais e bases externas LDAP ou Active Directory.

1.2.1.14. Será permitido que a solução de gerenciamento centralizado possua um “appliance virtual” específico para atendimento às necessidades de identificação e autenticação de usuários.

1.2.1.15. 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,

1.2.1.16. Deve permitir a criação de perfis customizados.

1.2.1.17. Deve permitir, de forma granular, assinalar permissões para os administradores criarem outros usuários, alterarem e ler configurações etc.

1.2.1.18. Deve permitir múltiplos administradores acessando o equipamento simultaneamente, sem restrição para leitura e escrita.

1.2.1.19. Deve suportar o bloqueio de alterações, evitando o conflito de configurações entre diferentes administradores efetuando alterações simultaneamente.

1.2.1.20. Deve registrar, em log de auditoria, as ações dos usuários administradores com o horário da alteração.

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

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

1.2.1.23. Deve possibilitar o gerenciamento (incluindo a criação, alteração, monitoração e exclusão) de objetos de rede. Deve 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.

1.2.1.24. 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).

1.2.1.25. Deve garantir que quando houver novas versões de software dos equipamentos, seja realizada a distribuição e atualização remota, de maneira centralizada.

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

1.2.1.27. Deve suportar configuração das funcionalidades de alta disponibilidade dos dispositivos físicos.

1.2.1.28. Deve permitir localizar em quais regras um objeto está sendo utilizado.

1.2.1.29. Deve permitir a identificação e exclusão de regras e objetos que estão aplicadas nos dispositivos, mas não afetam o desempenho e a segurança da rede (regras e objetos em desuso sob o ponto de vista lógico).

1.2.1.30. Deve suportar a geração de alertas automáticos via SNMP e syslog.

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

1.2.1.32. Deve informar o número de conexões simultâneas dos equipamentos gerenciados.

1.2.1.33. O gerenciamento da solução deve suportar acesso via SSH, cliente, WEB (HTTPS) e API aberta.

1.2.1.34. As consoles de gerenciamento centralizado, gerenciamento de logs, relatoria centralizada, poderão ser entregues em um único appliance, desde que atenda a todas as exigências deste documento.

1.2.2. **Console de Gerenciamento de Logs**

1.2.2.1. Deve ser fornecida em appliance virtual, compatível VMware vSphere ESXi 6.0 ou superior, ou baseado em software, compatível com Windows Server 2012 R2 ou superior, ou em appliance físico com suporte à fixação em bastidor (rack) padrãoEIA-310 com largura de 19’ (dezenove polegadas) e altura de até duas unidades de rack (2U), acompanhado de todos os acessórios necessários (cabos, suportes, gavetas, braços, trilhos etc).

1.2.2.2. Deve possuir relatórios de utilização dos recursos por aplicação, URLs, ameaças e etc.

1.2.2.3. Deve possuir visualização sumarizada de todas as aplicações, ameaças e URLs que foram identificadas e controladas pela solução.

1.2.2.4. Deve permitir a criação de relatórios customizados.

1.2.2.5. Deve ser capaz de receber logs de todos os firewa ls especificados nesta ATA.

1.2.2.6. 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.

1.2.2.7. Deve possibilitar o registro dos fluxos de dados relativos a cada sessão, armazenando: endereços IP de origem e destino dos pacotes, traduções NAT, portas e protocolos de origem e destino, usuário identificado, ação sobre o pacote (permitido ou negado).

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

1.2.2.9. Deve possuir funcionalidade de exportação de relatórios e logs para o computador local ou via FTP, SFTP ou SCP.

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

1.2.2.11. Deve estar licenciada em caráter permanente/perpétuo para todas as funcionalidades e quantidades mencionadas.

1.2.2.12. Deve estar licenciada e permitir a correlação de todos os eventos gerados por todos os equipamentos e contextos virtuais que compõem a solução.

1.2.2.13. O appliance virtual deve estar licenciado de maneira irrestrita quanto ao armazenamento, possibilitando cada órgão contratante armazenar o volume de logs que julgar necessário, utilizando recursos computacionais próprios;

1.2.2.14. Deve ser acessada via interface web ou através de um software cliente, com interface gráfica, instalado no Windows ou Linux.

1.2.2.15. Será permitida a entrega do “Console de Gerenciamento de Logs” como software agregado ao “Console de Gerenciamento Centralizado” ou ao “Console de Relatoria Centralizada”.

1.2.3. **Console de Relatoria Centralizada**

1.2.3.1. Deve ser fornecida em appliance virtual, compatível com VMware vSphere ESXi 6.5 ou superior, ou baseado em software, compatível com Windows Server 2012 R2 ou superior.

1.2.3.2. Deve ser acessada via interface web ou através de um software cliente, com interface gráfica, instalado no Windows ou no Linux.

1.2.3.3. Deve estar licenciada em caráter permanente/perpétuo para todas as funcionalidades e quantidades mencionadas.

1.2.3.4. Deve estar licenciada e permitir a gerência centralizada de relatórios, para no mínimo, 15 equipamentos.

1.2.3.5. As comunicações entre a Console de Relatoria e os firewalls e entre a Console de Relatoria e as estações dos administradores do sistema devem ser criptografadas e autenticadas.

1.2.3.6. Deve ser capaz de gerar relatórios de equipamentos em unidades remotas, fora da rede local.

1.2.3.7. Deve permitir a autenticação dos administradores através de contas locais e bases externas LDAP ou Active Directory.

1.2.3.8. A console deve suportar acesso via SSH, cliente e WEB (HTTPS).

1.2.3.9. Deve coletar logs dos Firewalls, do “Console de Gerenciamento Centralizado” e do “Console de Gerenciamento de Logs”.

1.2.3.10. Deve garantir a geração de relatórios com mapas geográficos, ou modo tabela, gerados em tempo real, para a visualização de origens e destinos do tráfego.

1.2.3.11. Deve permitir a extração de relatórios.

1.2.3.12. Deve possuir relatórios pré-definidos.

1.2.3.13. Deve permitir a geração de relatórios de logs de tráfego de dados.

1.2.3.14. Deve permitir a geração de relatórios de logs para auditoria das configurações de regras, objetos e acessos.

1.2.3.15. Deve possibilitar o envio de maneira automática de relatórios por e-mail.

1.2.3.16. Deve permitir o agendamento da geração de relatórios.

1.2.3.17. Deve ter a capacidade de definir filtros nos relatórios.

1.2.3.18. Deve gerar alertas automáticos via e-mail, snmp e syslog baseados em eventos de ocorrência como log, severidade de log, entre outros.

1.2.3.19. Deve permitir a criação de painéis (dashboards) customizados para visibilidades do tráfego de aplicativos, categorias de url, ameaças, serviços, países, origem e destino.

1.2.3.20. Deve possibilitar a visualização na interface gráfica de usuário (gui) da "console de relatoria centralizada as seguintes informações do sistema: logs diários recebidos, alertas gerados, entre outros.

1.2.3.21. Será permitida a entrega do "Console de Relatoria Centralizada" como software agregado ao "Console de Gerenciamento Centralizado" ou ao "Console de Gerenciamento de Logs".

1.3. **Características Gerais dos Treinamentos Operacionais dos Lotes 1, 2 e 3**

As especificações dos cursos de treinamento (itens 5 dos Lotes 1, 2 e 3) encontram-se no subtópico 5.2. do Estudo Técnico Preliminar.

2. LOTE 1 - FIREWALL TIPO 1

2.1. **Características Específicas do Firewall Tipo 1**

2.1.1. Throughput de 40 Gbps com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação IPS, Antivírus e Antispyware. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito.

2.1.2. Em relação ao filtro de pacotes, deve possuir o Throughput de no mínimo 60 Gbps com a funcionalidade de controle de aplicação habilitada para todas as assinaturas que o fabricante possuir.

2.1.3. Em relação ao túnel IPSec VPN, o throughput mínimo deverá ser de no mínimo 40 Gbps, com a inspeção e controle de aplicação e usuários ativada.

2.1.4. Deve permitir, no mínimo, 7.000.000 de conexões simultâneas.

2.1.5. Deve permitir, no mínimo, 380.000 novas conexões por segundo.

2.1.6. Deve permitir, no mínimo, 4000 VLANs.

2.1.7. Deve permitir, e estar licenciado para a utilização de 12.000 túneis VPN site-to-site simultâneos.

2.1.8. Deve permitir, e estar licenciado para a utilização de 25.000 túneis VPN client-to-site simultâneos.

2.1.9. Deve suportar afixação em bastidor (rack) padrão EIA-310 com largura de 19' (dezenove polegadas) e altura de até quatro unidades de rack(4U), acompanhado de todos os acessórios necessários (cabos, suportes, gavetas, braços, trilhos etc).

2.1.10. Deve possuir 2 (duas) fontes de alimentação independentes, redundantes e hotswappable.

2.1.11. O appliance deve possuir, no mínimo, 8 (oito) portas 1G/2.5G/5G/10G BASE-T RJ45.

2.1.12. Deve possuir, no mínimo, 10 (dez) interfaces SFP/SFP+, com transceivers SFP+ 10GB-SR, para conexão ao meio via cabo de fibra ótica.

2.1.13. Deve possuir, no mínimo, 4 (quatro) interfaces 25 Gbps para utilização de transceivers padrão SFP28.

2.1.14. Deve possuir, no mínimo, 4 (quatro) interfaces 40/100 Gbps para utilização de transceivers padrão QSFP+/QSFP28.

2.1.15. Deve possuir, disco Solid State Drive (SSD) ou cartão eMMC de, no mínimo, 400 GB.

2.1.16. Deve possuir, no mínimo, 20 sistemas virtuais lógicos (Contextos) no firewall Físico.

2.2. **Alta Disponibilidade**

2.2.1. Deve possibilitar a operação em alta disponibilidade (HA) no equipamento, permitindo uma arquitetura ativo/ativo e ativo/passivo com no mínimo 2 (dois) membros, com sincronismo de estados integrado.

2.2.2. Deve suportar o balanceamento de carga na arquitetura ativo/ativo.

2.2.3. Deve sincronizar sessões TCP/IP, tabelas NAT, tabelas FIB, associações de segurança das VPNs e todas as configurações necessárias para a manutenção da continuidade dos serviços.

2.2.4. Deve monitorar a falha dos links de comunicação.

2.2.5. Deve ser capaz de identificar e iniciar automaticamente um procedimento de failover sempre que ocorrer: a falha de um dos membros do cluster, a falha de qualquer componente ou processo crítico de um dos membros do cluster, a falha de um dos links de comunicação monitorados.

2.2.6. Deve ser capaz de realizar os procedimentos de failover sem perda das conexões ativas e sessões estabelecidas de forma transparente para o usuário.

2.2.7. Deve suportar a operação em cluster com no mínimo 2 equipamentos.

2.2.8. Desejável possuir 2 fans independentes, redundantese hotswappable.

2.2.9. Deve possuir discos de sistema e de logs independentes e redundantes (RAID).

3. LOTE 2 - FIREWALL TIPO 2

3.1. **Características Específicas do Firewall Tipo 2**

3.1.1. Throughput de 09 Gbps com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação IPS, Antivírus e Antispyware. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito.

3.1.2. Em relação ao filtro de pacotes, deve possuir o throughput mínimo de 19 Gbps.

3.1.3. Em relação ao túnel IPSec VPN, deve possuir o throughput mínimo de 9 Gbps.

3.1.4. Deve permitir, no mínimo, 1.900.000 conexões simultâneas.

3.1.5. Deve permitir, no mínimo, 200.000 novas conexões por segundo.

3.1.6. Deve permitir, no mínimo, 4000 VLANs.

3.1.7. Deve permitir, e estar licenciado para a utilização de 2000 túneis VPN site-to-site simultâneos.

3.1.8. Deve permitir, e estar licenciado para a utilização de 1800 túneis VPN client-to-site simultâneos.

3.1.9. Deve suportar a fixação em bastidor (rack) padrão EIA-310 com largura de 19' (dezenove polegadas) e altura de no máximo três unidades de rack (3U), acompanhado de todos os acessórios necessários (cabos, suportes, gavetas, braços, trilhos etc).

3.1.10. O appliance deve possuir, no mínimo, 10 (dez) portas 100/1000/10000 BASE-T ou SFP podendo ser uma composição entre os dois tipos, acompanhadas de seus respectivos transceivers.

3.1.11. Deve possuir, no mínimo, 4 (quatro) interfaces 10 (dez) Gigabit-Ethernet padrão SFP+, com transceivers SFP+ 10GB-SR, para conexão ao meio via cabo de fibra ótica.

3.1.12. Deve possuir, disco Solid State Drive (SSD) ou cartão eMMC de, no mínimo, 480GB cada disco.

3.1.13. Deve possuir, no mínimo, 5 (cinco) interfaces 1 (um) Gigabit-Ethernet padrão SFP, para conexão ao meio via cabo de fibra ótica.

4. LOTE 3 - FIREWALL TIPO 3

4.1. Características Específicas do Firewall Tipo 3

4.1.1. Throughput de 2 Gbps com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação IPS, Antivírus e Antispyware. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito.

4.1.2. Em relação ao filtro de pacotes, deve possuir o throughput mínimo de 4 Gbps.

4.1.3. Em relação ao túnel IPSec VPN, deve possuir o throughput mínimo de 3 Gbps.

4.1.4. Deve permitir, no mínimo, 350.000 conexões simultâneas.

4.1.5. Deve permitir, no mínimo, 65.000 novas conexões por segundo.

4.1.6. Deve permitir, no mínimo, 4000 VLANs.

4.1.7. Deve permitir, e estar licenciado para utilização de 2000 túneis VPN site-to-site simultâneos.

4.1.8. Deve permitir, e estar licenciado para utilização de 1500 túneis VPN client-to-site simultâneos.

4.1.9. Deve suportar a fixação em bastidor (rack) padrão EIA-310 com largura de 19’ (dezenove polegadas) e altura de no máximo uma unidade de rack (1U), acompanhado de todos os acessórios necessários (cabos, suportes, gavetas, braços, trilhos etc).

4.1.10. O appliance deve possuir, no mínimo, 08 (oito) portas de rede 1G RJ-45.

4.1.11. O appliance deve possuir uma porta 10/100/1000 para gerenciamento “out-of-band”.

4.1.12. Deve possuir, disco Solid State Drive (SSD) ou cartão eMMC de, no mínimo, 128GB.

Rio de Janeiro, 04 de junho de 2024

Documento assinado eletronicamente por **Isabela Reboucas Costa**, **Analista de Sistemas**, em 06/06/2024, às 16:05, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Manuelito de Sousa Reis Junior**, **Gerente**, em 06/06/2024, às 16:24, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Monique Goncalves Paz**, **Diretora**, em 06/06/2024, às 16:29, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Fabio Ivo**, **Assistente**, em 06/06/2024, às 16:50, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Rosana Alves de Andrade**, **Analista de Sistemas**, em 06/06/2024, às 16:54, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Charles Monteiro Guimarães**, **Diretor**, em 06/06/2024, às 17:22, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Cristina da Silva Barros Drongitis**, **Assessora Chefe**, em 26/08/2024, às 12:51, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

A autenticidade deste documento pode ser conferida no site http://sei.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **75937120** e o código CRC **5AA4C6DA**.

Rua da Conceição, 69, 24º Andar / 25º Andar - Bairro Centro, Rio de Janeiro/RJ, CEP 20051-011
Telefone:

Governo do Estado do Rio de Janeiro

Centro de Tecnologia de Informação e Comunicação do Estado do Rio de Janeiro

Vice Presidência de Tecnologia

ANEXO II DO ESTUDO TÉCNICO PRELIMINAR
Roteiro para Prova de Conceito - lote 01
firewall tipo 01

1. INTRODUÇÃO

1.1. Será realizada Prova de Conceito com o objetivo de verificar o atendimento dos requisitos funcionais considerados prioritários pelo PRODERJ, referente à proposta ofertada pela licitante classificada em primeiro lugar.

1.2. O roteiro da Prova de Conceito, nos termos que seguem abaixo, exigirá da referida licitante a comprovação de que sua solução atende as especificações de maior relevância aqui elencadas.

1.3. As especificações selecionadas neste anexo representam as características de maior impacto em relação à solução como um todo, e levam em consideração os aspectos técnicos que permitem comprovação em ambiente de teste, haja vista que determinados recursos/características/funcionalidades possuem restrições de comprovação quando a solução ainda não está completamente implementada.

1.4. Este anexo deve ser interpretado conforme as disposições do Estudo Técnico Preliminar (75936299) do qual é parte integrante e indissociável.

2. CARACTERÍSTICAS E FUNCIONALIDADES A SEREM COMPROVADAS

LOTE I - FIREWALL (TIPO 1)					
APPLIANCE FIREWALL TIPO 1 - INCLUSOS: HARDWARE, LICENCIAMENTO, INSTALAÇÃO, CONFIGURAÇÃO E GARANTIA POR 60 MESES					
Nº	**REF. ANEXO I**	**DESCRIÇÃO DO ITEM PARA COMPROVAÇÃO**	**CONTEXTO DO REQUISITO**	**OBSERVAÇÃO**	**REQUISITO APROVADO? (SIM/NÃO)**
1	1.1.4.3.	Deve permitir o acesso ao equipamento via SSH e interface web HTTPS.	Funcionalidades Básicas		
2	1.1.4.6.	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.	Funcionalidades Básicas		
3	1.1.4.10.	Os Firewalls de segurança físico ou virtualizados, devem possuir mecanismo para dedicar processamento no equipamento de segurança para funções e ações de Gerenciamento, mesmo que o equipamento esteja com alto processamento de CPU.	Funcionalidades Básicas		
4	1.1.5.3.	Deve suportar os protocolos DHCP e DHCPv6 e suas funcionalidades como cliente, servidor e relay.	Rede		
5	1.1.5.4.	Deve suportar Jumbo Frames.	Rede		
6	1.1.5.5.	Deve suportar sub interfaces Ethernet lógicas.	Rede		
7	1.1.5.8.	Deve permitir o registro de eventos de NAT com as informações de endereço interno, endereço público, data e hora do evento, portas de origem e destino.	Rede		

8	1.1.5.10.	Deve suportar as funcionalidades de roteamento estático e dinâmico em IPv4 e IPv6.	Rede		
9	1.1.5.16.	Deve suportar Policy Based Routing (PBR), possibilitando políticas de roteamento condicionado ao endereço IP de origem, endereço IP de destino e porta de comunicação.	Rede		
10	1.1.6.1.	Deve promover a integração com serviços de diretório LDAP e Active Directory, baseados em caracteres da língua portuguesa, para a identificação, autenticação, autorização e registro de eventos de acessos ou ameaças.	Autentificação e Identificação		
11	1.1.6.7.	Deve permitir a criação de políticas de segurança baseadas em usuários e grupos de usuários pertencentes a um diretório LDAP ou ao Active Directory.	Autentificação e Identificação		
12	1.1.6.10.	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.	Autentificação e Identificação		
13	1.1.7.1.	Deve identificar os países de origem e destino de todas as conexões estabelecidas através do equipamento.	Geolocalização		
14	1.1.7.4.	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.	Geolocalização		
15	1.1.7.5.	Deve possibilitar a visualização dos países de origem e destino nos logs de eventos de acessos e ameaças.	Geolocalização		
16	1.1.8.6.	Deve suportar Certificado Digital X.509.	VPN	Não precisa implementar certificado, basta mostrar as opções na manager.	
17	1.1.8.9.	Deve suportar VPN IPSec client-to-site (acesso remoto).	VPN		
18	1.1.8.11.	Deve permitir que o usuário realize a conexão VPN por meio de cliente instalado nos sistemas operacionais Windows, Mac OS ou Linux do seu equipamento ou então por meio de interface web do tipo portal.	VPN	No teste, a licitante precisará demonstrar este tópico apenas no Windows.	
19	1.1.8.15.	Deve suportar, no mínimo, os protocolos de roteamento estático e dinâmico OSPF e BGP.	VPN		

20	1.1.8.20.	Deve promover a integração com diretórios LDAP e Active Directory para a autenticação de usuários de VPN e regras de acesso.	VPN		
21	1.1.8.25.	Deve permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis de SSL.	VPN		
22	1.1.9.2.	Deve suportar a criação de políticas de controle de uso de largura de banda baseadas em: porta ou protocolo, endereço IP de origem ou destino, usuário ou grupo de usuários, aplicações (por exemplo, Youtube e WhatsApp).	QoS		
23	1.1.9.5.	Deve permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário.	QoS		
24	1.1.10.5.	Os valores dos parâmetros jitter e latência devem poder ser configurados em unidade mínima de milissegundos (ms).	Balanceamento de Links		
25	1.1.10.10.	Deve possuir roteamento baseado em políticas e múltiplas saídas (e tipos de saídas) WANs.	Balanceamento de Links		
26	1.1.10.12.	Deve suportar a configuração de regras que permita o failback imediato.	Balanceamento de Links	A licitante poderá demonstrar apenas as configurações na manager.	
27	1.1.11.3.	Deve aplicar novas políticas de segurança sem provocar indisponibilidade de serviço ou descontinuidade das conexões ativas.	Recursos de Segurança		
28	1.1.11.12.	Deve possuir funcionalidade de backup e restore da configuração e das políticas de segurança.	Recursos de Segurança		
29	1.1.10.15.	Deve possuir a capacidade de emular um ambiente operacional isolado e seguro (Sandbox), na nuvem do fabricante, para execução e observação de código malicioso, sem a utilização de assinaturas, com base na atividade, como, por exemplo, operações de arquivo, alterações de registro e sistema etc.	Recursos de Segurança		
30	1.1.12.5.	Deve suportar controle de acesso para, pelo menos, serviços e protocolos pré-definidos, bem como possibilitar a adição de novos serviços e protocolos.	Filtro de Pacotes		
31	1.1.12.9.	Deve identificar os usuários para qualquer protocolo ou aplicação baseada em TCP, UDP e ICMP.	Filtro de Pacotes		

32	1.1.12.11.	Deve suportar a implementação de políticas de segurança baseadas em: portas, protocolos, usuários, grupos de usuários, endereços IP, redes CIDR/VLSM, horário ou período de tempo, e suas combinações.	Filtro de Pacotes		
33	1.1.12.12.	Deve suportar a consulta a fontes externas de endereços IP, domínios e URL's podendo ser adicionados nas políticas de firewall para bloqueio ou permissão do tráfego.	Filtro de Pacotes		
34	1.1.13.9.	Deve classificar as aplicações em categorias.	Filtro de Conteúdo		
35	1.1.13.11.	Deve identificar os usuários que estão utilizando as aplicações.	Filtro de Conteúdo		
36	1.1.13.21.	Deve permitir a inclusão de URLs customizadas por política (whitelist).	Filtro de Conteúdo		
37	1.1.13.24.	Deve suportar a implementação de políticas de segurança baseadas em: URLs, categorias de URLs, endereço IP de origem ou destino, rede CIDR/VLSM de origem ou destino, usuário ou grupo de usuários, horário ou período de tempo, e suas combinações.	Filtro de Conteúdo		
38	1.1.13.25.	Deve alertar o usuário quando uma URL for bloqueada, por meio de página de bloqueio que possa ser customizada, e que informe, no mínimo, o motivo do bloqueio e a categoria na qual a URL foi classificada.	Filtro de Conteúdo		
39	1.1.13.27.	Deve permitir registrar todos os acessos autorizados ou bloqueados às páginas web, incluindo sua classificação e o usuário identificado.	Filtro de Conteúdo		
40	1.1.14.5.	Deve ser capaz de inspecionar tráfego criptografado usando SSL.	Prevenção de Intrusão - IPS		
41	1.1.14.9.	Deve permitir a criação de políticas de segurança que alertem, sem bloquear, sobre a ocorrência de um determinado ataque ou ameaça.	Prevenção de Intrusão - IPS		
42	1.1.14.14.	Deve bloquear malwares e spywares.	Prevenção de Intrusão - IPS		

43	2.1.1.	Throughput de 40 Gbps com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação IPS, Antivírus e Antispyware. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito.	Características Específicas do Firewall Tipo 1		
44	2.1.2.	Em relação ao filtro de pacotes, deve possuir o Throughput de no mínimo 60 Gbps com a funcionalidade de controle de aplicação habilitada para todas as assinaturas que o fabricante possuir.	Características Específicas do Firewall Tipo 1		
45	2.1.10.	Deve possuir 2 (duas) fontes de alimentação independentes, redundantes e hotswappable.	Características Específicas do Firewall Tipo 1		
46	2.1.11.	O appliance deve possuir, no mínimo, 8 (oito) portas 1G/2.5G/5G/10G BASE-T RJ45	Características Específicas do Firewall Tipo 1	Para a Prova de Conceito, comprovar somente a quantidade das referidas interfaces.	
47	2.1.12.	Deve possuir, no mínimo, 10 (dez) interfaces SFP/SFP+, com transceivers SFP+ 10GB-SR, para conexão ao meio via cabo de fibra ótica.	Características Específicas do Firewall Tipo 1	Para a Prova de Conceito, comprovar somente a quantidade das referidas interfaces.	
48	2.1.13.	Deve possuir, no mínimo, 4 (quatro) interfaces 25 Gbps para utilização de transceivers padrão SFP28.	Características Específicas do Firewall Tipo 1	Para a Prova de Conceito, comprovar somente a quantidade das referidas interfaces.	
49	2.1.14.	Deve possuir, no mínimo, 4 (quatro) interfaces 40/100 Gbps para utilização de transceivers padrão QSFP+/QSFP28.	Características Específicas do Firewall Tipo 1	Para a Prova de Conceito, comprovar somente a quantidade das referidas interfaces.	
50	2.2.1.	Deve possibilitar a operação em alta disponibilidade (HA) no equipamento, permitindo uma arquitetura ativo/ativo e ativo/passivo com no mínimo 2 (dois) membros, com sincronismo de estados integrado.	Características Específicas do Firewall Tipo 1 (HA)		
51	2.2.7.	Deve suportar a operação em cluster com no mínimo 2 equipamentos.	Características Específicas do Firewall Tipo 1 (HA)		
CONSOLE DE GERENCIAMENTO CENTRALIZADO PARA O FIREWALL TIPO 1 COM GARANTIA DE 60 MESES					
Nº	**REF. ANEXO I**	**DESCRIÇÃO DO ITEM PARA COMPROVAÇÃO**	**CONTEXTO DO REQUISITO**	**OBSERVAÇÃO**	**REQUISITO APROVADO? (SIM/NÃO)**
52	1.2.1.2.	Deve ser acessada via interface web ou através de um software cliente, com interface gráfica, instalado no Windows ou Linux;	Características Gerais das Consoles (Manager)		
53	1.2.1.9.	Deve permitir a criação e distribuição de políticas de segurança de forma centralizada, suportando organização hierárquica de regras.	Características Gerais das Consoles (Manager)		

54	1.2.1.11.	Deve ser capaz de gerenciar os firewalls em unidades remotas, fora da rede local.	Características Gerais das Consoles (Manager)		
55	1.2.1.12.	Deve permitir a autenticação dos administradores através de contas locais e bases externas LDAP ou Active Directory.	Características Gerais das Consoles (Manager)		
56	1.2.1.14.	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.	Características Gerais das Consoles (Manager)		
57	1.2.1.19.	Deve registrar, em log de auditoria, as ações dos usuários administradores com o horário da alteração.	Características Gerais das Consoles (Manager)		
58	1.2.1.25.	Deve ser capaz de testar a conectividade dos equipamentos gerenciados.	Características Gerais das Consoles (Manager)		
59	1.2.1.26.	Deve suportar configuração das funcionalidades de alta disponibilidade dos dispositivos físicos.	Características Gerais das Consoles (Manager)		
60	1.2.1.27.	Deve permitir localizar em quais regras um objeto está sendo utilizado.	Características Gerais das Consoles (Manager)		
61	1.2.1.30.	Deve informar a utilização dos recursos de CPU, memória e atividade de rede dos equipamentos gerenciados.	Características Gerais das Consoles (Manager)		
CONSOLE DE GERENCIAMENTO DE LOGS PARA O FIREWALL TIPO 1 COM GARANTIA DE 60 MESES					
Nº	**REF. ANEXO I**	**DESCRIÇÃO DO ITEM PARA COMPROVAÇÃO**	**CONTEXTO DO REQUISITO**	**OBSERVAÇÃO**	**REQUISITO APROVADO? (SIM/NÃO)**
62	1.2.2.6.	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.	Características Gerais das Consoles (Logs)		
63	1.2.2.12.	Deve estar licenciada e permitir a correlação de todos os eventos gerados por todos os equipamentos e contextos virtuais que compõem a solução.	Características Gerais das Consoles (Logs)		
64	1.2.2.14.	Deve ser acessada via interface web ou através de um software cliente, com interface gráfica, instalado no Windows ou Linux	Características Gerais das Consoles (Logs)		
CONSOLE DE RELATORIA CENTRALIZADA PARA O FIREWALL TIPO 1 COM GARANTIA DE 60 MESES					
Nº	**REF. ANEXO I**	**DESCRIÇÃO DO ITEM PARA COMPROVAÇÃO**	**CONTEXTO DO REQUISITO**	**OBSERVAÇÃO**	**REQUISITO APROVADO? (SIM/NÃO)**
65	1.2.3.2.	Deve ser acessada via interface web ou através de um software cliente, com interface gráfica, instalado no Windows ou Linux.	Características Gerais das Consoles (Relatórios)		
66	1.2.3.6.	Deve ser capaz de gerar relatórios de equipamentos em unidades remotas, fora da rede local.	Características Gerais das Consoles (Relatórios)		
67	1.2.3.12.	Possuir relatórios pré-definidos.	Características Gerais das Consoles (Relatórios)		
68	1.2.3.13.	Permitir a geração de relatórios de logs de tráfego de dados.	Características Gerais das Consoles (Relatórios)		
69	1.2.3.14.	Permitir a geração de relatórios de logs para	Características Gerais das Consoles (Relatórios)		

		auditoria das configurações de regras, objetos e acessos.			
70	1.2.3.15.	Possibilitar o envio de maneira automática de relatórios por e-mail.	Características Gerais das Consoles (Relatórios)		
71	1.2.3.17.	Ter a capacidade de definir filtros nos relatórios.	Características Gerais das Consoles (Relatórios)		
72	1.2.3.20.	Possibilitar a visualização na interface gráfica de usuário (gui) da "console de relatoria centralizada as seguintes informações do sistema: logs diários recebidos, alertas gerados, entre outros.	Características Gerais das Consoles (Relatórios)		

Rio de Janeiro, 04 de junho de 2024

Documento assinado eletronicamente por **Isabela Reboucas Costa**, **Analista de Sistemas**, em 06/06/2024, às 16:05, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Monique Goncalves Paz**, **Diretora**, em 06/06/2024, às 16:29, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Manuelito de Sousa Reis Junior**, **Gerente**, em 06/06/2024, às 16:34, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Fabio Ivo**, **Assistente**, em 06/06/2024, às 16:50, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Rosana Alves de Andrade**, **Analista de Sistemas**, em 06/06/2024, às 16:56, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Charles Monteiro Guimarães**, **Diretor**, em 06/06/2024, às 17:22, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Cristina da Silva Barros Drongitis**, **Assessora Chefe**, em 26/08/2024, às 12:51, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

A autenticidade deste documento pode ser conferida no site http://sei.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **75935971** e o código CRC **75249B50**.

Rua da Conceição, 69, 24º Andar / 25º Andar - Bairro Centro, Rio de Janeiro/RJ, CEP 20051-011
Telefone:

Governo do Estado do Rio de Janeiro

Centro de Tecnologia de Informação e Comunicação do Estado do Rio de Janeiro

Vice Presidência de Tecnologia

ANEXO III DO ESTUDO TÉCNICO PRELIMINAR
Roteiro para Prova de Conceito - lote 02
firewall tipo 02

1. INTRODUÇÃO

1.1. Será realizada Prova de Conceito com o objetivo de verificar o atendimento dos requisitos funcionais considerados prioritários pelo PRODERJ, referente à proposta ofertada pela licitante classificada em primeiro lugar.

1.2. O roteiro da Prova de Conceito, nos termos que seguem abaixo, exigirá da referida licitante a comprovação de que sua solução atende as especificações de maior relevância aqui elencadas.

1.3. As especificações selecionadas neste anexo representam as características de maior impacto em relação à solução como um todo, e levam em consideração os aspectos técnicos que permitem comprovação em ambiente de teste, haja vista que determinados recursos/características/funcionalidades possuem restrições de comprovação quando a solução ainda não está completamente implementada.

1.4. Este anexo deve ser interpretado conforme as disposições do Estudo Técnico Preliminar (75936299) do qual é parte integrante e indissociável.

2. CARACTERÍSTICAS E FUNCIONALIDADES A SEREM COMPROVADAS

LOTE 2 - FIREWALL (TIPO 2)					
APPLIANCE FIREWALL TIPO 2 - INCLUSOS: HARDWARE, LICENCIAMENTO, INSTALAÇÃO, CONFIGURAÇÃO E GARANTIA POR 60 MESES					
Nº	**REF. ANEXO I**	**DESCRIÇÃO DO ITEM PARA COMPROVAÇÃO**	**CONTEXTO DO REQUISITO**	**OBSERVAÇÃO**	**REQUISITO APROVADO? (SIM/NÃO)**
1	1.1.4.3.	Deve permitir o acesso ao equipamento via SSH e interface web HTTPS.	Funcionalidades Básicas		
2	1.1.4.6.	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.	Funcionalidades Básicas		
3	1.1.4.10.	Os Firewalls de segurança físico ou virtualizados, devem possuir mecanismo para dedicar processamento no equipamento de segurança para funções e ações de Gerenciamento, mesmo que o equipamento esteja com alto processamento de CPU.	Funcionalidades Básicas		
4	1.1.5.3.	Deve suportar os protocolos DHCP e DHCPv6 e suas funcionalidades como cliente, servidor e relay.	Rede		
5	1.1.5.4.	Deve suportar Jumbo Frames.	Rede		
6	1.1.5.5.	Deve suportar sub interfaces Ethernet lógicas.	Rede		
7	1.1.5.8.	Deve permitir o registro de eventos de NAT com as informações de endereço interno, endereço público, data e hora do evento, portas de origem e destino.	Rede		

8	1.1.5.10.	Deve suportar as funcionalidades de roteamento estático e dinâmico em IPv4 e IPv6.	Rede		
9	1.1.5.16.	Deve suportar Policy Based Routing (PBR), possibilitando políticas de roteamento condicionado ao endereço IP de origem, endereço IP de destino e porta de comunicação.	Rede		
10	1.1.6.1.	Deve promover a integração com serviços de diretório LDAP e Active Directory, baseados em caracteres da língua portuguesa, para a identificação, autenticação, autorização e registro de eventos de acessos ou ameaças.	Autentificação e Identificação		
11	1.1.6.7.	Deve permitir a criação de políticas de segurança baseadas em usuários e grupos de usuários pertencentes a um diretório LDAP ou ao Active Directory.	Autentificação e Identificação		
12	1.1.6.10.	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.	Autentificação e Identificação		
13	1.1.7.1.	Deve identificar os países de origem e destino de todas as conexões estabelecidas através do equipamento.	Geolocalização		
14	1.1.7.4.	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.	Geolocalização		
15	1.1.7.5.	Deve possibilitar a visualização dos países de origem e destino nos logs de eventos de acessos e ameaças.	Geolocalização		
16	1.1.8.6.	Deve suportar Certificado Digital X.509.	VPN	Não precisa implementar certificado, basta mostrar as opções na manager.	
17	1.1.8.9.	Deve suportar VPN IPSec client-to-site (acesso remoto).	VPN		
18	1.1.8.11.	Deve permitir que o usuário realize a conexão VPN por meio de cliente instalado nos sistemas operacionais Windows, Mac OS ou Linux do seu equipamento ou então por meio de interface web do tipo portal.	VPN	No teste, a licitante precisará demonstrar este tópico apenas no Windows.	
19	1.1.8.15.	Deve suportar, no mínimo, os protocolos de roteamento estático e dinâmico OSPF e BGP.	VPN		

20	1.1.8.20.	Deve promover a integração com diretórios LDAP e Active Directory para a autenticação de usuários de VPN e regras de acesso.	VPN		
21	1.1.8.25.	Deve permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis de SSL.	VPN		
22	1.1.9.2.	Deve suportar a criação de políticas de controle de uso de largura de banda baseadas em: porta ou protocolo, endereço IP de origem ou destino, usuário ou grupo de usuários, aplicações (por exemplo, Youtube e WhatsApp).	QoS		
23	1.1.9.5.	Deve permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário.	QoS		
24	1.1.10.5.	Os valores dos parâmetros jitter e latência devem poder ser configurados em unidade mínima de milissegundos (ms).	Balanceamento de Links		
25	1.1.10.10.	Deve possuir roteamento baseado em políticas e múltiplas saídas (e tipos de saídas) WANs.	Balanceamento de Links		
26	1.1.10.12.	Deve suportar a configuração de regras que permita o failback imediato.	Balanceamento de Links	A licitante poderá demonstrar apenas as configurações na manager.	
27	1.1.11.3.	Deve aplicar novas políticas de segurança sem provocar indisponibilidade de serviço ou descontinuidade das conexões ativas.	Recursos de Segurança		
28	1.1.11.12.	Deve possuir funcionalidade de backup e restore da configuração e das políticas de segurança.	Recursos de Segurança		
29	1.1.10.15.	Deve possuir a capacidade de emular um ambiente operacional isolado e seguro (Sandbox), na nuvem do fabricante, para execução e observação de código malicioso, sem a utilização de assinaturas, com base na atividade, como, por exemplo, operações de arquivo, alterações de registro e sistema etc.	Recursos de Segurança		
30	1.1.12.5.	Deve suportar controle de acesso para pelo menos serviços e protocolos pré-definidos, bem como possibilitar a adição de novos serviços e protocolos.	Filtro de Pacotes		
31	1.1.12.9.	Deve identificar os usuários para qualquer protocolo ou aplicação baseada em TCP, UDP e ICMP.	Filtro de Pacotes		

32	1.1.12.11.	Deve suportar a implementação de políticas de segurança baseadas em: portas, protocolos, usuários, grupos de usuários, endereços IP, redes CIDR/VLSM, horário ou período de tempo, e suas combinações.	Filtro de Pacotes		
33	1.1.12.12.	Deve suportar a consulta a fontes externas de endereços IP, domínios e URL's podendo ser adicionados nas políticas de firewall para bloqueio ou permissão do tráfego.	Filtro de Pacotes		
34	1.1.13.9.	Deve classificar as aplicações em categorias.	Filtro de Conteúdo		
35	1.1.13.11.	Deve identificar os usuários que estão utilizando as aplicações.	Filtro de Conteúdo		
36	1.1.13.21.	Deve permitir a inclusão de URLs customizadas por política (whitelist).	Filtro de Conteúdo		
37	1.1.13.24.	Deve suportar a implementação de políticas de segurança baseadas em: URLs, categorias de URLs, endereço IP de origem ou destino, rede CIDR/VLSM de origem ou destino, usuário ou grupo de usuários, horário ou período de tempo, e suas combinações.	Filtro de Conteúdo		
38	1.1.13.25.	Deve alertar o usuário quando uma URL for bloqueada, por meio de página de bloqueio que possa ser customizada, e que informe, no mínimo, o motivo do bloqueio e a categoria na qual a URL foi classificada.	Filtro de Conteúdo		
39	1.1.13.27.	Deve permitir registrar todos os acessos autorizados ou bloqueados às páginas web, incluindo sua classificação e o usuário identificado.	Filtro de Conteúdo		
40	1.1.14.5.	Deve ser capaz de inspecionar tráfego criptografado usando SSL.	Prevenção de Intrusão - IPS		
41	1.1.14.9.	Deve permitir a criação de políticas de segurança que alertem, sem bloquear, sobre a ocorrência de um determinado ataque ou ameaça.	Prevenção de Intrusão - IPS		
42	1.1.14.14.	Deve bloquear malwares e spywares.	Prevenção de Intrusão - IPS		

43	3.1.1.	Throughput de 10 Gbps com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação IPS, Antivírus e Antispyware. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito.	Características Específicas do Firewall Tipo 2		
44	3.1.2.	Em relação ao filtro de pacotes, deve possuir o Throughput mínimo de 19 Gbps.	Características Específicas do Firewall Tipo 2		
45	3.1.10.	O appliance deve possuir, no mínimo, 10 (dez) portas 100/1000/10000 BASE-T ou SFP podendo ser uma composição entre os dois tipos, acompanhadas de seus respectivos transceivers.	Características Específicas do Firewall Tipo 2	Para a Prova de Conceito, comprovar somente a quantidade das referidas interfaces.	
46	3.1.11.	Deve possuir, no mínimo, 5 (cinco) interfaces 10 (dez) Gigabit-Ethernet padrão SFP+, com transceivers SFP+ 10GB-SR, para conexão ao meio via cabo de fibra ótica.	Características Específicas do Firewall Tipo 2	Para a Prova de Conceito, comprovar somente a quantidade das referidas interfaces.	
47	3.1.13.	Deve possuir, no mínimo, 5 (cinco) interfaces 1 (um) Gigabit-Ethernet padrão SFP, para conexão ao meio via cabo de fibra ótica.	Características Específicas do Firewall Tipo 2	Para a Prova de Conceito, comprovar somente a quantidade das referidas interfaces.	
48	3.1.14.	Deve possuir, no mínimo, 4 (quatro) interfaces 25 (vinte e cinco) Gigabit-Ethernet padrão SFP28.	Características Específicas do Firewall Tipo 2	Para a Prova de Conceito, comprovar somente a quantidade das referidas interfaces.	
CONSOLE DE GERENCIAMENTO CENTRALIZADO PARA O FIREWALL TIPO 2 COM GARANTIA DE 60 MESES					
Nº	**REF. ANEXO I**	**DESCRIÇÃO DO ITEM PARA COMPROVAÇÃO**	**CONTEXTO DO REQUISITO**	**OBSERVAÇÃO**	**REQUISITO APROVADO? (SIM/NÃO)**
49	1.2.1.2.	Deve ser acessada via interface web ou através de um software cliente, com interface gráfica, instalado no Windows ou Linux;	Características Gerais das Consoles (Manager)		
50	1.2.1.9.	Deve permitir a criação e distribuição de políticas de segurança de forma centralizada, suportando organização hierárquica de regras.	Características Gerais das Consoles (Manager)		
51	1.2.1.11.	Deve ser capaz de gerenciar os firewalls em unidades remotas, fora da rede local.	Características Gerais das Consoles (Manager)		
52	1.2.1.12.	Deve permitir a autenticação dos administradores através de contas locais e bases externas LDAP ou Active Directory.	Características Gerais das Consoles (Manager)		
53	1.2.1.14.	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.	Características Gerais das Consoles (Manager)		
54	1.2.1.19.	Deve registrar, em log de auditoria, as ações dos usuários administradores com o horário da alteração.	Características Gerais das Consoles (Manager)		
55	1.2.1.25.	Deve ser capaz de testar a conectividade dos	Características Gerais das Consoles (Manager)		

		equipamentos gerenciados.			
56	1.2.1.26.	Deve suportar configuração das funcionalidades de alta disponibilidade dos dispositivos físicos.	Características Gerais das Consoles (Manager)		
57	1.2.1.27.	Deve permitir localizar em quais regras um objeto está sendo utilizado.	Características Gerais das Consoles (Manager)		
58	1.2.1.30.	Deve informar a utilização dos recursos de CPU, memória e atividade de rede dos equipamentos gerenciados.	Características Gerais das Consoles (Manager)		
CONSOLE DE GERENCIAMENTO DE LOGS PARA O FIREWALL TIPO 2 COM GARANTIA DE 60 MESES					
Nº	**REF. ANEXO I**	**DESCRIÇÃO DO ITEM PARA COMPROVAÇÃO**	**CONTEXTO DO REQUISITO**	**OBSERVAÇÃO**	**REQUISITO APROVADO? (SIM/NÃO)**
59	1.2.2.6.	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.	Características Gerais das Consoles (Logs)		
60	1.2.2.12.	Deve estar licenciada e permitir a correlação de todos os eventos gerados por todos os equipamentos e contextos virtuais que compõem a solução.	Características Gerais das Consoles (Logs)		
61	1.2.2.15.	Deve ser acessada via interface web ou através de um software cliente, com interface gráfica, instalado no Windows ou Linux	Características Gerais das Consoles (Logs)		
CONSOLE DE RELATORIA CENTRALIZADA PARA O FIREWALL TIPO 2 COM GARANTIA DE 60 MESES					
Nº	**REF. ANEXO I**	**DESCRIÇÃO DO ITEM PARA COMPROVAÇÃO**	**CONTEXTO DO REQUISITO**	**OBSERVAÇÃO**	**REQUISITO APROVADO? (SIM/NÃO)**
62	1.2.3.2.	Deve ser acessada via interface web ou através de um software cliente, com interface gráfica, instalado no Windows ou no Linux.	Características Gerais das Consoles (Relatórios)		
63	1.2.3.6.	Deve ser capaz de gerar relatórios de equipamentos em unidades remotas, fora da rede local.	Características Gerais das Consoles (Relatórios)		
64	1.2.3.12.	Possuir relatórios pré-definidos.	Características Gerais das Consoles (Relatórios)		
65	1.2.3.13.	Permitir a geração de relatórios de logs de tráfego de dados.	Características Gerais das Consoles (Relatórios)		
66	1.2.3.14.	Permitir a geração de relatórios de logs para auditoria das configurações de regras, objetos e acessos.	Características Gerais das Consoles (Relatórios)		
67	1.2.3.15.	Possibilitar o envio de maneira automática de relatórios por e-mail.	Características Gerais das Consoles (Relatórios)		
68	1.2.3.17.	Ter a capacidade de definir filtros nos relatórios.	Características Gerais das Consoles (Relatórios)		
69	1.2.3.20.	Possibilitar a visualização na interface gráfica de usuário (gui) da “console de relatoria centralizada as seguintes informações do sistema: logs diários recebidos, alertas gerados, entre outros.	Características Gerais das Consoles (Relatórios)		

Rio de Janeiro, 04 de junho de 2024

Documento assinado eletronicamente por **Isabela Reboucas Costa**, **Analista de Sistemas**, em 06/06/2024, às 16:05, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Manuelito de Sousa Reis Junior**, **Gerente**, em 06/06/2024, às 16:27, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Monique Goncalves Paz**, **Diretora**, em 06/06/2024, às 16:30, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Fabio Ivo**, **Assistente**, em 06/06/2024, às 16:51, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Rosana Alves de Andrade**, **Analista de Sistemas**, em 06/06/2024, às 17:00, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Charles Monteiro Guimarães**, **Diretor**, em 06/06/2024, às 17:22, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Cristina da Silva Barros Drongitis**, **Assessora Chefe**, em 26/08/2024, às 12:51, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

A autenticidade deste documento pode ser conferida no site http://sei.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **75936978** e o código CRC **BB3AD5FA**.

Rua da Conceição, 69, 24º Andar / 25º Andar - Bairro Centro, Rio de Janeiro/RJ, CEP 20051-011
Telefone:

Governo do Estado do Rio de Janeiro

Centro de Tecnologia de Informação e Comunicação do Estado do Rio de Janeiro

Vice Presidência de Tecnologia

ANEXO IV DO ESTUDO TÉCNICO PRELIMINAR
Roteiro para Prova de Conceito - lote 03
firewall tipo 03

1. INTRODUÇÃO

1.1. Será realizado a Prova de Conceito com o objetivo de verificar o atendimento dos requisitos funcionais considerados prioritários pelo PRODERJ, referente à proposta ofertada pela licitante classificada em primeiro lugar.

1.2. O roteiro da Prova de Conceito, nos termos que seguem abaixo, exigirá da referida licitante a comprovação de que sua solução atende as especificações de maior relevância aqui elencadas.

1.3. As especificações selecionadas neste anexo representam as características de maior impacto em relação à solução como um todo, e levam em consideração os aspectos técnicos que permitem comprovação em ambiente de teste, haja vista que determinados recursos/características/funcionalidades possuem restrições de comprovação quando a solução ainda não está completamente implementada.

1.4. Este anexo deve ser interpretado conforme as disposições do Estudo Técnico Preliminar (75936299) do qual é parte integrante e indissociável.

2. CARACTERÍSTICAS E FUNCIONALIDADES A SEREM COMPROVADAS

LOTE 3 - FIREWALL (TIPO 3)					
APPLIANCE FIREWALL TIPO 3 - INCLUSOS: HARDWARE, LICENCIAMENTO, INSTALAÇÃO, CONFIGURAÇÃO E GARANTIA POR 60 MESES					
Nº	**REF. ANEXO I**	**DESCRIÇÃO DO ITEM PARA COMPROVAÇÃO**	**CONTEXTO DO REQUISITO**	**OBSERVAÇÃO**	**REQUISITO APROVADO? (SIM/NÃO)**
1	1.1.4.3.	Deve permitir o acesso ao equipamento via SSH e interface web HTTPS.	Funcionalidades Básicas		
2	1.1.4.6.	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.	Funcionalidades Básicas		
3	1.1.4.10.	Os Firewalls de segurança físico ou virtualizados, devem possuir mecanismo para dedicar processamento no equipamento de segurança para funções e ações de Gerenciamento, mesmo que o equipamento esteja com alto processamento de CPU.	Funcionalidades Básicas		
4	1.1.5.3.	Deve suportar os protocolos DHCP e DHCPv6 e suas funcionalidades como cliente, servidor e relay.	Rede		
5	1.1.5.4.	Deve suportar Jumbo Frames.	Rede		
6	1.1.5.5.	Deve suportar sub interfaces Ethernet lógicas.	Rede		
7	1.1.5.8.	Deve permitir o registro de eventos de NAT com as informações de endereço interno, endereço público, data e hora do evento, portas de origem e destino.	Rede		

8	1.1.5.10.	Deve suportar as funcionalidades de roteamento estático e dinâmico em IPv4 e IPv6.	Rede		
9	1.1.5.16.	Deve suportar Policy Based Routing (PBR), possibilitando políticas de roteamento condicionado ao endereço IP de origem, endereço IP de destino e porta de comunicação.	Rede		
10	1.1.6.1.	Deve promover a integração com serviços de diretório LDAP e Active Directory, baseados em caracteres da língua portuguesa, para a identificação, autenticação, autorização e registro de eventos de acessos ou ameaças.	Autentificação e Identificação		
11	1.1.6.7.	Deve permitir a criação de políticas de segurança baseadas em usuários e grupos de usuários pertencentes a um diretório LDAP ou ao Active Directory.	Autentificação e Identificação		
12	1.1.6.10.	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.	Autentificação e Identificação		
13	1.1.7.1.	Deve identificar os países de origem e destino de todas as conexões estabelecidas através do equipamento.	Geolocalização		
14	1.1.7.4.	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.	Geolocalização		
15	1.1.7.5.	Deve possibilitar a visualização dos países de origem e destino nos logs de eventos de acessos e ameaças.	Geolocalização		
16	1.1.8.6.	Deve suportar Certificado Digital X.509.	VPN	Não precisa implementar certificado, basta mostrar as opções na manager.	
17	1.1.8.9.	Deve suportar VPN IPSec client-to-site (acesso remoto).	VPN		
18	1.1.8.11.	Deve permitir que o usuário realize a conexão VPN por meio de cliente instalado nos sistemas operacionais Windows, Mac OS ou Linux do seu equipamento ou então por meio de interface web do tipo portal.	VPN	No teste, a licitante precisará demonstrar este tópico apenas no Windows.	
19	1.1.8.15.	Deve suportar, no mínimo, os protocolos de roteamento estático e dinâmico OSPF e BGP.	VPN		

20	1.1.8.20.	Deve promover a integração com diretórios LDAP e Active Directory para a autenticação de usuários de VPN e regras de acesso.	VPN		
21	1.1.8.25.	Deve permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis de SSL.	VPN		
22	1.1.9.2.	Deve suportar a criação de políticas de controle de uso de largura de banda baseadas em: porta ou protocolo, endereço IP de origem ou destino, usuário ou grupo de usuários, aplicações (por exemplo, Youtube e WhatsApp).	QoS		
23	1.1.9.5.	Deve permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário.	QoS		
24	1.1.10.5.	Os valores dos parâmetros jitter e latência devem poder ser configurados em unidade mínima de milissegundos (ms).	Balanceamento de Links		
25	1.1.10.10.	Deve possuir roteamento baseado em políticas e múltiplas saídas (e tipos de saídas) WANs.	Balanceamento de Links		
26	1.1.10.12.	Deve suportar a configuração de regras que permita o failback imediato.	Balanceamento de Links	A licitante poderá demonstrar apenas as configurações na manager.	
27	1.1.11.3.	Deve aplicar novas políticas de segurança sem provocar indisponibilidade de serviço ou descontinuidade das conexões ativas.	Recursos de Segurança		
28	1.1.11.12.	Deve possuir funcionalidade de backup e restore da configuração e das políticas de segurança.	Recursos de Segurança		
29	1.1.10.15.	Deve possuir a capacidade de emular um ambiente operacional isolado e seguro (Sandbox), na nuvem do fabricante, para execução e observação de código malicioso, sem a utilização de assinaturas, com base na atividade, como, por exemplo, operações de arquivo, alterações de registro e sistema etc.	Recursos de Segurança		
30	1.1.12.5.	Deve suportar controle de acesso para pelo menos serviços e protocolos pré-definidos, bem como possibilitar a adição de novos serviços e protocolos.	Filtro de Pacotes		
31	1.1.12.9.	Deve identificar os usuários para qualquer protocolo ou aplicação baseada em TCP, UDP e ICMP.	Filtro de Pacotes		

32	1.1.12.11.	Deve suportar a implementação de políticas de segurança baseadas em: portas, protocolos, usuários, grupos de usuários, endereços IP, redes CIDR/VLSM, horário ou período de tempo, e suas combinações.	Filtro de Pacotes		
33	1.1.12.12.	Deve suportar a consulta a fontes externas de endereços IP, domínios e URL's podendo ser adicionados nas políticas de firewall para bloqueio ou permissão do tráfego.	Filtro de Pacotes		
34	1.1.13.9.	Deve classificar as aplicações em categorias.	Filtro de Conteúdo		
35	1.1.13.11.	Deve identificar os usuários que estão utilizando as aplicações.	Filtro de Conteúdo		
36	1.1.13.21.	Deve permitir a inclusão de URLs customizadas por política (whitelist).	Filtro de Conteúdo		
37	1.1.13.24.	Deve suportar a implementação de políticas de segurança baseadas em: URLs, categorias de URLs, endereço IP de origem ou destino, rede CIDR/VLSM de origem ou destino, usuário ou grupo de usuários, horário ou período de tempo, e suas combinações.	Filtro de Conteúdo		
38	1.1.13.25.	Deve alertar o usuário quando uma URL for bloqueada, por meio de página de bloqueio que possa ser customizada, e que informe, no mínimo, o motivo do bloqueio e a categoria na qual a URL foi classificada.	Filtro de Conteúdo		
39	1.1.13.27.	Deve permitir registrar todos os acessos autorizados ou bloqueados às páginas web, incluindo sua classificação e o usuário identificado.	Filtro de Conteúdo		
40	1.1.14.5.	Deve ser capaz de inspecionar tráfego criptografado usando SSL.	Prevenção de Intrusão - IPS		
41	1.1.14.9.	Deve permitir a criação de políticas de segurança que alertem, sem bloquear, sobre a ocorrência de um determinado ataque ou ameaça.	Prevenção de Intrusão - IPS		
42	1.1.14.14.	Deve bloquear malwares e spywares.	Prevenção de Intrusão - IPS		

43	4.1.1.	Throughput de 2 Gbps com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação IPS, Antivírus e Antispyware. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito.	Características Específicas do Firewall Tipo 3		
44	4.1.2.	Em relação ao filtro de pacotes, deve possuir o Throughput de no mínimo 4 Gbps.	Características Específicas do Firewall Tipo 3		
45	4.1.10.	O appliance deve possuir, no mínimo, 08 (oito) portas de rede 1G RJ-45.	Características Específicas do Firewall Tipo 3	Para a Prova de Conceito, comprovar somente a quantidade das referidas interfaces.	
46	4.1.11.	O appliance deve possuir uma porta 10/100/1000 para gerenciamento "out-of-band".	Características Específicas do Firewall Tipo 3	Para a Prova de Conceito, comprovar somente a quantidade das referidas interfaces.	
CONSOLE DE GERENCIAMENTO CENTRALIZADO PARA O FIREWALL TIPO 3 COM GARANTIA DE 60 MESES					
Nº	**REF. ANEXO I**	**DESCRIÇÃO DO ITEM PARA COMPROVAÇÃO**	**CONTEXTO DO REQUISITO**	**OBSERVAÇÃO**	**REQUISITO APROVADO? (SIM/NÃO)**
47	1.2.1.2.	Deve ser acessada via interface web ou através de um software cliente, com interface gráfica, instalado no Windows ou Linux;	Características Gerais das Consoles (Manager)		
48	1.2.1.9.	Deve permitir a criação e distribuição de políticas de segurança de forma centralizada, suportando organização hierárquica de regras.	Características Gerais das Consoles (Manager)		
49	1.2.1.11.	Deve ser capaz de gerenciar os firewalls em unidades remotas, fora da rede local.	Características Gerais das Consoles (Manager)		
50	1.2.1.12.	Deve permitir a autenticação dos administradores através de contas locais e bases externas LDAP ou Active Directory.	Características Gerais das Consoles (Manager)		
51	1.2.1.14.	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.	Características Gerais das Consoles (Manager)		
52	1.2.1.19.	Deve registrar, em log de auditoria, as ações dos usuários administradores com o horário da alteração.	Características Gerais das Consoles (Manager)		
53	1.2.1.25.	Deve ser capaz de testar a conectividade dos equipamentos gerenciados.	Características Gerais das Consoles (Manager)		
54	1.2.1.26.	Deve suportar configuração das funcionalidades de alta disponibilidade dos dispositivos físicos.	Características Gerais das Consoles (Manager)		
55	1.2.1.27.	Deve permitir localizar em quais regras um objeto está sendo utilizado.	Características Gerais das Consoles (Manager)		
56	1.2.1.30.	Deve informar a utilização dos recursos de CPU,	Características Gerais das Consoles (Manager)		

		memória e atividade de rede dos equipamentos gerenciados.			
CONSOLE DE GERENCIAMENTO DE LOGS PARA O FIREWALL TIPO 3 COM GARANTIA DE 60 MESES					
Nº	**REF. ANEXO I**	**DESCRIÇÃO DO ITEM PARA COMPROVAÇÃO**	**CONTEXTO DO REQUISITO**	**OBSERVAÇÃO**	**REQUISITO APROVADO? (SIM/NÃO)**
57	1.2.2.6.	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.	Características Gerais das Consoles (Logs)		
58	1.2.2.12.	Deve estar licenciada e permitir a correlação de todos os eventos gerados por todos os equipamentos e contextos virtuais que compõem a solução.	Características Gerais das Consoles (Logs)		
59	1.2.2.15.	Deve ser acessada via interface web ou através de um software cliente, com interface gráfica, instalado no Windows ou Linux	Características Gerais das Consoles (Logs)		
CONSOLE DE RELATORIA CENTRALIZADA PARA O FIREWALL TIPO 3 COM GARANTIA DE 60 MESES					
Nº	**REF. ANEXO I**	**DESCRIÇÃO DO ITEM PARA COMPROVAÇÃO**	**CONTEXTO DO REQUISITO**	**OBSERVAÇÃO**	**REQUISITO APROVADO? (SIM/NÃO)**
60	1.2.3.2.	Deve ser acessada via interface web ou através de um software cliente, com interface gráfica, instalado no Windows ou no Linux.	Características Gerais das Consoles (Relatórios)		
61	1.2.3.6.	Deve ser capaz de gerar relatórios de equipamentos em unidades remotas, fora da rede local.	Características Gerais das Consoles (Relatórios)		
62	1.2.3.12.	Possuir relatórios pré-definidos.	Características Gerais das Consoles (Relatórios)		
63	1.2.3.13.	Permitir a geração de relatórios de logs de tráfego de dados.	Características Gerais das Consoles (Relatórios)		
64	1.2.3.14.	Permitir a geração de relatórios de logs para auditoria das configurações de regras, objetos e acessos.	Características Gerais das Consoles (Relatórios)		
65	1.2.3.15.	Possibilitar o envio de maneira automática de relatórios por e-mail.	Características Gerais das Consoles (Relatórios)		
66	1.2.3.17.	Ter a capacidade de definir filtros nos relatórios.	Características Gerais das Consoles (Relatórios)		
67	1.2.3.20.	Possibilitar a visualização na interface gráfica de usuário (gui) da “console de relatoria centralizada as seguintes informações do sistema: logs diários recebidos, alertas gerados, entre outros.	Características Gerais das Consoles (Relatórios)		

Rio de Janeiro, 04 de junho de 2024

Documento assinado eletronicamente por **Isabela Reboucas Costa**, **Analista de Sistemas**, em 06/06/2024, às 16:06, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Manuelito de Sousa Reis Junior**, **Gerente**, em 06/06/2024, às 16:27, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Monique Goncalves Paz**, **Diretora**, em 06/06/2024, às 16:30, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Fabio Ivo**, **Assistente**, em 06/06/2024, às 16:52, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Rosana Alves de Andrade**, **Analista de Sistemas**, em 06/06/2024, às 17:02, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Charles Monteiro Guimarães**, **Diretor**, em 06/06/2024, às 17:22, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Cristina da Silva Barros Drongitis**, **Assessora Chefe**, em 26/08/2024, às 12:51, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

A autenticidade deste documento pode ser conferida no site http://sei.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **75936561** e o código CRC **1865A9B5**.

Rua da Conceição, 69, 24º Andar / 25º Andar - Bairro Centro, Rio de Janeiro/RJ, CEP 20051-011
Telefone:

Governo do Estado do Rio de Janeiro

Centro de Tecnologia de Informação e Comunicação do Estado do Rio de Janeiro

Diretoria de Segurança da Informação

ANEXO V DO ESTUDO TÉCNICO PRELIMINAR
MAPA DE RISCOS

1. OBJETO

1.1. A análise dos riscos pretende identificar, avaliar e adotar respostas aos eventos de riscos do modelo de contratação proposto, de forma a assegurar o alcance do objetivo da contratação, por meio da identificação antecipada dos possíveis eventos que poderiam ameaçar o processo licitatório, a execução contratual, o cumprimento das obrigações contratuais, etc.

1.2. Este anexo deve ser interpretado conforme as disposições do Estudo Técnico Preliminar (75936299) do qual é parte integrante e indissociável.

2. IDENTIFICAÇÃO E ANÁLISE DOS PRINCIPAIS RISCOS

2.1. No escopo da presente contratação, foram identificados os riscos inerentes ao negócio, os passíveis de comprometer o êxito do processo de contratação e os referentes à gestão contratual.

2.2. Cada risco identificado foi enquadrado conforme seu tipo (infraestrutura, segurança ou organizacional), considerando-se a probabilidade de ocorrência dos eventos, os possíveis danos potenciais em caso de acontecimentos, as possíveis ações preventivas e de contingências, bem como a identificação de responsáveis por ação. Para tanto, tais riscos foram classificados a partir da atribuição de valores aos níveis de probabilidade (P) e impacto (I), conforme tabela abaixo:

Escala Qualitativa de Classificação	
Classificação	**Valor**
Baixo	5
Médio	10
Alto	15

2.3. Em seguida, o produto obtido da relação entre a probabilidade e o impacto resultou na elaboração da Matriz Probabilidade x Impacto, instrumento responsável pela definição dos critérios quantitativos de classificação do nível de risco, a fim de direcionar as ações relacionadas aos riscos durante a fase de planejamento e gestão do contrato.

Probabilidade (P)	15	75	150	225
	10	50	100	150
	5	25	50	75
Impacto (I)		5	10	15

2.4. Caso o risco se enquadre na região verde, seu nível de risco é entendido como baixo, logo, admite-se sua aceitação ou adoção das medidas preventivas, por meio do uso de controles de segurança. Se estiver na região amarela, entende-se como médio; e se estiver na região vermelha, entende-se como nível de risco alto. Nos casos de riscos classificados como médio e alto, deve-se adotar obrigatoriamente os controles de segurança previstos.

2.5. Uma vez definidos os riscos e seus níveis, indicou-se a resposta de ação correspondente a cada um deles, de acordo com o quadro abaixo:

Respostas aos riscos	
Evitar	Eliminar o risco, evitando-o totalmente.
Mitigar	Reduzir a probabilidade e/ou o impacto do risco, ação realizada independente do risco ocorrer ou não.
Transferir	Passar o custo da consequência para um terceiro.
Aceitação Ativa	Criar um plano de contingência para ser acionado, caso o risco ocorra.
Aceitação Passiva	Não tomar nenhuma ação preventiva, lidando com o problema apenas caso o risco ocorra.

2.6. A partir do percurso metodológico descrito, foram identificados os seguintes riscos:

Tabela de relação de riscos identificados						
Id	**Risco**	**Tipo de Risco**	**Probabilidade**	**Impacto**	**Nível de Risco (P X I)**	**Respostas aos Riscos**
R1	Não Indicação de servidores pelas áreas envolvidas no processo de aquisição para compor a Equipe de Planejamento da Contratação para elaborar a documentação necessária	infraestrutura	baixa (5)	alto (15)	75	Aceitação Ativa
R2	Levantamento inadequado dos itens	infraestrutura	baixa (5)	alto (15)	75	Aceitação Ativa
R3	Edital e Termo de Referência incompletos ou inconsistentes	organizacional	baixa (5)	alto (15)	75	Aceitação Ativa
R4	Insuficiência de recursos orçamentários para contratação dos serviços	organizacional	baixa (5)	alto (15)	75	Aceitação Ativa
R5	Não autorização de despesa para a contratação	infraestrutura / organizacional	baixa (5)	alto (15)	75	Aceitação Ativa
R6	Erro na pesquisa das quantidades necessárias para a licitação	infraestrutura	média (10)	alto (15)	150	Aceitação Ativa / Mitigar
R7	Demora na conclusão do processo licitatório, ocasionando atrasos na homologação e consequente contratação	infraestrutura / organizacional	baixa (5)	alto (15)	75	Aceitação Ativa
R8	Recusa do licitante vencedor em assinar o contrato	infraestrutura / organizacional	baixa (5)	alto (15)	75	Aceitação Ativa
R9	Atraso na entrega dos equipamentos (itens do objeto contratado)	infraestrutura	baixa (5)	alto (15)	75	Aceitação Ativa
R10	Paralisação dos sistemas em produção após instalação da solução.	infraestrutura	média (10)	alto (15)	150	Aceitação Ativa / Mitigar
R11	Exclusão da DSI quanto ao estabelecimento das políticas e regras para a configuração da solução	segurança	baixa (5)	alto (15)	75	Aceitação Ativa
R12	Quantitativo de pessoal ou capacitação insuficiente dos agentes de fiscalização e gestão do contrato	organizacional	baixa (5)	alto (15)	75	Aceitação Ativa
R13	Contratada fornecer bem fora dos padrões pretendidos	infraestrutura	baixa (5)	alto (15)	75	Aceitação Ativa
R14	Falência, insolvência, quebra contratual pela contratada	infraestrutura / organizacional	baixa (5)	alto (15)	75	Aceitação Ativa
R15	Falta de disponibilidade financeira para pagamento de despesa no prazo	infraestrutura / organizacional	baixa (5)	alto (15)	75	Aceitação Ativa
R16	Não aplicação de sanções à contratada pela Administração	organizacional	baixa (5)	alto (15)	75	Aceitação Ativa

3. IDENTIFICAÇÃO E ANÁLISE DOS PRINCIPAIS RISCOS

Em atendimento ao art. 38, II e III da IN SGD/ME nº 01/2019.

RISCO 1			
Não Indicação de servidores pelas áreas envolvidas no processo de aquisição para compor a Equipe de Planejamento da Contratação para elaborar a documentação necessária.			
Probabilidade:	(x) Baixa	( ) Média	( ) Alta
Impacto:	( ) Baixa	( ) Média	(x) Alta
Fase Impactada:	(x) Fase Preparatória ( ) Seleção do Fornecedor ( ) Gestão do Contrato		
Id	**Dano**		
1.1.	Atraso na contratação;		
	Contratação em desacordo com a necessidade da Administração.		
Id	**Ação Preventiva**		**Responsável**
1.1.1.	Designar pessoal das áreas envolvidas na contratação para a composição da equipe de planejamento da contratação.		Diretores das Áreas Envolvidas
Id	**Ação de Contingência**		**Responsável**
1.1.2.	Refazer a documentação de acordo com a necessidade da Administração.		Equipe de Planejamento da Contratação

RISCO 2			
Levantamento inadequado dos itens.			
Probabilidade:	(x) Baixa	( ) Média	( ) Alta
Impacto:	( ) Baixa	( ) Média	(x) Alta
Fase Impactada:	(x) Fase Preparatória ( ) Seleção do Fornecedor ( ) Gestão do Contrato		
Id	**Dano**		
2.1.	Não alcançar todas as necessidades e resultados pretendidos.		
Id	**Ação Preventiva**		**Responsável**
2.1.1.	Verificar a eventual adequação das especificações por ocasião da elaboração do Termo de Referência.		Responsáveis pelo Termo de Referência
Id	**Ação de Contingência**		**Responsável**
2.1.2.	Verificar a documentação já utilizada por outros Órgãos recentemente.		Responsáveis pelo Termo de Referência

RISCO 3			
Edital e Termo de Referência incompletos ou inconsistentes.			
Probabilidade:	(x) Baixa	( ) Média	( ) Alta
Impacto:	( ) Baixa	( ) Média	(x) Alta
Fase Impactada:	(x) Fase Preparatória ( ) Seleção do Fornecedor ( ) Gestão do Contrato		
Id	**Dano**		
3.1.	Licitação fracassada; Contratação em desacordo com a necessidade da Administração; Prejuízo ao erário		
Id	**Ação Preventiva**		**Responsável**
3.1.1.	Revisar cuidadosamente o Edital e o Termo de Referência, de modo a verificar suas adequações.		Equipe de Planejamento da Contratação, GEA
Id	**Ação de Contingência**		**Responsável**
3.1.2.	Revogar ou anular o processo de licitação.		VPT / VPA

RISCO 4			
Insuficiência de recursos orçamentários para contratação dos serviços.			
Probabilidade:	(x) Baixa	( ) Média	( ) Alta
Impacto:	( ) Baixa	( ) Média	(x) Alta
Fase Impactada:	(x) Fase Preparatória ( ) Seleção do Fornecedor ( ) Gestão do Contrato		
Id	**Dano**		
4.1.	Inviabilidade de execução contratual.		
Id	**Ação Preventiva**		**Responsável**
4.1.1.	Prever recursos necessários no orçamento anual.		DOF
Id	**Ação de Contingência**		**Responsável**
4.1.2.	Readequar a contratação à capacidade orçamentária disponível.		Equipe de Planejamento da Contratação

RISCO 5			
Não autorização de despesa para a contratação			
Probabilidade:	(x) Baixa	( ) Média	( ) Alta
Impacto:	( ) Baixa	( ) Média	(x) Alta
Fase Impactada:	(x) Fase Preparatória ( ) Seleção do Fornecedor ( ) Gestão do Contrato		
Id	**Dano**		
5.1.	Inviabilidade de execução contratual.		
Id	**Ação Preventiva**		**Responsável**
5.1.1.	Prever recursos necessários no orçamento anual.		DOF
Id	**Ação de Contingência**		**Responsável**
5.1.2.	Readequar a contratação à capacidade orçamentária disponível.		Equipe de Planejamento da Contratação

RISCO 6		
Erro na pesquisa das quantidades necessárias para a licitação.		
Probabilidade:	( ) Baixa (x) Média	( ) Alta
Impacto:	( ) Baixa ( ) Média	(x) Alta
Fase Impactada:	(x) Fase Preparatória ( ) Seleção do Fornecedor ( ) Gestão do Contrato	

Id	Dano	
6.1	Impedimento da contratação por erro nos quantitativos.	
Id	**Ação Preventiva**	**Responsável**
6.1.1	Melhorar a pesquisa junto aos Órgãos e Secretarias do Estado do Rio de Janeiro.	GEA
Id	**Ação de Contingência**	**Responsável**
6.1.2	Revogar ou anular o processo de licitação.	VPA

RISCO 7			
Demora na conclusão do processo licitatório, ocasionando atrasos na homologação e consequente contratação.			
Probabilidade:	(x) Baixa	( ) Média	( ) Alta
Impacto:	( ) Baixa	( ) Média	(x) Alta
Fase Impactada:	( ) Fase Preparatória (x) Seleção do Fornecedor ( ) Gestão do Contrato		
Id	**Dano**		
7.1.	Atraso na contratação.		
Id	**Ação Preventiva**		**Responsável**
7.1.1.	Designar pessoal capacitado e em quantidade suficiente para a condução do processo licitatório.		Presidente / VPA
Id	**Ação de Contingência**		**Responsável**
7.1.2.	Designar pessoal adicional para a condução do processo licitatório.		Presidente / VPA

RISCO 8			
Recusa do licitante vencedor em assinar o contrato			
Probabilidade:	(x) Baixa	( ) Média	( ) Alta
Impacto:	( ) Baixa	( ) Média	(x) Alta
Fase Impactada:	( ) Fase Preparatória ( ) Seleção do Fornecedor (x) Gestão do Contrato		
Id	**Dano**		
8.1.	Impossibilidade de iniciar a execução dos serviços.		
Id	**Ação Preventiva**		**Responsável**
8.1.1.	Verificar situações que possam ensejar a inexequibilidade contratual.		AJU
Id	**Ação de Contingência**		**Responsável**
8.1.2.	Refazer os procedimentos de contratação.		GGC / AJU

RISCO 9			
Atraso na entrega dos equipamentos (itens do objeto contratado)			
Probabilidade:	(x) Baixa	( ) Média	( ) Alta
Impacto:	( ) Baixa	( ) Média	(x) Alta
Fase Impactada:	( ) Fase Preparatória ( ) Seleção do Fornecedor (x) Gestão do Contrato		
Id	**Dano**		
9.1.	Ativos desprotegidos com maior risco de ciberataques aos sistemas do Governo do Estado.		
Id	**Ação Preventiva**		**Responsável**
9.1.1.	Comunicar ao fornecedor, três dias antes do prazo, e exigir celeridade na entrega, visto que o processo licitatório foi concluído.		Gestor do Contrato
Id	**Ação de Contingência**		**Responsável**
9.1.2.	Decidir sobre a realização da rescisão contratual.		VPT / VPA

RISCO 10			
Paralisação dos sistemas em produção após instalação da solução.			
Probabilidade:	( ) Baixa	(x) Média	( ) Alta
Impacto:	( ) Baixa	( ) Média	(x) Alta
Fase Impactada:	( ) Fase Preparatória ( ) Seleção do Fornecedor (x) Gestão do Contrato		
Id	**Dano**		
10.1.	Interromper o funcionamento de vários sistemas e serviços críticos no âmbito de vários órgãos do Governo do Estado do Rio de Janeiro.		
Id	**Ação Preventiva**		**Responsável**
10.1.1.	Planejar a instalação no ambiente de homologação para identificar possíveis intercorrências que a instalação da solução possa causar.		DIT
Id	**Ação de Contingência**		**Responsável**
10.1.2.	Desinstalar a solução;		DIT

	Comunicar o fornecedor em busca de uma solução para não gerar novo impacto na instalação.	Gestor do Contrato

RISCO 11			
Exclusão da DSI quanto ao estabelecimento das políticas e regras para a configuração da solução.			
Probabilidade:	(x) Baixa	( ) Média	( ) Alta
Impacto:	( ) Baixa	( ) Média	(x) Alta
Fase Impactada:	( ) Fase Preparatória ( ) Seleção do Fornecedor (x) Gestão do Contrato		
Id	**Dano**		
11.1.	Criação de políticas e regras que possam abrir vulnerabilidades no ambiente de rede a ser protegido.		
Id	**Ação Preventiva**		**Responsável**
11.1.1.	Solicitar que os setores competentes participem da criação das políticas e regras, de modo que sejam construídas conjuntamente entre as áreas de infraestrutura e segurança.		DIT
Id	**Ação de Contingência**		**Responsável**
11.1.2.	Refazer e implementar as políticas e regras da solução		DIT

Risco 12			
Quantitativo de pessoal ou capacitação insuficiente dos agentes de fiscalização e gestão do contrato.			
Probabilidade:	(x) Baixa	( ) Média	( ) Alta
Impacto:	( ) Baixa	( ) Média	(x) Alta
Fase Impactada:	( ) Fase Preparatória ( ) Seleção do Fornecedor (x) Gestão do Contrato		
Id	**Dano**		
12.1.	Falha no acompanhamento da execução contratual.		
Id	**Ação Preventiva**		**Responsável**
12.1.1.	Designar quantitativo de pessoal suficiente;		PRE
	Capacitação da equipe.		VPA
	Realizar reuniões periódicas para atualização dos procedimentos de fiscalização contratual e compartilhamento de informações		Comissão de Fiscalização
Id	**Ação de Contingência**		**Responsável**
12.1.2.	Atribuição das atividades de gestão e fiscalização do contrato a outros servidores que já estejam capacitados.		Equipe de Planejamento da Contratação

RISCO 13			
Contratada fornecer bem fora dos padrões pretendidos.			
Probabilidade:	(x) Baixa	( ) Média	( ) Alta
Impacto:	( ) Baixa	( ) Média	(x) Alta
Fase Impactada:	( ) Fase Preparatória ( ) Seleção do Fornecedor (x) Gestão do Contrato		
Id	**Dano**		
13.1.	Aquisição de uma solução de firewall abaixo das exigências técnicas definidas, acarretando danos ao erário		
Id	**Ação Preventiva**		**Responsável**
13.1.1.	Acompanhar e cobrar da contratada o fornecimento dos equipamentos contratados dentro dos padrões pretendidos. Não realizar o recebimento dos bens fora dos padrões pretendidos		Fiscais do Contrato
Id	**Ação de Contingência**		**Responsável**
13.1.2.	Notificar a contratada pelo descumprimento de obrigação contratual;		Gestor do Contrato
	Exigir a entrega de equipamentos em conformidade com o que foi disciplinado no Termo de Referência.		Gestor do Contrato

RISCO 14			
Falência, insolvência, quebra contratual pela contratada.			
Probabilidade:	(x) Baixa	( ) Média	( ) Alta
Impacto:	( ) Baixa	( ) Média	(x) Alta
Fase Impactada:	( ) Fase Preparatória ( ) Seleção do Fornecedor (x) Gestão do Contrato		
Id	**Dano**		
14.1.	Interrupção imediata do contrato		
Id	**Ação Preventiva**		**Responsável**
14.1.1.	Acompanhar as condições de habilitação da contratada, em especial quanto à qualificação econômico-financeira.		GGC
Id	**Ação de Contingência**		**Responsável**
14.1.2.	Reavaliar as empresas existentes no mercado para compra emergencial enquanto se elabora novo instrumento licitatório		GGC / DAF / GEA / DSI

RISCO 15			
Falta de disponibilidade financeira para pagamento de despesa no prazo			
Probabilidade:	(x) Baixa	( ) Média	( ) Alta
Impacto:	( ) Baixa	( ) Média	(x) Alta
Fase Impactada:	( ) Fase Preparatória ( ) Seleção do Fornecedor (x) Gestão do Contrato		
Id	**Dano**		
15.1.	Cometimento de ato ilegal; Prejuízo ao erário no caso de exigência por parte da contratada de pagamento em valor corrigido		
Id	**Ação Preventiva**		**Responsável**
15.1.1.	Obedecer à ordem de pagamentos conforme entrada no setor financeiro.		DOF / GOF
Id	**Ação de Contingência**		**Responsável**
15.1.2.	Solicitar repasse de recurso ao Tesouro para realizar pagamento no prazo.		DOF / GOF

RISCO 16			
Não aplicação de sanções à contratada pela Administração			
Probabilidade:	(x) Baixa	( ) Média	( ) Alta
Impacto:	( ) Baixa	( ) Média	(x) Alta
Fase Impactada:	( ) Fase Preparatória ( ) Seleção do Fornecedor (x) Gestão do Contrato		
Id	**Dano**		
16.1.	Prejuízo ao erário; Manutenção de empresa inadequada no mercado.		
Id	**Ação Preventiva**		**Responsável**
16.1.1.	Notificar a contratada por falhas na execução contratual.		GGC / Gestor do Contrato
Id	**Ação de Contingência**		**Responsável**
16.1.2.	Instaurar processo sancionador para eventual aplicação de sanção.		GGC / AJU

Rio de Janeiro, 04 de junho de 2024

Documento assinado eletronicamente por **Isabela Reboucas Costa**, **Analista de Sistemas**, em 06/06/2024, às 16:06, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Manuelito de Sousa Reis Junior**, **Gerente**, em 06/06/2024, às 16:28, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Monique Goncalves Paz**, **Diretora**, em 06/06/2024, às 16:31, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Fabio Ivo**, **Assistente**, em 06/06/2024, às 16:53, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Rosana Alves de Andrade**, **Analista de Sistemas**, em 06/06/2024, às 17:03, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Charles Monteiro Guimarães**, **Diretor**, em 06/06/2024, às 17:22, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Cristina da Silva Barros Drongitis**, **Assessora Chefe**, em 26/08/2024, às 12:51, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

A autenticidade deste documento pode ser conferida no site http://sei.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **75942352** e o código CRC **30D97DC3**.

Rua da Conceição, 69, 24º Andar / 25º Andar - Bairro Centro, Rio de Janeiro/RJ, CEP 20051-011
Telefone:

Governo do Estado do Rio de Janeiro

Centro de Tecnologia de Informação e Comunicação do Estado do Rio de Janeiro

Vice Presidência de Tecnologia

ANEXO VI DO ESTUDO TÉCNICO PRELIMINAR
MODELO DE RELATÓRIO DE CUMPRIMENTO DO OBJETO
(para atendimento do subtópico 13.9.1.1 do ETP)

obs: Este anexo deve ser interpretado conforme as disposições do Estudo Técnico Preliminar (75936299) do qual é parte integrante e indissociável.

(logo da empresa)

1. IDENTIFICAÇÃO			
Contrato nº			
Contratada		**CNPJ**	
nº da OS/OF		**Período de Referência**	

2. ESPECIFICAÇÃO DOS BENS/SERVIÇOS E VOLUMES DE ENTREGA/EXECUÇÃO					
Descrição do Objeto Contratado					
Item / Lote	**Descrição do bem ou serviço**	**Métrica**	**Quantidade**	**Valor Unitário**	**Valor Total**
				Valor Total	

3. OBSERVAÇÕES

4. ENCAMINHAMENTO
Por este instrumento, encaminhamos as informações e documentos comprobatórios dos serviços correspondentes à OS/OF acima identificada, conforme definido no Modelo de Execução do contrato supracitado, para que seja verificado o devido cumprimento dos requisitos e demais condições contratuais

5. PREPOSTO
_____ Nome CPF Local e Data

Rio de Janeiro, 04 de junho de 2024

Documento assinado eletronicamente por **Isabela Reboucas Costa**, **Analista de Sistemas**, em 06/06/2024, às 16:06, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Manuelito de Sousa Reis Junior**, **Gerente**, em 06/06/2024, às 16:28, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Monique Goncalves Paz**, **Diretora**, em 06/06/2024, às 16:31, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Fabio Ivo**, **Assistente**, em 06/06/2024, às 16:53, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Rosana Alves de Andrade**, **Analista de Sistemas**, em 06/06/2024, às 17:04, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Charles Monteiro Guimarães**, **Diretor**, em 06/06/2024, às 17:22, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Cristina da Silva Barros Drongitis**, **Assessora Chefe**, em 26/08/2024, às 12:51, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

A autenticidade deste documento pode ser conferida no site http://sei.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **75942000** e o código CRC **E1C60ED6**.

Rua da Conceição, 69, 24º Andar / 25º Andar - Bairro Centro, Rio de Janeiro/RJ, CEP 20051-011
Telefone:

Governo do Estado do Rio de Janeiro

Centro de Tecnologia de Informação e Comunicação do Estado do Rio de Janeiro

Vice Presidência de Tecnologia

ANEXO VII DO ESTUDO TÉCNICO PRELIMINAR

ORIENTAÇÃO AOS ÓRGÃOS PARTÍCIPES PARA O PREENCHIMENTO DA INTENÇÃO NO REGISTRO DE PREÇOS (IRP)

0.1. Este guia foi desenvolvido para orientar os órgãos e entidades da Administração Pública, interessados em participar do presente certame com Registro de Preços, no momento do preenchimento do questionário na fase de Intenção de Registro de Preços - IRP na plataforma de compras do governo do Estado.

0.2. Este anexo deve ser interpretado conforme as disposições do Estudo Técnico Preliminar (75936299) do qual é parte integrante e indissociável.

0.3. Para fins de quantificação de cada um dos itens componentes do objeto proposto, os órgãos interessados em participar deste Sistema de Registro de Preços devem observar as considerações constantes na tabela a seguir:

Lote 1 - Firewall (Tipo 1)					
item	**ID SIGA**	**Descrição**	**Justificativa**	**Métrica**	**Forma de Quantificação**
1	168256	APPLIANCE FIREWALL TIPO 1 - INCLUSOS: HARDWARE, LICENCIAMENTO, INSTALAÇÃO, CONFIGURAÇÃO E GARANTIA POR 60 MESES	Foi adotada a estratégia de oferecer 3 “tamanhos” diferentes de firewall. Este item corresponde ao equipamento de maior capacidade. Indicação de uso: Grandes Data Centers.	Unidade	Recomendamos, no mínimo, duas unidades por Contratante, por motivos de clusterização e/ou alta disponibilidade.
2	172443	CONSOLE DE GERENCIAMENTO CENTRALIZADO PARA O FIREWALL TIPO 1 COM GARANTIA DE 60 MESES	A depender da topologia que será implementada, o gerenciamento centralizado de vários equipamentos poderá ser necessário.	Unidade	Recomendamos, a depender da topologia, de uma a duas unidades da console.
3	172442	CONSOLE DE GERENCIAMENTO DE LOGS PARA O FIREWALL TIPO 1 COM GARANTIA DE 60 MESES	A depender da topologia a ser implementada, poderá ser necessário que os logs sejam armazenados e processados em um sistema apartado.	Unidade	Recomendamos ao menos uma unidade caso a Contratante tenha adquirido múltiplos equipamentos do “item 1”.
4	172444	CONSOLE DE RELATORIA CENTRALIZADA PARA O FIREWALL TIPO 1 COM GARANTIA DE 60 MESES	A depender da necessidade e do volume de informações e alertas geradas pela solução, pode ser necessária a segregação do sistema de relatoria.	Unidade	Recomendamos ao menos uma unidade caso a Contratante tenha adquirido múltiplos equipamentos do “item 1” deste lote.
5	180944	TREINAMENTO OPERACIONAL PARA A SOLUÇÃO DO LOTE 1	Serviço opcional de treinamento na solução. Recomendável, dada a complexidade da ferramenta.	Aluno / Vaga	Quantidade de alunos a serem treinados.

Lote 1 - Firewall (Tipo 2)					
item	**ID SIGA**	**Descrição**	**Justificativa**	**Métrica**	**Forma de Quantificação**
1	168257	APPLIANCE FIREWALL TIPO 2 - INCLUSOS: HARDWARE, LICENCIAMENTO, INSTALAÇÃO, CONFIGURAÇÃO E GARANTIA POR 60 MESES	Foi adotada a estratégia de oferecer 3 “tamanhos” diferentes de firewall. Este item corresponde ao equipamento capacidade intermediária. Indicação de uso: Links de internet com velocidade de até 7 gbps.	Unidade	Recomendamos, no mínimo, duas unidades por Contratante, por motivos de clusterização e/ou alta disponibilidade.
2	180938	CONSOLE DE GERENCIAMENTO CENTRALIZADO PARA O FIREWALL TIPO 2 COM GARANTIA DE 60 MESES	A depender da topologia que será implementada, o gerenciamento centralizado de vários equipamentos poderá ser necessário.	Unidade	Recomendamos, a depender da topologia, de uma a duas unidades da console.
3	180940	CONSOLE DE GERENCIAMENTO DE LOGS PARA O FIREWALL TIPO 2 COM GARANTIA DE 60 MESES	A depender da topologia a ser implementada, poderá ser necessário que os logs sejam armazenados e processados em um sistema apartado.	Unidade	Recomendamos ao menos uma unidade caso a Contratante tenha adquirido múltiplos equipamentos do “item 1” deste lote.
4	180942	CONSOLE DE RELATORIA CENTRALIZADA PARA O FIREWALL TIPO 2 COM GARANTIA DE 60 MESES	A depender da necessidade e do volume de informações e alertas geradas pela solução, pode ser necessária a segregação do sistema de relatoria.	Unidade	Recomendamos ao menos uma unidade caso a Contratante tenha adquirido múltiplos equipamentos do “item 1”.
5	180945	TREINAMENTO OPERACIONAL PARA A SOLUÇÃO DO LOTE 2	Serviço opcional de treinamento na solução. Recomendável, dada a complexidade da ferramenta.	Aluno / Vaga	Quantidade de alunos a serem treinados.

Lote 1 - Firewall (Tipo 3)					
item	**ID SIGA**	**Descrição**	**Justificativa**	**Métrica**	**Forma de Quantificação**
1	168258	APPLIANCE FIREWALL TIPO 3 - INCLUSOS: HARDWARE, LICENCIAMENTO, INSTALAÇÃO, CONFIGURAÇÃO E GARANTIA POR 60 MESES	Foi adotada a estratégia de oferecer 3 “tamanhos” diferentes de firewall. Este item corresponde ao equipamento de menor capacidade. Indicação de uso: Links de internet com velocidade de até 2 gbps.	Unidade	Recomendamos, no mínimo, duas unidades por Contratante, por motivos de clusterização e/ou alta disponibilidade.
2	180939	CONSOLE DE GERENCIAMENTO CENTRALIZADO PARA O FIREWALL TIPO 3 COM GARANTIA DE 60 MESES	A depender da topologia que será implementada, o gerenciamento centralizado de vários equipamentos poderá ser necessário.	Unidade	Recomendamos, a depender da topologia, de uma a duas unidades da console.
3	180941	CONSOLE DE GERENCIAMENTO DE LOGS PARA O FIREWALL TIPO 3 COM GARANTIA DE 60 MESES	A depender da topologia a ser implementada, poderá ser necessário que os logs sejam armazenados e processados em um sistema apartado.	Unidade	Recomendamos ao menos uma unidade caso a Contratante tenha adquirido múltiplos equipamentos do “item 1” deste lote.

4	180943	CONSOLE DE RELATORIA CENTRALIZADA PARA O FIREWALL TIPO 3 COM GARANTIA DE 60 MESES	A depender da necessidade e do volume de informações e alertas geradas pela solução, pode ser necessária a segregação do sistema de relatoria.	Unidade	Recomendamos ao menos uma unidade caso a Contratante tenha adquirido múltiplos equipamentos do "item 1" deste lote.
5	180946	TREINAMENTO OPERACIONAL PARA A SOLUÇÃO DO LOTE 3	Serviço opcional de treinamento na solução. Recomendável, dada a complexidade da ferramenta.	Aluno / Vaga	Quantidade de alunos a serem treinados.

CONTATO:

Em caso de dúvidas o órgão interessado poderá entrar em contato com o PRODERJ através do e-mail dsi@proderj.rj.gov.br

Rio de Janeiro, 04 de junho de 2024

Documento assinado eletronicamente por **Isabela Reboucas Costa**, **Analista de Sistemas**, em 06/06/2024, às 16:06, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Manuelito de Sousa Reis Junior**, **Gerente**, em 06/06/2024, às 16:28, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Monique Goncalves Paz**, **Diretora**, em 06/06/2024, às 16:32, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Fabio Ivo**, **Assistente**, em 06/06/2024, às 16:53, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Rosana Alves de Andrade**, **Analista de Sistemas**, em 06/06/2024, às 17:05, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Charles Monteiro Guimarães**, **Diretor**, em 06/06/2024, às 17:22, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Cristina da Silva Barros Drongitis**, **Assessora Chefe**, em 26/08/2024, às 12:51, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

A autenticidade deste documento pode ser conferida no site http://sei.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **75942064** e o código CRC **9AE3A4AA**.

Rua da Conceição, 69, 24º Andar / 25º Andar - Bairro Centro, Rio de Janeiro/RJ, CEP 20051-011
Telefone: