Governo do Estado do Rio de Janeiro
Secretaria de Estado de Fazenda
Subsecretaria de Tecnologia da Informação e Comunicação

TERMO DE REFERÊNCIA – VERSÃO 4

1. OBJETIVO

Contratação de empresa especializada na comercialização **de solução integrada de segurança, incluindo balanceamento de carga, controle e proteção de acesso, e disponibilidade e controle de aplicações,** a fim de atender as necessidades de natureza contínua da Secretaria de Estado de Fazenda do Rio de Janeiro (SEFAZ-RJ), valendo-se dos recursos provenientes do Fundo Especial de Administração Fazendária (Fonte de Recursos 100).

2. JUSTIFICATIVA

A Secretaria de Fazenda do Estado do Rio de Janeiro (SEFAZ-RJ) possui extenso parque tecnológico, e disponibiliza parte significativa de seus processos de negócios através de portais ou de serviços online, que se tornaram a maneira predominante para o relacionamento com o cidadão, com o contribuinte, com o governo e com a sociedade em geral.

Atualmente, a SEFAZ-RJ mantém 23 (vinte e três) portais e 197 (cento e noventa e sete) sistemas ou serviços expostos na web, que são suportados por 917 (novecentas e dezessete) máquinas virtuais. Todos esses ativos exigem infraestrutura que garanta integridade, confidencialidade, disponibilidade e autenticidade.

Ressalta-se a criticidade das informações fiscais armazenadas na SEFAZ-RJ, que conta, em particular, com o banco de dados de documentos fiscais eletrônicos e de escrituração fiscal digital, que contém informações sujeitas a sigilo fiscal, ou seja, informações que revelam a situação econômica ou financeira de praticamente todas as pessoas físicas e jurídicas do Estado do Rio de Janeiro e de diversas outras unidades federadas (Código Tributário Nacional, Art. 198).

Por consequência, a SEFAZ-RJ possui arquitetura robusta de segurança da informação, da qual a utilização de WAF (*Web Application Firewall*) é fundamental. Além das funções usuais de firewall de rede, este atua como proteção de aplicações WEB, repelindo ataques externos aos produtos e serviços hospedados na SEFAZ-RJ, dentre os quais se incluem, além dos produtos fazendários, o Sistema Eletrônico de Informações (SEI).

Essa proteção é fundamental porque alguns sistemas da SEFAZ-RJ, bem como o próprio SEI, contém falhas de segurança, visto que são softwares antigos/legados, desenvolvidos em arquiteturas e tecnologias ultrapassadas, não consentâneos com os elevados requisitos de segurança de informação que são necessários nos tempos atuais.

Assim sendo, a SEFAZ-RJ utiliza dois tipos de equipamentos do tipo *appliance* (combinação de hardware e software do mesmo fabricante): o F5 BIG-IP modelo 10200, atuando como firewall para proteção contra diversos ataques cibernéticos e o *appliance* F5 BIG-IP modelo 4200, atuando como solução de balanceamento de carga para todos os serviços providos e para aqueles acessados através dos portais desta Secretaria. Estes foram adquiridos em 2014 (E-04/056/372/2013) e tiveram suporte ativo até 2017.

Cada modelo possui dois equipamentos a fim de operar em alta disponibilidade e integridade da informação, tanto no nível de aplicação quanto no nível de arquitetura. Disponibilizam, além dos serviços já citados, a gestão de certificados digitais e o serviço de DNS (*Domain Name System*) ou sistema de nomes de domínios.

O quadro demonstrativo abaixo indica os principais parâmetros gerenciados pela solução:

Quadro 1 – Parâmetros de operação

Descrição	Ação
Tráfego sujo tratado	Manutenção da usabilidade dos sistemas, ambientes e navegabilidade, através da classificação e processamento do tráfego direcionado à infraestrutura da Pasta.
Tentativas de ataque mitigados	Manutenção da segurança e integridade de dados, através do tratamento dos ataques cibernéticos sofridos.
Certificados Digitais gerenciados	Manutenção do correto funcionamento de sites e sistemas, através da gestão dos certificados digitais necessários.
DNS	Manutenção do correto funcionamento do Sistema de Nomes de Domínio, através do serviço de localização e tradução de números IP / endereços de sites.
Balanceamento de carga	Manutenção da usabilidade de aplicações, mesmo ocorrendo quedas de links, servidores ou por conta de saturação de ambientes, causados por aumento de acessos ou processamento.
Proteção DDoS	Manutenção de funcionamento de sites e sistemas, através da mitigação de ataques de negação.
Proteção de aplicações	Proteção contra-ataques conhecidos, exploração de vulnerabilidade e bloqueio de requisições inválidas.

Os dados apresentados no quadro 1 demonstram, resumidamente, o rol de serviços tecnológicos providos pelo *appliance* e, portanto, sua importância para o adequado funcionamento dos sistemas de Tecnologia da Informação e Comunicação (TIC) da SEFAZ-RJ, de modo que uma nova solução deverá contemplar esses elementos integralmente.

Com relação à capacidade de processamento, conforme se observa na figura 1, o *core* 11 (representado pela linha rosa), responsável pelos serviços de estatísticas de plataforma, segue ultrapassando os 60% de utilização. É importante ressaltar que a quantidade de processamento consumido é proporcional ao tráfego sendo filtrado, e os *links* de internet da SEFAZ-RJ, atualmente de 300 Mbps, frequentemente sobrecarregados, estão em processo de atualização para 2.8Gbps[1], ou seja, aproximadamente 10 vezes mais largura de banda.

Adicionalmente, com relação à alta disponibilidade da arquitetura, entende-se que o total de processamento de cada nó não deva ultrapassar 50%, ainda que esteja sofrendo pesado ataque de DDoS, de maneira que, em caso de indisponibilidade por qualquer motivo, o nó remanescente possa suportar os requisitos de negócio da SEFAZ-RJ sem degradação de desempenho.

Além disso, é preciso que a solução WAF disponha de sobra de processamento para ser capaz de suportar a evolução dos produtos e serviços digitais da SEFAZ-RJ pelos próximos 5 anos, considerando-se não somente a expansão do consumo de serviços *online* (e consequente tráfego de dados), mas também a expansão das funcionalidades do software de segurança embarcado, conforme for sendo atualizado.

Tendo isso em vista, constata-se a necessidade de que o novo WAF expanda de forma significativa a capacidade de processamento em relação ao cenário atual.

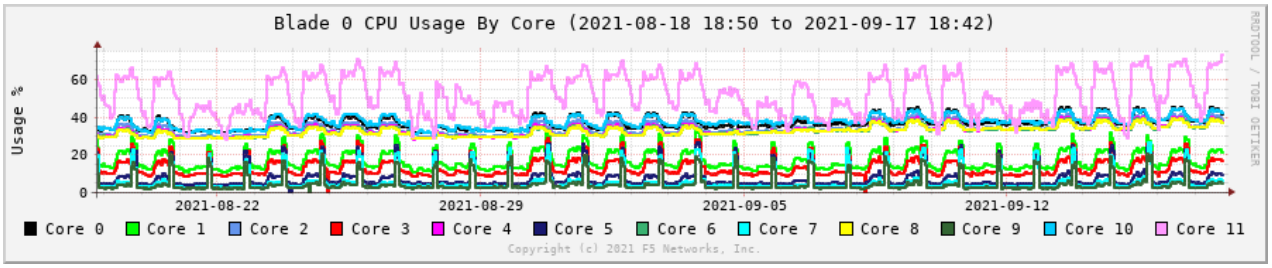


Figura 1 - Consumo de processamento tráfego externo

De maneira similar, demonstra-se consumo de processamento nos balanceadores de carga (figura 2), os quais ultrapassam os 30% de uso, indicando, mesmo em momento de demanda mínima, que tais índices sofrerão grande elevação por conta do aumento das velocidades e quantidade de *links* a serem implantados na nova topologia, acarretando problemas de desempenho e falhas por conta de saturação de processamento.

[1] Rede Conecta.RJ do ERJ, SEI-040227/000001/2021 e SEI-040227/000035/2021

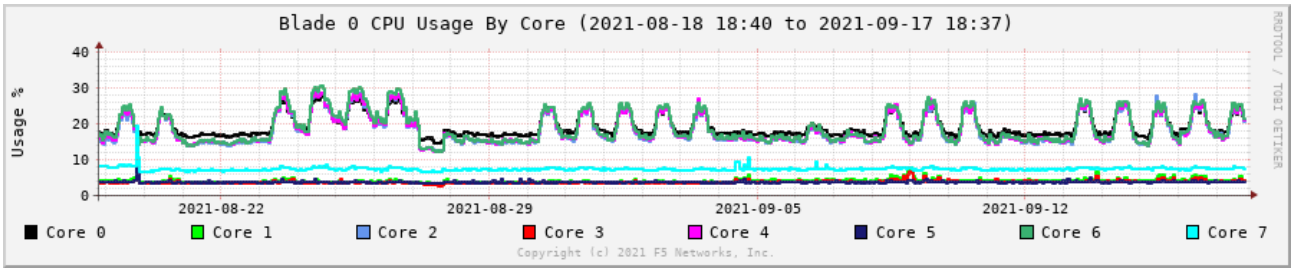
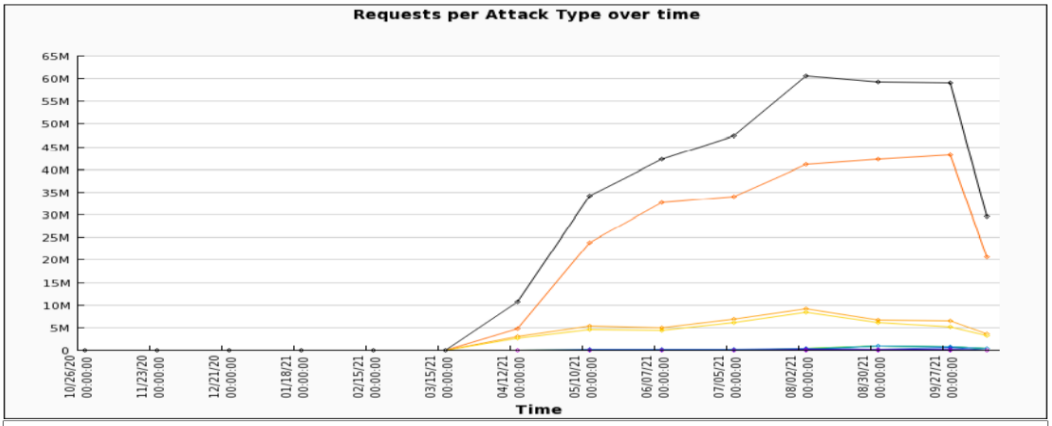


Figura 2 - Consumo de processamento tráfego balanceamento

Apresenta-se abaixo (figura 3) as tentativas de ataques à infraestrutura SEFAZ-RJ, que foram mitigadas pela solução atual, mantendo-se a estabilidade de todo o ecossistema computacional, no período compreendido entre março e outubro de 2021:



Attack Type	▼ Requests
Abuse of Functionality	242438638
HTTP Parser Attack	46381277
Injection Attempt	40853569
Detection Evasion	2741307
Cross Site Scripting (XSS)	2572206
Buffer Overflow	2538337
Forceful Browsing	2480541
Other Application Activity	1857358
Information Leakage	806425
Non-browser Client	208404
Total Attacks count for all requests	343112768

Figura 3 - Ataques mitigados

Isto quer dizer que foram bloqueados pelo WAF da SEFAZ-RJ cerca de 343 milhões de ataques em aproximadamente 7 meses, período da coleta de estatísticas acima, o que resulta na média de 68 mil ataques por hora. Tendo em vista a obsolescência que é imposta pela evolução tecnológica constante, é necessário atualizar a solução, e mantê-la atualizada, a fim de maximizar a proteção contra ameaças e minimizar o risco de um ataque cibernético lograr êxito contra a camada de perímetro.

Além de atualizar a solução WAF atual, é necessário expandir seu escopo para incluir a

proteção *web* ao tráfego oriundo da Rede Governo (Infovia 2.0 e Conecta.RJ), pois aplicações da SEFAZ-RJ são expostas também nesta rede para consumo por outros órgãos do ERJ, demanda que deverá aumentar a partir do ano de 2022 em função do lançamento do portal governamental RJ Digital, que consumirá APIs diretamente da SEFAZ-RJ por meio desta rede.

Assim, para lograr êxito total da solução, faz-se necessário também contratar os serviços de suporte técnico especializado dos equipamentos e treinamento para a equipe da SEFAZ-RJ, de forma que possam atualizar-se e dar continuidade à operação durante todo o ciclo de vida do produto.

Em síntese, a necessidade da contratação pretendida consiste em garantir o acesso seguro aos dados e informações dispostos pela SEFAZ-RJ por meio da modernização da solução de WAF, incluindo todas as funcionalidades atualmente em uso, como balanceamento do tráfego de dados, gerenciamento de certificados digitais, DNS, balanceamento de *links* e *sites*, estabelecimento de melhor gerenciamento de cache de conteúdo estático e do tratamento de conteúdo SSL (encriptação de páginas, ponta-a-ponta), além, sobretudo, da proteção contra invasões/ataques cibernéticos.

2.1 Benefícios a serem alcançados com a contratação

Com a presente contratação serão alcançados os seguintes benefícios:

- Melhor distribuição do tráfego de dados entre os links contratados pela SEFAZ-RJ, reduzindo o tempo de atendimento ao contribuinte, com atuação para a não indisponibilidade de serviços em caso de saturação de links ou processamento;
- Otimização do uso dos servidores de aplicações, com a distribuição inteligente de demandas para aqueles com maior disponibilidade de recursos para atender as solicitações dos contribuintes;
- Manutenção com possibilidade de refinamento nos níveis de proteção atualmente oferecidos aos portais de autoatendimento ao contribuinte;
- Aplicação de solução de segurança especializada contra ataques de negação de serviço distribuídos ou não;
- Manutenção ou melhoria na garantia dos níveis de confidencialidade, integridade e disponibilidade da informação;
- Proteção contra varredura de site por robôs de internet (comportamento não-humano);
- Proteção contra os ataques mais recorrentes da internet; e

- Maior e melhor gerenciamento nos acessos remotos, realizados por usuários autorizados.

2.2 Alinhamento da solução aos instrumentos de planejamento

Alinhamento ao Plano Estratégico Diretor de Tecnologia da Informação e Comunicação (PEDTIC)	
Objetivo Estratégico de TIC	OETIC 3
Meta	M35 – Prover e manter atualizadas as soluções de proteção de dados e informações
Ação	A195 – Modernizar solução de WAF, balanceamento de carga e DNS

Alinhamento ao Plano de Contratações Anual (PCA)	
Unidade Operacional (UO)	20610 - FAF
Grupo de Gastos (GG)	L2
Ação	8103 – Gestão de Tecnologia da Informação e Comunicação
Subelemento	3.3.90.40.11 – Suporte de infraestrutura de TIC
Item Unitário de Despesa (IUD)	298 – Serviços de informática

3. OBJETO

3.1 Descrição detalhada da solução de TIC

Aquisição de solução de balanceamento global e local de carga e *firewall* de aplicação, abrangendo o fornecimento de equipamentos, suporte técnico e implantação da solução e treinamento oficial na solução adquirida pelo período de 12 (doze) meses, conforme as especificações técnicas, condições, quantidades e exigências estabelecidas neste Termo de Referência e seus anexos.

3.2 Demanda e quantidade a serem contratadas

Item	ID SIGA	Descrição	Unidade	Quantidade
1	173970	**Segmentação 1** - *Appliance* de solução integrada de segurança para interligação de redes (F5 BIG-IP I5800)	Unidade	2
2	173975	**Segmentação 2** - *Appliance* de solução integrada de segurança para interligação de internet (F5 BIG-IP I10800)	Unidade	2
3	173971	**Segmentação Concentrador** - *Appliance* de solução integrada de segurança para interligação de internet (F5 BIG-IP I5800)	Unidade	2

4	173992	Suporte técnico (24x7x365) por 12 (doze) meses	Serviço	1
5	173972	Treinamento oficial para a solução F5 BIG-IP por aluno	Vaga	4

3.3 Detalhamento das especificações técnicas

As especificações técnicas da contratação estão dispostas no ANEXO III – "ESPECIFICAÇÕES TÉCNICAS".

3.4 Critérios de medição utilizados

3.4.1 Itens 1 a 3: A medição se dará através da efetiva entrega e implantação dos *appliances* adquiridos, de acordo com os requisitos definidos nos subitens 5.2 a 5.4 deste documento.

3.4.2 Item 4: Os critérios de medição que possibilitarão aferir os efetivos resultados do serviço contemplado serão baseados na observação da disponibilidade total dos serviços; da atualização das versões de *hardware* e *software*; dos chamados abertos através da interface de suporte ou canal telefônico versus o seu tempo de atendimento.

3.4.3 Item 5: A medição se dará a partir do recebimento do relatório de conclusão de curso dos participantes que finalizarem o treinamento, assim como dos certificados de conclusão.

3.5 Horário e local de prestação

3.5.1 Os serviços de suporte técnico previstos no item 3 deverão ser prestados remotamente e de forma ininterrupta, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, durante os 365 (trezentos e sessenta e cinco) dias do ano, inclusive sábados, domingos e feriados, através dos canais de suporte técnico estabelecidos pela fabricante da solução ou localmente, na Secretaria de Estado de Fazenda – SEFAZ-RJ, situada à Avenida Presidente Vargas, nº 670, 14º andar, Centro, Rio de Janeiro.

3.5.2 A instalação dos itens 1 a 3 deverá ser realizada nas dependências da SEFAZ-RJ, de acordo com o cronograma a ser estabelecido entre as partes.

3.5.3 O responsável pelo recebimento será o servidor Gabriel Motta Costa, e-mail: gmcosta@fazenda.rj.gov.br.

4. PRAZOS CONTRATUAIS

4.1 Vigência

4.1.1 A vigência da presente contratação será de 12 (doze) meses contados a partir da data convencionada no termo contratual, desde que posterior à data de publicação do extrato do contrato no Diário Oficial, valendo a data de publicação do extrato como termo inicial de vigência, caso posterior à data convencionada nesta cláusula.

4.1.1.1 Para os itens 4 e 5, o início de vigência da contatação ocorrerá logo após a instalação dos equipamentos dos itens de 1 a 3.

4.1.2 Para o item 4, a contratação poderá ser prorrogada por iguais e sucessivos períodos, por interesse da administração, até o limite de 60 (sessenta) meses, nos termos do art. 57, inciso II, da Lei n° 8.666/1993.

4.1.3 Para os itens 1,2,3 e 5 a contratação poderá ser prorrogada nos termos do art. 57, §1º, da lei 8.666/93.

4.1.4 Para fins de reajuste contratual será utilizado o Índice de Custo da Tecnologia da Informação (ICTI), ocorrido no período ou outro indicador que o venha substituir.

4.2 Execução

4.2.1 Entrega dos equipamentos e implantação da solução

4.2.1.1 A CONTRATADA deverá entregar os itens 1 a 3 em até 120 (cento e vinte) dias corridos, após a emissão do documento "Autorização de Compra ou Ordem de Serviços", conforme modelo constante no ANEXO VI – "MODELO DE AUTORIZAÇÃO DE COMPRA ou ORDEM DE SERVIÇOS".

4.2.1.2 A implantação dos itens 1 a 3 deverá acontecer em até 5 (cinco) dias a partir da entrega prevista no subitem 4.2.1.1, com janela de indisponibilidade tolerável de até 6 (seis) horas.

4.2.1.3 O prazo para entrega será iniciado a partir da confirmação do recebimento da Autorização da Compra por parte da CONTRATADA, com a indicação das quantidades, locais de entrega, prazos e responsáveis pelo recebimento e conferência do objeto.

4.2.1.4 A entrega deverá ocorrer de segunda-feira a sexta-feira das 09 horas às 18 horas (horário oficial de Brasília), no edifício sede da Secretaria de Estado de Fazenda (SEFAZ-RJ), situada à Avenida Presidente Vargas, nº 670, 14º andar, Centro, Rio de Janeiro.

4.2.1.5 A CONTRATADA é responsável pelo correto armazenamento e transporte de todos os itens que compõe a solução, devendo informar à CONTRATANTE com, no mínimo, 05 (cinco) dias corridos de antecedência, sobre a entrega dos equipamentos, informando os dados de identificação da transportadora (Razão Social, CNPJ etc.) e da respectiva equipe de entrega (Nome completo e Nº do RG Civil) para a liberação de acesso no local da entrega.

4.2.1.6 A entrega compreende o transporte dos equipamentos desde o endereço de origem da CONTRATADA até o local de recebimento, sem ônus adicional para a CONTRATANTE, devendo ser realizado em veículo adequado, acondicionado em embalagens protetoras lacradas e devidamente identificadas.

4.2.2 Treinamento

4.2.2.1 Após a publicação do extrato do contrato no DOERJ, a CONTRATADA deverá realizar o treinamento de acordo com a solicitação da CONTRATANTE, a ser realizada mediante a entrega de Ordem de Execução de Serviços (ANEXO VI – MODELO DE AUTORIZAÇÃO DE COMPRA ou ORDEM DE SERVIÇOS).

5. MODELO DE EXECUÇÃO E GESTÃO DO CONTRATO

5.1 Reunião inicial

5.1.1 Deverá ser realizada reunião inicial com o objetivo de alinhamento de questões operacionais e de gerenciamento do contrato, dirimindo possíveis dúvidas acerca da execução dos serviços.

5.1.2 Deverão participar dessa reunião, no mínimo, por parte da CONTRATANTE, os responsáveis técnicos pela implementação da solução no ambiente da SEFAZ-RJ e, por parte da CONTRATADA, seu representante legal e seu preposto.

5.1.3 A reunião será realizada na sede da CONTRATANTE ou de forma remota, em até 5 (cinco) dias úteis após o início de vigência do contrato, mediante convocação do Superintendente de Infraestrutura da Subsecretaria de Tecnologia de Informação e Comunicação (SUBTIC) da SEFAZ-RJ com, no mínimo, 2 (dois) dias úteis de antecedência.

5.1.4 Ao seu final, deverá ser produzida ata de reunião devidamente assinada pelas partes, cuja elaboração ficará a cargo da CONTRATANTE, que consignará todos os assuntos tratados, na ocasião por todos os participantes.

5.2 Instalação dos equipamentos

5.2.1 **Itens 1 a 3:** Este serviço compreende a instalação e configuração da solução no *datacenter* da CONTRATANTE, possibilitando a utilização de seus recursos.

5.2.2 A solução deverá ser instalada no *datacenter* da CONTRATANTE, mediante agendamento prévio entre as partes e com janela de indisponibilidade tolerável de até 6 (seis) horas.

5.2.3 Caso a solução se encontre em desconformidade com as exigências estabelecidas, a CONTRATADA deverá providenciar os ajustes e correções dentro deste prazo.

5.2.4 A CONTRATADA, com o apoio do fabricante, fornecerá a instalação de *hardware* e configuração de *software* e indicará um único ponto de contato para coordenar todas as atividades e comunicação necessárias entre as equipes a fim de garantir uma implantação bem-sucedida.

5.2.5 A solução será entregue com a instalação do *hardware*, incluindo documentação de planejamento de instalação e configuração, validação e testes de funcionalidade de *hardware*, rede e sistema operacional, *softwares* e *hardwares* necessários para a configuração de todos os aspectos dos componentes do sistema operacional e de rede, interna e externa a solução.

5.3 Suporte técnico

5.3.1 O regime de atendimento 24x7 compreende suporte ininterrupto, 24 horas por dia, 7 dias da semana, incluindo feriados nacionais, estaduais e municipais.

5.3.2 O suporte técnico do fabricante deverá abranger todos os elementos da solução, garantindo sua substituição, atualização e correto funcionamento pelo período de 12 (doze) meses.

5.3.1 A abertura de chamado será feita por meio de telefone 0800, mensagens mediante e-mail ou outro sistema de abertura que permita o registro com controle de histórico.

5.3.2 A CONTRATANTE deverá ter acesso direto à base de dados de conhecimento do fabricante da solução que contenha informações, assistência e orientação para instalação, desinstalação, configuração e atualização de *firmware* e *software*, aplicação de correções (*patches*), diagnósticos, avaliações e resolução de problemas e demais atividades relacionadas à correta operação e funcionamento da solução;

5.3.3 No caso de substituição de peças ou de todos os *appliances*, o *Return Merchandise Authorization* – Autorização para Devolução de Mercadorias (RMA) deverá ocorrer em até 1

(um) dia útil após o diagnóstico de falha em chamado aberto com o fabricante.

5.3.3.1 No caso de substituição, a CONTRATADA deverá retirar adequadamente das dependências da CONTRATANTE as peças ou os equipamentos substituídos e acondicioná-los de forma a permitir sua completa segurança e identificação durante o transporte, responsabilizando-se pela sua devolução ao fabricante e pelas despesas operacionais decorrentes.

5.3.3.2 Cabe também à CONTRATADA, às suas expensas, a entrega das peças novas ou equipamentos substitutos na dependência da CONTRATANTE, executando as instalações *on-site* e configurações em janelas definidas pela CONTRATANTE.

5.3.3.3 A CONTRATADA, sem ônus adicional para a CONTRATANTE, será responsável por quaisquer despesas relacionadas ao deslocamento do seu(s) técnico(s) ao local da instalação e do exercício da garantia do equipamento, seja para retirada e/ou entrega, incluindo todas as despesas de transporte, frete e seguro correspondentes.

5.3.3.4 As peças ou os equipamentos substitutos deverão ser entregues nas dependências da CONTRATANTE até o próximo dia útil, em conformidade com o subitem 5.6.

5.3.4 O suporte técnico deverá permitir que a CONTRATANTE acione o fabricante diretamente para abertura de chamados de suporte e manutenção dos equipamentos e sistemas que compõem a solução, durante a vigência da garantia.

5.3.5 A CONTRATADA deverá providenciar permissão de acesso ao sítio do fabricante para acompanhamento pela CONTRATANTE de chamados, *download* e acesso a documentações, *patches*, *fixes*, *firmwares*, arquivos de qualquer tipo e/ou qualquer outro material referente à solução.

5.4 Treinamento

5.4.1 O conteúdo programático do treinamento deverá ser aprovado previamente pela CONTRATANTE e cobrir o uso de todas as funcionalidades da solução adquirida, devendo abordar, no mínimo, os seguintes módulos:

5.4.1.1 F5 ADM - *Administering* Big-IP;

5.4.1.2 F5 LTM - *Configuring* Big-IP *Local Traffic Manager Configuring*;

5.4.1.3 F5 *Advanced* WAF (*previously licensed as ASM*);

5.4.1.4 F5 *Configuring* BIG-IP- DNS (Antigo GTM);

5.4.1.5 F5 APM - Big-IP *Access Policy Manager*;

5.4.1.6 F5 *Troubleshooting* BIG-IP; e

5.4.1.7 F5 *Configuring* BIG-IP (AFM): *Advanced Firewall Manage.*

5.4.2 A CONTRATADA deverá entregar à CONTRATANTE documento que evidencie o conteúdo programático do treinamento em até 2 dias úteis a partir da emissão da Ordem de Execução de Serviços (ANEXO VI – MODELO DE AUTORIZAÇÃO DE COMPRA ou ORDEM DE SERVIÇOS), devendo este ser apreciado pela CONTRATANTE em até 24 (vinte e quatro) horas. Caso não seja aprovado, a CONTRATADA deverá entregar nova versão do referido documento impreterivelmente em até 24 (vinte e quatro) horas da comunicação da CONTRATANTE.

5.4.3 Os treinamentos deverão ter duração de, no mínimo, 60 (sessenta) horas/aula e ser ministrados por profissionais certificados na solução.

5.4.4 Os treinamentos deverão ser ministrados em língua portuguesa do Brasil para a capacitação de 4 (quatro) alunos, na modalidade *on-line*, em datas e horários acordados com a CONTRATANTE. A capacitação não necessariamente deverá ser feita em uma única turma.

5.4.5 É obrigatório o fornecimento de material impresso ou eletrônico, redigido no idioma Português do Brasil ou Inglês.

5.4.6 O conteúdo do treinamento deverá ser organizado em módulos, sequenciados logicamente, visando o conhecimento cumulativo, contendo, ao final de cada módulo, exercícios práticos com laboratórios para fixação.

5.4.7 Os treinamentos serão realizados em horário comercial, de segunda a sexta-feira, exceto feriados e dias em que não haja expediente na CONTRATANTE.

5.4.8 Todos os custos relativos aos treinamentos serão de responsabilidade da CONTRATADA.

5.4.9 A CONTRATADA deverá fornecer aos participantes certificados de conclusão de cada treinamento realizado.

5.4.10 A CONTRATADA deverá fornecer à CONTRATANTE relatório de conclusão de curso dos participantes que finalizaram o treinamento.

5.4.11 A CONTRATANTE poderá a seu critério, em qualquer tempo, durante o treinamento, contestar a prestação do serviço, solicitando a substituição de instrutor. Caso a deficiência não possa ser

sanada sem prejuízo para o andamento do curso, esse será suspenso, devendo a CONTRATADA agendar novo curso, sem ônus adicional para a CONTRATANTE.

5.4.12 Após a realização do treinamento, a CONTRATANTE realizará a avaliação de satisfação junto aos participantes, cujo resultado deverá alcançar a média de, pelo menos, 70% (setenta por cento) de satisfação dentre os critérios avaliados para validação e emissão do Termo de Recebimento Definitivo. Caso não alcance o resultado esperado, o treinamento deverá ser ministrado novamente, sem ônus à CONTRATANTE.

5.5 Visita técnica

5.5.1 As licitantes interessadas em participar da licitação poderão, a seu critério, proceder à visita técnica no local onde serão executados os serviços, examinando as áreas e tomando ciência das características e peculiaridades dos serviços, considerando que:

5.5.1.1 A visita técnica deverá ser marcada e realizada em dias úteis, das 10h às 16h, devendo ser agendada pelo e-mail producao@fazenda.rj.gov.br e acompanhada por um dos servidores da área técnica da SUBTIC. As visitas poderão ser efetivadas em até 3 (três) dias úteis antes da data fixada para a realização do pregão eletrônico.

5.5.1.2 A realização da visita técnica não se consubstancia em condição para a participação na licitação, ficando, contudo, as licitantes cientes de que após apresentação das propostas não serão admitidas, em hipótese alguma, alegações posteriores no sentido da inviabilidade de cumprir com as obrigações em razão do desconhecimento dos serviços e de dificuldades técnicas encontradas na realização dos serviços objeto da licitação.

5.6 Avaliação da qualidade e aceite do objeto

5.6.1 O recebimento provisório se dará em até 5 (cinco) dias corridos para verificação da conformidade das quantidades e especificações com aquelas contratadas e consignadas neste Termo de Referência.

5.6.1.1 Para os itens 1 a 3, o recebimento se dará após a instalação de tais equipamentos.

5.6.1.2 Para o item 4, o recebimento se dará por meio da disponibilização, em portal do fabricante, de documento que evidencie o número de contrato do suporte técnico e sua respectiva data de expiração (*End of Support*).

5.6.1.3 Para o item 5, o recebimento será emitido após a efetiva realização dos treinamentos.

5.6.2 O recebimento definitivo se dará no prazo de até 15 (quinze) dias corridos, contados a partir da data de emissão do Recebimento Provisório e após a comprovação do perfeito funcionamento dos serviços e cumprimento das demais condições estabelecidas.

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

5.6.4 Após a regularização pertinente, e contando-se da data de apresentação para apreciação da CONTRATANTE, esta terá o prazo de até 5 (cinco) dias úteis para verificação em face dos termos pactuados. Constatada a conformidade, será procedida a emissão do recebimento definitivo.

5.6.5 O aceite/aprovação do objeto não exclui a responsabilidade civil da CONTRATADA, por vício de quantidade, qualidade ou disparidades com as especificações estabelecidas neste Termo de Referência.

6. ACORDO DE NÍVEL DE SERVIÇO (ANS)

6.1 Níveis de serviço

6.1.1 O suporte técnico da CONTRATADA deve estar disponível para abertura de chamados 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, mediante e-mail ou outro sistema de abertura que permita o registro com controle de histórico.

6.1.2 O tempo de solução será contabilizado entre a abertura do chamado e restabelecimento do sistema em sua totalidade.

6.1.3 O tempo de atendimento inicia-se com a primeira intervenção pelo representante da CONTRATADA, local ou remotamente.

6.1.4 As multas por descumprimento de prazo serão aplicadas sobre os valores mensais do suporte técnico, em razão proporcional ao valor anual de pagamento, sem prejuízo das demais sanções previstas neste Termo de Referência.

6.1.5 Em caso de problema ou incidente de *hardware* ou de *software*, os seguintes prazos máximos deverão ser obedecidos para o início do atendimento e término da correção do problema:

Tipo de Incidente	Exemplos de cenários	Início do atendimento	Prazo de solução	Critérios de medição	Multa por descumprimento
Crítico	Parada total da solução - mecanismos de contingência não funcionam; indisponibilidade total ou parcial das instâncias de um cluster no sítio; indisponibilidade total de um ou mais serviços das instâncias que compõem um sítio; degradação de serviços providos pelas instâncias que compõem o sítio; indisponibilidade ou degradação no mecanismo de balanceamento entre os sítios.	1 (uma) hora	4 (quatro) horas se software; próximo dia útil, se *hardware*	**Meta:** Cumprir os prazos de início de atendimento e de solução **Indicador:** Tempo de atendimento **Instrumento de Medição:** Ferramenta de suporte técnico disponibilizada pela Contratada	0,5% do valor do Suporte Técnico mensal dos serviços por hora que exceda o prazo de recuperação, até 8 horas; 1,00% nas horas seguintes.
Médio impacto	Aqueles para os quais houver solução de contorno cujo impacto não comprometa a operação dos serviços que utilizam a solução.	Próximo dia útil	7 (sete) dias	**Meta:** Cumprir os prazos de início de atendimento e de solução **Indicador:** Tempo de atendimento **Instrumento de Medição:** Ferramenta de suporte técnico disponibilizada pela Contratada	Infração de n° 2 (subitem 9.2 do Termo de Referência)
Baixo impacto	Aqueles que não afetem o perfeito funcionamento da solução.		30 (trinta) dias		Infração de n° 1 (subitem 9.2 do Termo de Referência)

6.1.6 Excepcionalmente, a critério exclusivo da CONTRATANTE, mediante justificativa tecnicamente fundamentada que demonstre a impossibilidade de atendimento dos prazos acima, poderá ser concedido prazo adicional à contratada para resolução de problemas.

6.1.7 A finalização de cada atendimento só poderá ser efetuada com anuência formal do responsável técnico da CONTRATANTE.

6.1.8. A multa moratória será aplicada até o limite do art. 412, do Código Civil.

6.1.9. Foram estabelecidas multas moratórias atreladas aos descumprimentos contratuais neste ANS, em detrimento da previsão de glosas, tendo em vista que o pagamento pela prestação dos serviços

continuados será realizado em parcela única no início da execução contratual, nos termos dos subitens 5.6.1.2, 5.6.2, 13.1 e 13.2 deste Termo de Referência.

7. OBRIGAÇÕES DA CONTRATANTE

7.1 Realizar os pagamentos devidos à CONTRATADA, nas condições estabelecidas neste Termo de Referência.

7.2 Fornecer à CONTRATADA documentações relevantes dos sistemas, aplicações e infraestrutura pertinentes à execução do contrato.

7.3 Acompanhar, fiscalizar, conferir e avaliar os serviços prestados, utilizando o Acordo de Nível de Serviço.

7.4 Acompanhar o andamento da entrega dos produtos e serviços contratados.

7.5 Designar servidores para realizar a fiscalização e o acompanhamento da execução do objeto, devendo este fazer anotações e registros de todas as ocorrências em livro próprio, determinando o que for necessário à regularização das falhas ou defeitos observados.

7.6 Tomar decisões em problemas que necessitam resolução do CONTRATANTE de forma a não impactar o cronograma estabelecido entre as partes.

7.7 Garantir o livre acesso às informações e documentações relevantes dos sistemas, aplicações e infraestrutura da CONTRATANTE, incluindo documentação técnica necessária para a execução dos serviços contratados.

7.8 Garantir que os profissionais da equipe da CONTRATANTE, necessários ao cumprimento do cronograma estabelecido entre as partes, estarão disponíveis quando necessário.

7.9 Receber e avaliar os serviços prestados pela CONTRATADA, conforme descrição das OS.

7.10 Aplicar à CONTRATADA as sanções administrativas necessárias.

7.11 Verificar o cumprimento dos requisitos de qualificação técnico-profissional da equipe técnica que irão atuar na prestação do serviço;

7.12 Comunicar à CONTRATADA, por escrito, sobre imperfeições, falhas ou irregularidades

verificadas na execução do objeto, para que sejam sanadas as ocorrências, com as devidas reparações ou correções;

7.13 A Administração não responderá por quaisquer compromissos assumidos pela CONTRATADA com terceiros, ainda que vinculados à execução do contrato, bem como por qualquer dano causado a terceiros em decorrência de ato da CONTRATADA, de seus empregados, prepostos ou subordinados;

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

7.15 Executar as medidas previstas no Mapa de Gerenciamento de riscos, que visam a minimização de possíveis danos à CONTRATANTE;

7.16 Na abertura de chamados de suporte técnico, identificar o nível de criticidade da demanda, quando aplicável; e

7.17 A CONTRATATANTE fica proibida de repassar e/ou compartilhar quaisquer informações fiscais sigilosas, em função de seus deveres de proteção e sigilo, extraídos do art. 198 do Código Tributário Nacional, da Lei Geral de Proteção de Dados Pessoais - Lei nº 13.709/2018, assim como outros dados e informações sigilosas por expressa disposição legal (como, por exemplo, as hipóteses de sigilo permitidas e previstas na Lei de Acesso à Informação - Lei nº 12.527/2011, Lei Geral de Proteção de Dados Pessoais - Lei nº 13.709/2018, e Marco Civil da Internet - Lei nº12.965/2014).

8. OBRIGAÇÕES DA CONTRATADA

8.1 Designar formalmente preposto da empresa e substituto eventual, para representá-la na execução do contrato e atuar como interlocutor principal junto a SEFAZ-RJ, incumbido de receber, diligenciar, encaminhar e responder as principais questões técnicas, legais e administrativas referentes ao andamento contratual.

8.2 Participar, com a presença do preposto da equipe indicada, dentro do período compreendido entre a assinatura do contrato e o início da prestação dos serviços, de reuniões de alinhamento de expectativas contratuais com uma equipe designada pela SEFAZ-RJ para a Fiscalização do Contrato.

8.3 Manter-se, durante o período de vigência do contrato, em compatibilidade com as obrigações trabalhistas, bem como com todas as condições de habilitação e qualificação exigidas na licitação.

8.4 Prover os serviços ora contratados, de acordo com o estabelecido no Termo de Referência, com pessoal adequado e capacitado em todos os níveis de trabalho.

8.5 Itens 1 a 3: Ser empresa credenciada pelo fabricante para venda, entrega e instalação dos equipamentos.

8.6 Item 4: Ser empresa credenciada pelo fabricante para a prestação dos serviços de suporte técnico especializado.

8.7 Reportar à SEFAZ-RJ, verbalmente e por escrito, erros ou irregularidades que possam comprometer a execução dos serviços ou qualquer situação que caracterize descumprimento ou atraso no cumprimento das obrigações constantes deste Termo de Referência.

8.8 Responder por todos os ônus referentes à realização dos serviços ora contratados, desde os salários dos seus empregados, como também os encargos trabalhistas, previdenciários, fiscais e comerciais, que venham a incidir sobre o presente Contrato.

8.9 Emitir notas fiscais/faturas de acordo com a legislação, contendo descrição dos serviços, indicação de sua quantidade, preço unitário e valor total.

8.10 Suprir eventuais despesas de custeio com deslocamento dos profissionais da CONTRATADA ao local de execução dos serviços, bem como todas as despesas de transporte, diárias, seguro ou quaisquer outros custos envolvidos ficam a cargo exclusivo da CONTRATADA, sendo vedado qualquer ônus adicional à CONTRATANTE.

8.11 Prestar todas as informações solicitadas pela CONTRATANTE com referência ao objeto adquirido, sempre que necessário.

8.12 Executar fielmente o objeto contratado, de acordo com as normas legais, em conformidade com a proposta apresentada, prazos estipulados pela CONTRATANTE.

8.13 Zelar pelo sigilo de quaisquer informações dos sistemas, dados hospedados em algum dispositivo de armazenamento, usuários, topologia, configurações, políticas de segurança e ao modo de funcionamento e tratamento das informações da SEFAZ-RJ, durante a vigência do contrato, bem

como após o seu término, salvo quando houver autorização expressa da CONTRATANTE para divulgação.

8.14 Fornecer todos os documentos exigidos pela CONTRATANTE (ex.: especificações técnicas, planilhas, diagramas de arquitetura, cronogramas etc.) em formato compatível com as principais ferramentas Microsoft, tais como: Word, Excel, Visio e Project, e Adobe, dentre outras, sem nenhum ônus adicional.

8.15 Documentar e repassar à CONTRATANTE todo o conhecimento técnico utilizado na execução dos serviços prestados.

8.16 Entregar à CONTRATANTE evidências irrefutáveis que comprovem a execução dos serviços, como condição de ateste/aceite das fases previstas.

8.17 Reparar, corrigir, remover, reconstruir ou substituir, no todo ou em parte e às suas expensas, bens ou prestações objeto do contrato em que se verificarem vícios, defeitos ou incorreções resultantes de execução irregular ou do emprego ou fornecimento de materiais inadequados ou desconformes com as especificações;

8.18 Indenizar todo e qualquer dano e prejuízo pessoal ou material que possa advir, direta ou indiretamente, do exercício de suas atividades ou serem causados por seus prepostos à CONTRATANTE, aos usuários ou terceiros;

8.19 Atender, por meio do preposto indicado, qualquer solicitação por parte dos fiscais do contrato, prestando as informações referentes à prestação dos serviços, bem como as correções de eventuais irregularidades na execução do objeto contratado;

8.20 Manter atualizados seu endereço, e-mail, telefones e dados bancários;

8.21 Comunicar à CONTRATANTE a disponibilização dos produtos;

9. PENALIDADES

9.1 No caso de a CONTRATADA inadimplir as obrigações assumidas, no todo ou em parte, ficará sujeita às sanções previstas nos artigos 86 e 87 da Lei nº 8.666/1993.

9.2 Os quadros abaixo descrevem o grau das penalidades específicas de acordo com as infrações cometidas:

Grau	Correspondência
1	1% sobre o valor do contrato.
2	3% sobre o valor do contrato.
3	1% por dia útil que exceder o prazo estipulado, a incidir sobre o valor do contrato, da nota de empenho ou do saldo não atendido, respeitando o limite do art. 412 do Código Civil sem prejuízo da rescisão unilateral ou de aplicação das sanções administrativas.
4	até 5% sobre o valor do contrato, aplicada de acordo com a gravidade da infração e proporcionalmente sobre as parcelas não executadas.

Infrações		
Item	**Descrição**	**Grau**
1	Suspender ou interromper os serviços determinados pela Administração, por ocorrência.	3
2	Execução de serviços por funcionário sem qualificação técnica.	1
3	Deixar de fornecer ou repor garantia contratual.	4
4	Deixar de cumprir cronograma/programação dos serviços na sua íntegra, restando serviços incompletos e/ou mal acabados, trazendo com isso transtornos à Contratante, por ocorrência.	1
5	Deixar de cumprir determinação formal, instrução complementar do órgão fiscalizador, ou as normas disciplinares e de segurança da Contratante, por ocorrência.	1
6	Deixar de manter a documentação de habilitação atualizada.	2
7	Não manter um preposto responsável pelo gerenciamento dos serviços, com poderes de representante ou preposto, para tratar com a entidade sobre assuntos relacionados à execução do contrato.	2
8	Inexecução parcial ou total do objeto	4

9.3 As penalidades descritas acima são meramente exemplificativas, reservando-se à Comissão de Acompanhamento e Fiscalização do contrato o direito de verificada a ocorrência de infração, segundo a proporcionalidade e a razoabilidade, utilizar outros critérios para a dosimetria da pena.

9.4 Nas reincidências específicas, a multa compensatória deverá corresponder ao dobro do valor da que tiver sido inicialmente imposta, observando-se sempre o limite de 20% (vinte por cento) do valor global do contrato, conforme preceitua o artigo 87 do Decreto Estadual n° 3.149/80.

9.5 As penalidades descritas acima serão aplicadas, sem prejuízo, das demais previstas na Lei nº 8.666/93 e no Edital.

9.6. Em qualquer hipótese de aplicação de sanções administrativas, assegurar-se-á o direito ao contraditório e ampla defesa.

10. QUALIFICAÇÃO TÉCNICA

10.1 Será exigida comprovação de aptidão para a prestação de serviços pertinentes e compatíveis em características e quantidades com o objeto da licitação, sendo necessário apresentar os seguintes documentos:

a) A comprovação de aptidão referida no item anterior será feita mediante apresentação de atestado(s) fornecido(s) por pessoa(s) jurídica(s) de direito público ou privado, na forma do artigo 30, II c/c §1°, da Lei Federal nº 8.666/93;

b) O(s) atestado(s) deve(m) conter o nome, endereço e o telefone de contato do(s) atestador(es), ou qualquer outro meio com o qual o Órgão possa valer-se para manter contato com a(s) pessoas(s) declarante(s), e a razão social e dados de identificação da instituição eminente como CNPJ, endereço e telefone;

c) Para os itens 1 a 4, o(s) atestado(s) deve(m) comprovar a aptidão para fornecimento de um quantitativo de 50% (cinquenta por cento) do total de itens ou do serviço a serem arrematados desde que os objetos do(s) atestado(s) sejam compatíveis em características e quantidades ao da presente licitação.

d) Para comprovação da qualificação técnica exigida será permitido o somatório de quantitativos através da apresentação de mais de um atestado, para os contratos que forem executados simultaneamente.

11. DISPONIBILIDADE ORÇAMENTÁRIA E FINANCEIRA

As despesas decorrentes desta contratação correrão à conta da Unidade Orçamentária 2061 – FAF (Fundo Especial de Administração Fazendária).

- Programa de Trabalho: 2061.04.126.0435.8103
- Natureza de Despesa: 3.3.90.40.11
- Fonte de Recursos: 100

12. DISPOSIÇÕES GERAIS

12.1 Natureza do bem ou serviço

A aquisição e serviços pretendidos nesta contratação são considerados comuns por ser possível estabelecer, para efeito de julgamento de propostas, mediante especificações do mercado, padrões de qualidade e desempenho peculiares ao objeto.

12.2 Registro justificado de mão de obra residente

A prestação de serviços não envolve "dedicação exclusiva de mão de obra" – nos termos do art. 17 da IN 05/SEGES/MPDG de 26/05/2017 –, uma vez que a CONTRATADA poderá compartilhar os recursos humanos e materiais disponíveis para execução simultânea de outros contratos. A prestação dos serviços eventuais e temporários também não gera vínculo empregatício entre os empregados da CONTRATADA e a CONTRATANTE, vedando-se qualquer relação entre estes que caracterize pessoalidade e subordinação direta.

12.3 Subcontratação

Segundo o Acórdão nº 2002/2005 – Plenário do TCU, foi consignado que a subcontratação deve ser adotada unicamente quando necessária para garantir a execução do contrato e desde que não atente contra os princípios constitucionais inerentes ao processo licitatório, e nem ofenda outros princípios relacionados às licitações, notadamente o da seleção da proposta mais vantajosa para a Administração (art. 3º, Lei nº 8.666/93).

Dado que a subcontratação não figura como condição necessária para a execução do contrato, aponta-se que não será admitida a possibilidade de subcontratação do objeto.

12.4 Participação de consórcios e/ou cooperativas

A figura do consórcio que, diga-se, é uma associação de dois ou mais indivíduos, empresas, organizações ou governos (ou qualquer combinação destas entidades), com o objetivo de participar numa atividade em comum ou de partilha de recursos para atingir um objetivo comum, é usualmente 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.

Destaca-se, na presente licitação, a natureza simples e comum da contratação, não se vislumbrando qualquer vantagem em admitir-se consórcios, sendo certo que a competitividade do

certame em nada será impactada em função da restrição, vez que o objeto é compatível com empresas atuantes no ramo licitado e demonstram possuir condições suficientes para a execução de contratos dessa natureza, o que por consequência não tornará restrito o universo de possíveis licitantes individuais.

Tendo em vista que a admissão ou não de empresas estabelecidas em consórcio é ato discricionário da administração previsto no Art. 33 da Lei nº 8.666/93, não serão admitidas empresas estabelecidas em consórcio no presente processo licitatório.

Não se aplica a participação de cooperativa para o objeto desta contratação, dada a necessidade de subordinação para a prestação dos serviços. Segundo o Acórdão 2221/2013 – Plenário do TCU, destaca-se que "é irregular a participação de cooperativas em licitação cujo objeto se refira a prestação de serviço que demande requisitos próprios da relação de emprego, como subordinação (hierarquia) e habitualidade (jornada de trabalho) dos trabalhadores".

Nos termos da Orientação Administrativa PGE nº 08, deve ser vedada a participação das cooperativas de serviços nas licitações destinadas a selecionar contratado para prestar serviços em relação aos quais se presume a subordinação dos trabalhadores que o exercem.

12.5 Parcelamento do objeto

12.5.1 Itens 1 a 3 – *Appliances* WAF e balanceadores de carga

Segundo o "Guia de Boas Práticas em Contratação de soluções de Tecnologia da Informação" elaborado pelo Tribunal de Contas da União (TCU), *"uma solução de TI engloba todos os elementos necessários que se integram para o alcance dos resultados pretendidos com a contratação, de modo a atender à necessidade que a desencadeou"* (TCU, 2012, p. 19).

Significa dizer que a solução deve ser planejada como um todo, mas também é preciso que seja dividida em tantos objetos quanto possível para fins de contratação. De acordo com os arts. 15, inciso IV, e 23, § 1º, da Lei 8.666/93, as licitações públicas devem ser apartadas em tantos itens que se comprovem técnica e economicamente viáveis, procedendo-se à licitação com vistas ao melhor aproveitamento dos recursos disponíveis no mercado, sem perda da economia de escala.

Nesse fulcro, os integrantes da Equipe de Planejamento da Contratação avaliaram que, muito embora a possibilidade de licitação dos itens pretendidos conjuntamente – em lote único – possa oferecer benefícios quanto à gestão da execução contratual e sua fiscalização, a separação da solução em parcelas demonstra-se plenamente possível e razoável para fins de contratação, dada a sua natureza perfeitamente divisível.

Ou seja, entende-se que a presença de diversas empresas para o fornecimento dos itens relacionados aos *Appliances* WAF e balanceadores de carga não comprometeria ou configuraria óbice à contratação pretendida, adicionando-se que o eventual risco da geração de conflitos decorrente dos diferentes prazos de instalação dos equipamentos seria suprido, satisfatoriamente, a partir do planejamento detalhado das equipes de TIC da SEFAZ-RJ, a fim de evitar transtornos e sobrecarga de trabalho de coordenação, supervisão e fiscalização das atividades a serem executadas.

Por fim, a divisão dos itens está coadunada ao princípio da ampliação da competitividade, conforme previsto no art. 23 §§ 1° e 2° da Lei nº 8.666/93 e Súmula nº 247 Tribunal de Contas da União.

12.5.2 Item 4 – Suporte técnico

Entende-se que não há óbice de natureza técnica ao parcelamento do serviço suporte técnico (24x7x365) dos equipamentos referentes aos itens 1 a 3. Significa dizer que o fornecimento de suporte, bem como as ações de *upgrade* de *hardware e* atualização de novas versões do *software* podem ser contratados separadamente dos referidos equipamentos, sem que haja ainda prejuízos de ordem econômica ou perda de economia de escala.

No mais, é de entendimento da área técnica que a divisibilidade não deva ser estendida para além disso, dado que o suporte técnico de cada equipamento realizado de forma segregada lograria grande transtorno operacional, devendo a equipe técnica sempre buscar a qual contrato de suporte técnico cada equipamento estaria conectado, nesse caso. Não somente isso, mas também se incorreria em eventual risco de não renovação de parte dos equipamentos, o que prejudicaria o funcionamento do conjunto de *appliances*, operacionalmente. Portanto, entende-se que o suporte técnico deva ser concentrado em um único item, sendo o vencedor obrigado a fornecer o objeto para todos os equipamentos.

12.5.3 Item 5 – Treinamento

Em função de sua natureza, não há óbices de natureza técnica ao treinamento ser licitado de forma apartada. Igualmente, não se vislumbram óbices de ordem econômica em parcelar, tampouco causaria prejuízos de escala, visto que seu valor estimado consiste em ordem de grandeza inferior ao valor dos itens referentes aos equipamentos.

Vislumbra-se, ainda, que sua separação em item apartado poderia trazer melhor aproveitamento do mercado, haja vista a existência de empresas especializadas em treinamento e capacitação.

13. CONDIÇÕES DE PAGAMENTO

13.1 Os pagamentos serão efetuados em até 30 (trinta) dias após a emissão de Termo de Recebimento Definitivo e o ateste pela Comissão de Fiscalização do Contrato nas respectivas Notas Fiscais.

13.2 Os pagamentos referentes aos itens 1 a 3 ocorrerão em parcela única, após a emissão do Termo de Recebimento Definitivo dos respectivos itens;

13.3 A parcela referente ao item 4 será paga em parcela única, após a emissão do Termo de Recebimento Definitivo do serviço.

13.4 Por fim, a parcela referente ao item 5 será paga em parcela única, após a emissão do Termo de Recebimento Definitivo do serviço.

14. GARANTIA CONTRATUAL

14.1 A CONTRATADA se obriga a prestar garantia, durante toda a vigência do contrato, de 5% (cinco por cento) do valor global do contrato, devendo apresentar o comprovante à SEFAZ-RJ, no prazo máximo de 5 (cinco) dias úteis, contados da data da assinatura do Termo de Contrato, em uma das seguintes modalidades: caução em dinheiro a ser depositada via GRE; título da dívida pública; fiança bancária ou seguro-garantia.

14.2 A garantia deverá contemplar a cobertura para os seguintes eventos:

a) Prejuízos advindos do não cumprimento do contrato;
b) Multas punitivas aplicadas pela fiscalização à contratada;
c) Prejuízos diretos causados à CONTRATANTE decorrentes de culpa ou dolo durante a execução do contrato; e
d) Obrigações previdenciárias e trabalhistas não honradas pela CONTRATADA.

15. PROCEDIMENTOS DE GESTÃO E FISCALIZAÇÃO

15.1 O contrato deverá ser executado fielmente, de acordo com as cláusulas avençadas, nos termos do presente instrumento e da legislação vigente, respondendo o inadimplente pelas consequências da inexecução total ou parcial.

15.2 A execução do contrato será acompanhada e fiscalizada por comissão constituída de 3 (três) membros, que serão oportunamente designados pela Departamento Geral de Administração e Finanças (DEPGAF) da CONTRATANTE.

15.3 Os representantes da SEFAZ-RJ, sob pena de responsabilização administrativa, anotarão em registro próprio todas as ocorrências relacionadas com a execução do contrato, determinando o que for necessário à regularização das faltas ou defeitos observados. As decisões e providências que ultrapassarem a competência dos representantes deverão ser solicitadas a seus superiores, em tempo hábil, para a adoção das medidas convenientes.

15.4 A CONTRATADA declara, antecipadamente, aceitar todas as condições, métodos e processos de inspeção, verificação e controle adotados pela fiscalização, obrigando-se a fornecer todos os dados, elementos e esclarecimentos solicitados.

15.5 A fiscalização não exclui ou reduz a responsabilidade da CONTRATADA, inclusive perante terceiros, por qualquer irregularidade, nem a exime de manter fiscalização própria.

16. MODALIDADE DE CONTRATAÇÃO

O certame licitatório será realizado na modalidade de pregão, em sua forma eletrônica, do tipo menor preço por item, em conformidade com a Lei Federal nº 10.520/02 e a Resolução SEPLAG nº 429/2011.

17. REGIME DE EXECUÇÃO

Para a presente contratação será adotado como regime de execução a empreitada por preço global.

18. DOS CRITÉRIOS DE ACEITAÇÃO E JULGAMENTO DAS PROPOSTAS

18.1 Adotar-se-á como critério de aceitabilidade de preços o de maior preço estimado por item, desclassificando-se as propostas cujos preços o excedam ou sejam manifestamente inexequíveis.

18.2 Para julgamento e classificação das propostas será adotado o critério do menor preço por item.

19. DOCUMENTOS COMPLEMENTARES

Integram este Termo de Referência os documentos a seguir relacionados, os quais estão vinculados à execução do contrato e sendo dele parte integrante, após devidamente ajustados com as informações correspondentes às partes contratantes:

- ANEXO I – CRONOGRAMA FÍSICO-FINANCEIRO
- ANEXO II – PLANILHA DE CUSTOS E FORMAÇÃO DE PREÇOS
- ANEXO III – ESPECIFICAÇÕES TÉCNICAS
- ANEXO IV – MODELO DE TERMO DE RECEBIMENTO PROVISÓRIO
- ANEXO V – MODELO DE TERMO DE RECEBIMENTO DEFINITIVO
- ANEXO VI – MODELO DE AUTORIZAÇÃO DE COMPRA ou ORDM DE SERVIÇOS
- ANEXO VII – TERMO DE SIGILO E CONFIDENCIALIDADE

20. ASSINATURAS

Por este instrumento, **assinado eletronicamente,** a Equipe de Planejamento da Contratação, conclui o Termo de Referência na fase de Planejamento da Contratação.

Rio de Janeiro, 11 de maio de 2022.

ASSINADO ELETRONICAMENTE

INTEGRANTE REQUISITANTE	**INTEGRANTE TÉCNICO**	**INTEGRANTE ADMINISTRATIVO**

AUTORIDADE MÁXIMA DE TIC

ANEXO I – CRONOGRAMA FÍSICO-FINANCEIRO

	Item 1	Item 2	Item 3	Item 4	Item 5
Descrição	Segmentação 1 - *Appliance* de solução integrada de segurança para interligação de redes	Segmentação 2 - *Appliance* de solução integrada de segurança para interligação de internet	Segmentação Concentrador - *Appliance* de solução integrada de segurança para interligação de internet	Suporte técnico (24x7x365) por 12 (doze) meses	Treinamento oficial para a solução F5 BIG-IP por aluno
Mês 1					
Mês 2					
Mês 3					
Mês 4					
Mês 5	100%	100%	100%	100%	100%
Mês 6					
Mês 7					
Mês 8					
Mês 9					
Mês 10					
Mês 11					
Mês 12					
TOTAL	**100%**	**100%**	**100%**	**100%**	**100%**

ANEXO II – PLANILHA DE CUSTOS E FORMAÇÃO DE PREÇOS

Item	Descrição	Qtd	Und	Valor Unitário	Valor Global
1	**Segmentação 1** - *Appliance* de solução integrada de segurança para interligação de redes	2	Unidade	R$	R$
2	**Segmentação 2** - *Appliance* de solução integrada de segurança para interligação de internet	2	Unidade	R$	R$
3	**Segmentação Concentrador** - *Appliance* de solução integrada de segurança para interligação de internet	2	Unidade	R$	R$
4	Suporte técnico (24x7x365) por 12 (doze) meses	1	Serviço	R$	R$
5	Treinamento oficial para a solução F5 BIG-IP por aluno	4	Vaga	R$	R$

ANEXO III – ESPECIFICAÇÕES TÉCNICAS

Item 1 - Segmentação 1 - *Appliance* de solução integrada de segurança para interligação de redes (F5 *BIG*-IP I5800) e **Item 3** - Segmentação Concentrador - *Appliance* de solução integrada de segurança para interligação de internet (F5 *BIG*-IP I5800)

Solução composta por *hardware* e *software* do mesmo fabricante, licenciado com todas as funcionalidades listadas neste documento, permitindo que as funções sejam utilizadas em todas e quaisquer instância criada no *appliance*, tendo como características gerais, *hardware* dedicado do tipo *appliance* com sistema operacional customizado para garantir segurança e melhor performance.

1.1 Possuir quantidade de memória e capacidade de processamento suficiente para atendimento de todas as funcionalidades e desempenho solicitados neste documento;

1.2 Acompanhar todos os cabos e suportes necessários para a instalação do equipamento;

1.3 Fontes de alimentação redundantes e internas, do tipo N+N, *hot-swappable*, *auto-sense*, para operar de 100 a 240 VAC monofásico, na frequência de 50/60Hz, com comutação entre as fontes de forma automática e sem qualquer interrupção no funcionamento do equipamento;

1.4 Possuir fluxo de ar “front to rear”;

1.5 Possuir pelo menos 01 (um) disco com tecnologia SSD ou superior;

1.6 Acompanhar todas as licenças de software ou hardware necessárias para atendimento às funcionalidades exigidas neste documento;

1.7 Possuir no mínimo 08 (oito) portas SFP+ acompanhadas dos respectivos adaptadores 10GBase-SR;

1.8 Possuir no mínimo 04 (quatro) portas QSFP+;

1.9 Possuir no mínimo 01 (uma) porta para gerenciamento out-of-band 10/100/1000Base-T;

1.10 Possuir no mínimo 01 (uma) porta de console serial;

1.11 Possuir no mínimo 01 (uma) porta USB para transferência de arquivos;

1.12 Permitir agregação de até 8 portas baseado no protocolo LACP;

1.13 Transporte de múltiplas VLAN por uma única porta (ou por um conjunto agregado de portas) utilizando o protocolo 802.1q;

1.14 Todas as interfaces ethernet deverão possuir isolamento de comunicação entre si;

1.15 Implementa no mínimo 4 (quatro) instâncias virtuais com virtualização completa, com as seguintes características:

1.15.1 Dedicar cores de processamento e memória para cada instância;

1.15.2 Permitir criar uma instância com, pelo menos, metade de cores de processamento;

1.15.3 Permitir criar e executar simultaneamente instância virtuais com versões de sistemas operacionais diferentes;

1.15.4 Reiniciar uma instância sem afetar as demais;

1.15.5 Tabelas de roteamento distintas em cada instância;

1.15.6 Qualquer falha em uma instância não deve afetar as demais;

1.15.7 Nenhuma instância poderá comprometer o poder de processamento das outras;

1.15.8 Implementa no mínimo 500.000 novas conexões TCP por segundo em camada 4;

1.15.9 Implementa no mínimo 30 milhões de conexões concorrentes em camada 4;

1.15.10 Implementa no mínimo 50 Gbps de tráfego em camada 4;

1.15.11 Suporta 30 milhões de pacotes SYN/segundo, sob ataque de SYN Flood;

1.15.12 Implementa no mínimo 1,5 milhões de requisições por segundo em camada 7;

1.15.13 Implementa no mínimo 25 Gbps de tráfego em camada 7;

1.15.14 Implementa no mínimo 20 Gbps de tráfego SSL/TLS;

1.15.15 Implementa no mínimo 30.000 transações por segundo (TPS) TLSv1.2 com chaves RSA de 2048bits;

1.15.16 Implementa no mínimo 20.000 Transações por segundo (TPS) TLSv1.2 com chaves ECDSA de 256bits;

1.15.17 Implementa compressão de tráfego com throughput mínimo de 25 Gbps;

1.15.18 Suporta 2048 VLANs;

Item 2 - Segmentação 2 - *Appliance* de solução integrada de segurança para interligação de internet (F5 *BIG*-IP I10800)

Solução composta por *hardware* e *software* do mesmo fabricante, licenciado com todas as funcionalidades listadas neste documento, permitindo que as funções sejam utilizadas em todas e quaisquer instância criada no *appliance*, tendo como características gerais, *hardware* dedicado do tipo *appliance* com sistema operacional customizado para garantir segurança e melhor performance.

2.1 *Hardware* dedicado tipo *appliance* com sistema operacional customizado para garantir segurança e melhor performance;

2.2 Possuir quantidade de memória e capacidade de processamento suficiente para atendimento de todas as funcionalidades e desempenho solicitados neste documento;

2.3 Permitir a instalação em rack padrão 19 polegadas, possuir altura máxima de até 2U;

2.4 Acompanha todos os cabos e suportes necessários para a instalação do equipamento;

2.5 Fontes de alimentação redundantes e internas, do tipo N+N, *hot-swappable*, auto-sense, para operar de 100 a 240 VAC monofásico, na frequência de 50/60Hz, com comutação entre as fontes de forma automática e sem qualquer interrupção no funcionamento do equipamento;

2.6 Possuir fluxo de ar "*front to rear*";

2.7 Acompanha todas as licenças de software ou hardware necessárias para atendimento às funcionalidades exigidas neste documento;

2.8 Possuir no mínimo 08 (oito) portas SFP+ acompanhadas dos respectivos adaptadores 10GBase-SR;

2.9 Possuir no mínimo 04 (quatro) portas QSFP+;

2.10 Possuir no mínimo 01 (uma) porta para gerenciamento out-of-band 10/100/1000Base-T;

2.11 Possuir no mínimo 01 (uma) porta de console serial;

2.12 Possuir no mínimo 01 (uma) porta USB para transferência de arquivos;

2.13 Permitir agregação de até 8 portas baseado no protocolo LACP;

2.14 Transporte de múltiplas VLAN por uma única porta (ou por um conjunto agregado de portas) utilizando o protocolo 802.1q;

2.15 Todas as interfaces ethernet deverão possuir isolamento de comunicação entre si;

2.16 Implementar no mínimo 15 instâncias virtuais com virtualização completa, com as seguintes características:

2.16.1 Dedicar cores de processamento e memória para cada instância;

2.16.2 Permitir criar uma instância com, pelo menos, metade de cores de processamento;

2.16.3 Permitir criar e executar simultaneamente instância virtuais com versões de sistemas operacionais diferentes;

2.16.4 Reiniciar uma instância sem afetar as demais;

2.16.5 Tabelas de roteamento distintas em cada instância;

2.16.6 Qualquer falha em uma instância não deve afetar as demais;

2.16.7 Nenhuma instância poderá comprometer o poder de processamento das outras;

2.16.8 Implementa no mínimo 1,2 milhões de novas conexões TCP por segundo em camada 4;

2.16.9 Implementa no mínimo 90 milhões de conexões concorrentes em camada 4;

2.16.10 Implementa no mínimo 150 Gbps de tráfego em camada 4;

2.16.11 Suporta 40 milhões de pacotes SYN/segundo, sob ataque de SYN Flood;

2.16.12 Implementa no mínimo 3 milhões de requisições por segundo em camada 7;

2.16.13 Implementa no mínimo 70 Gbps de tráfego em camada 7;

2.16.14 Implementa no mínimo 40 Gbps de tráfego SSL/TLS;

2.16.15 Implementa no mínimo 65.000 transações por segundo (TPS) TLSv1.2 com chaves RSA de 2048bits;

2.16.16 Implementa no mínimo 45.000 transações por segundo (TPS) TLSv1.2 com chaves ECDSA de 256bits;

2.16.17 Implementa compressão de tráfego com throughput mínimo de 35Gbps;

2.16.18 Suporta 2048 VLANs.

3. Funcionalidades gerais

3.1 Permitir a configuração da solução em alta disponibilidade;

3.2 Implementar solução de redundância de dispositivos em modo ativo-ativo ou ativo-*standby*, de maneira que, em caso de falha de um dos equipamentos, o estado de todas as sessões do tipo "*stateful*" seja remanejado para o equipamento redundante, preservando o estado original de todas as tabelas de sessões e de persistência;

3.3 Implementar a sincronização entre os equipamentos redundantes, assegurando que não haverá "*downtime*" e queda de sessões do tipo "*stateful*" em caso de falha de uma das unidades;

3.4 Possuir suporte ao HTTP/2 tanto na conexão com o cliente quanto na conexão com o servidor;

3.5 A plataforma deve possuir um alto nível de customização e programabilidade, permitindo o uso de REST API;

3.6 Possuir visibilidade com relação a performance e segurança das aplicações através da gerência centralizada;

3.7 Possuir integração com outras plataformas de automação e orquestração como por exemplo *ansible* e *terraform;*

3.8 Possuir integração com *ansible* e *terraform* para configuração e *deploy* com módulos desenvolvidos pelo fabricante;

3.9 Possuir API aberta para o *deploy* de serviços em ambientes de Data Center e *Multi-Cloud*;

3.10 Simplificar a parte operacional e ao mesmo tempo melhorar o gerenciamento e orquestração do ambiente;

3.11 Possuir integração nativamente ao *Kubernetes/Openshift* para realizar o balanceamento entre pods;

3.12 Deve criar os serviços de Balanceamento de Carga dinamicamente ao mesmo tempo em que uma nova aplicação é provisionada pelo *Kubernetes/Openshift*;

3.13 Permitir que os pods de uma determinada aplicação sejam automaticamente incluídos e excluídos do pool de balanceamento de carga;

3.14 Possuir suporte a VXLAN;

3.15 Implementar roteamento estático e roteamento dinâmico para os protocolos OSPFv3 e BGPv4;

3.16 Ser capaz de balancear servidores com qualquer *hardware*, sistema operacional e tipo de aplicação;

3.17 Implementar a otimização do protocolo TCP para ajustes a parâmetros das conexões clientes e servidor;

3.18 Permitir incluir e retirar equipamentos sem que haja indisponibilidade do serviço (deve haver divisão ou consolidação dos serviços pelos elementos ativos);

3.19 Em caso de queda (desligamento/perda) de um ou mais equipamentos é possível a redistribuição da carga entre os demais membros sem que haja interrupção do serviço (considerando que a capacidade restante é suficiente para suportar a carga);

3.20 Permitir que os equipamentos sejam gerenciados por uma solução centralizada do mesmo fabricante;

3.21 Suportar sincronização de relógio interno via protocolo NTP.

4. Características de Camada 4 e 7

4.1 Implementar todas as aplicações comuns de um Switch Layer 7:

4.1.1 Server Load-Balancing;

4.1.2 Firewall Load-Balancing;

4.1.3 Proxy Load-Balancing;

4.1.4 Global Site Load-Balancing;

4.1.5 Transparent Cache Switch;

4.1.6 Implementar Balanceamento L4 em direção ao servidor, onde a resposta do servidor real é enviada diretamente ao cliente;

4.1.7 Implementa abrir um número específico de conexões TCP com o servidor e inserir todos os HTTP requests gerados pelos clientes nestas conexões, reduzindo a necessidade de estabelecimento de novas conexões com os servidores, aumentando a performance do serviço;

4.2 Implementa os seguintes métodos de balanceamento local:

4.2.1 Round Robin;

4.2.2 Least Connections;

4.2.3 Weighted Percentage (por peso);

4.2.4 Fastest – servidor com resposta mais rápida;

4.3 Implementar balanceamento das sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência de sessão dos seguintes tipos:

4.3.1 por cookie;

4.3.2 por endereço IP destino;

4.3.3 por Endereço IP origem;

4.3.4 por sessão SSL;

4.3.5 analisando a URL acessada;

4.3.6 analisando a URL e Cookie concorrentemente;

4.3.7 analisando qualquer parâmetro no header HTTP;

4.4 Implementar os seguintes métodos de monitoramento dos servidores reais, de forma nativa ou através do uso de monitores personalizados:

4.4.1 Layer 3 – ICMP;

4.4.2 Layer 4 – Conexões TCP e UDP pela porta respectiva no servidor;

4.4.3 Layer 7 – Verificação específica ao protocolo de aplicação, suportando, no mínimo: HTTP, HTTPS, FTP, DNS, RADIUS, SMTP, LDAP, POP3, SIP, SNMP;

4.4.4 Implementar de limitar o número de sessões estabelecidas no Virtual Server (VIP), sem prejuízo as sessões existentes;

4.4.5 Implementar de limitar o número de sessões estabelecidas com cada servidor real, sem prejuízo as sessões existentes;

4.5 Implementar as seguintes funcionalidades de segurança:

4.5.1 Network Address Translation (NAT);

4.5.2 Proteção contra todos os tipos de ataques Denial of Service (DoS e DDoS);

4.5.3 Proteger contra ataques de DNS DDoS utilizando mecanismo que bloqueie somente as requisições maliciosas e permita requisições legítimas aos domínios existentes.

4.5.4 Limite do número de conexões;

4.5.5 Listas de Controle de Acesso (ACL);

4.5.6 Log de ataques do tipo DoS;

4.5.7 Limpeza de cabeçalho HTTP (Manipular qualquer conteúdo da aplicação para remover ou alterar as informações enviadas ao servidor ou ao cliente);

4.5.8 Suporta e Implementa configuração de proxy reverso;

4.5.9 Implementa de fazer log de todas as sessões, onde os registros deverão conter:

4.5.10 Endereço IP de origem;

4.5.11 Porta TCP ou UDP de origem;

4.5.12 Endereço IP de destino;

4.5.13 Porta TCP ou UDP de destino;

4.5.14 Protocolo de camada 4 (TCP ou UDP);

4.5.15 Data e hora da mensagem;

4.5.16 URL acessada;

4.5.17 Cookie Utilizado;

4.5.18 A configuração da solução é baseada em perfis, permitindo fácil administração;

4.5.19 Os perfis devem ser hierarquizados, permitindo maior facilidade na administração de políticas similares;

4.6 Deverá ser capaz de fazer compressão de conteúdo HTTP, para reduzir a quantidade de informações enviadas ao cliente:

4.6.1 Permitir compressão tipo GZIP e DEFLATE;

4.6.2 Permitir definir compressão especificamente para certos tipos de objetos;

4.6.3 Deverá ser capaz de fazer aceleração de SSL, onde os certificados digitais são instalados na solução e as requisições HTTP são enviadas aos servidores sem criptografia:

4.6.3.1 Permitir configurar a solução para re-criptografar em SSL a requisição ao enviar para o servidor, permitindo as demais otimizações em ambiente 100% criptografado;

4.6.3.2 Implementa Cache de Conteúdo para HTTP, permitindo que objetos sejam armazenados em RAM e requisições HTTP sejam respondidas diretamente pela solução:

4.6.3.3 recurso de cache deverá permitir a definição de quais tipos de objeto serão armazenados em cache e quais nunca devem ser cacheados;

4.6.3.4 O recurso de cache permitir determinar o tamanho mínimo e tamanho máximo dos objetos que serão cacheados;

4.6.3.5 O recurso de cache permitir determinar o número máximo de objetos que serão cacheados;

4.6.3.6 O recurso de cache possuir a capacidade para determinar a URI (Uniform Resource Identifiers) que deve ser cacheada;

4.6.3.7 O recurso de cache possuir a capacidade para ler, alterar e ignorar o parâmetro cache-control no cabeçalho HTTP;

4.6.3.8 O recurso de cache possuir a capacidade para inserir e alterar o parâmetro age header no cabeçalho HTTP;

4.7 Implementa a realização de GSLB de forma nativa, permitindo inclusive a replicação automatizada da configuração de GSLB entre os equipamentos ofertados, mesmo em sites distintos;

4.8 Opera em, no mínimo, a seguintes formas:

4.8.1 DNS autoritativo;

4.8.2 DNS resolver;

4.8.3 DNS cache;

4.8.4 Balanceamento de DNS servers;

4.8.5 DNSSec;

4.8.6 A solução é capaz de realizar IP Anycast;

4.9 A solução suporta DNS64

4.10 Deve responder queries DNS pelo menos dos seguintes tipos: A, AAAA, CNAME, MX, SRV e NAPTR.

4.11 A solução é capaz de fazer resoluções baseada em topologia (localização geográfica do cliente), sem que seja necessário adquirir licenças adicionais de terceiros.

4.12 Permitir usar a solução como DNS Autoritativo;

4.13 Possuir proteções de ataques DNS, no mínimo:

4.14 Inspeção de protocolo;

4.15 Validação de protocolo;

4.16 UDP flood;

4.17 Pacotes mal formados;

4.18 Ataque teardrop;

4.19 Ataque ICMP;

4.20 Implementar as seguintes funcionalidades de balanceamento global (GSLB):

4.21 Round Robin;

4.22 Geolocation;

4.23 Health Check;

4.24 Disponibilidade e carga da aplicação (site load);

4.25 Weighted Site;

4.26 Least Connection;

4.27 EDNS-Client-Subnet (ECS);

4.28 Para as funções de GLSB, é capaz de coletar métricas de desempenho de outros equipamentos do mesmo fabricante;

4.29 Bloqueio de pacotes inválidos, incluindo verificação para DNS malformed, Bad ICMP Frame, Bad ICMP Checksum, ICMP Frame too Large, Bad IGMP Frame, Bad IP TTL Value, Bad IP Version, Header Length Too Short, Bad Source, Bad IPV6 Hop Count, Bad IPV6 Version, Bad TCP Checksum, Bad TCP Flags, SYN && FIN Set, Bad UDP Checksum, ARP Flood, ICMPv4 Flood, ICMPv6 Flood , IGMP Flood, IGMP Fragment Flood, TCP RST Flood, TCP SYN ACK Flood, TCP SYN Flood, UDP Flood, SIP ACK Method, SIP Malformed, Single Endpoint

Flood, Single Endpoint Sweep, LAND Attack) e fornecer estatísticas para os pacotes descartados;

4.30 Mitigar, no mínimo, os seguintes tipos de ataques:

4.30.1 ICMP/UDP/TCP Floods;

4.30.2 TCP Flag Abuses;

4.30.3 GET/POST Floods;

4.30.4 SYN Floods;

4.30.5 UDP Bandwidth Attacks;

4.30.6 Smurfing;

4.30.7 NTP Reflection Attacks;

4.30.8 TCP/UDP Bandwidth Attacks;

4.30.9 Fragging Attack;

4.30.10 Slowloris;

4.30.11 Connection Attacks;

4.30.12 Botnet;

4.30.13 Fragmentation attacks;

5. Firewall de Aplicação WEB (WAF)

5.1 Suporta os protocolos IPv4 e IPv6 (Internet Protocol);

5.2 Suporta HTTP/1.0, HTTP/1.1 e HTTP/2.0 (Hypertext Transfer Protocol);

5.3 Suporta SSLv3 (Secure Sockets Layer), TLS 1.1, TLS 1.2 e TLS 1.3 (Transport Layer Security);

5.4 Deve operar em modo de aprendizado (learning) e proxy (reverso e transparente), podendo ser configurado para operar em um dos modos;

5.5 Em modo de aprendizado (learning), é capaz de realizar análise e avaliação de tráfego, gerando relatórios;

5.6 Deve realizar a decifração de tráfego SSL, a partir da importação de chaves criptográficas, para permitir a inspeção de todo conteúdo do pacote originalmente cifrado, de modo man-in-the-middle;

5.7 Deve ter capacidade de inspeção e monitoramento até a camada de aplicação HTTP, incluindo cabeçalhos, campos de formulários, conteúdo, requests e responses;

5.8 Deve ter capacidade de aprendizado da estrutura e os elementos das aplicações WEB automaticamente;

5.9 Deve aprender o comportamento ou ser possível configurar métodos HTTP, cookies, arquivos XML, ações SOAP, elementos XML, diretórios, URLs e parâmetros de URL, campos e valores esperados, incluindo se o campo é obrigatório, read-only, tamanho, tipo de dado, tipos de caracteres utilizados;

5.10 Deve checar os formatos ilegais de elementos XML;

5.11 Deve identificar o campo X-Forwarded-For como endereço IP de origem original de um pacote, a fim de identificar a origem real de tráfego que sofra NAT de origem;

5.12 Deve identificar e criar perfis de utilização de aplicações, incluindo Javascript, CGI, ASP, PHP e Java;

5.13 Deve realizar o correlacionamento de múltiplos eventos de segurança para distinguir, de forma precisa, tráfego legítimo de tráfego malicioso;

5.14 Deve usar políticas comportamentais para distinguir, de forma precisa, tráfego legítimo de tráfego malicioso;

5.15 Deve realizar a identificação de ataques baseados em assinaturas, regras e perfis de utilização;

5.16 Deve realizar a criação de políticas diferenciadas por aplicação e por URL;

5.17 Deve realizar a criação dinâmica de política de segurança, com aprendizado automático de padrão de utilização da aplicação, realizado sobre o fluxo de tráfego bidirecional;

5.18 Deve criar políticas de forma automática, por meio da observação do tráfego da aplicação, com base no tráfego do ambiente de produção ou desenvolvimento;

5.19 Deve realizar os seguintes critérios de decisão para realização de bloqueio ou geração de alerta, podendo ser utilizado um ou mais critérios simultaneamente: user-agent (navegador), usuário, IP de origem, país de origem, assinatura de ataque, conteúdo do payload, conteúdo do cabeçalho, conteúdo do cookie, código de response, hostname, tipo de protocolo (HTTP ou HTTPS), número de ocorrências e método HTTP;

5.20 Deve realizar configuração granular por aplicação protegida, restrições de métodos HTTP permitidos, tipos ou versões de protocolos e tipos de caracteres;

5.21 Deve realizar a atualização automática da base de assinatura de ataques através de serviço online fornecido pelo fabricante;

5.22 A base deve ser exclusiva de assinaturas de WAF, não sendo aceitas atualização de base de assinaturas baseadas em reputação de IP ou de URL;

5.23 As atualizações devem ser específicas das assinaturas durante o período da garantia, não sendo aceita a atualização de assinaturas exclusivamente por atualização do sistema operacional;

5.24 Deve proteger contra atraques CSRF (Cross-Site Request Forgery), podendo ser possível especificar quais URLs serão examinadas;

5.25 Possuir controle de fluxo por aplicação permitindo definir o fluxo de acesso de uma URL para outra da mesma aplicação. Dessa forma qualquer tentativa de acesso a um determinado site que não siga o fluxo passando pelas URLs pré-definidas deverá ser bloqueado como uma tentativa de acesso ilegal;

5.26 Deve realizar a aplicação de políticas de forma manual e automática, possibilitando a criação de exceções por endereço IP de origem e destino;

5.27 Deve realizar a aplicação de assinaturas de detecção e bloqueio de intrusão sem interrupção de tráfego;

5.28 Suporta a criação de página HTML informativa e personalizável como resposta de bloqueios;

5.29 Suporta o recurso de assinar cookies, criptografar e editar endereços de URL (URL rewriting);

5.30 Suporta a restrição do tipo de arquivo para upload de arquivos;

5.31 Suporta recurso de geolocalização de endereço IP, incluindo identificação do país de origem;

5.32 Deve realizar a reputação de endereços IP, através de serviço de assinatura com atualização frequente online durante o período da garantia, impedindo que aplicações internas sejam acessadas por endereços IP maliciosos, botnets e proxys anônimos;

5.33 A solução é capaz de criar filtros de endereços IPs baseados em reputação, com no mínimo as seguintes categorias: Windows Exploits, Web Attacks, Botnets, Scanners, Denial of Service, Reputation, Phishing, Proxy;

5.34 Deve aplicar os filtros de reputação considerando o endereço IP e o cabeçalho HTTP X-Forwarded-For;

5.35 Deve realizar a reputação de endereços IP, permitindo a configuração de whitelist para permitir a liberação de acessos considerados legítimos e de baixo risco;

5.36 Deve realizar proteção contra ataques automatizados, incluindo botnets, identificando comportamento não humano, navegadores operados por scripts ou qualquer outra forma não operada por humanos;

5.37 Deve realizar a identificação e bloqueio contra ataques sofisticados sem impactar nas transações das aplicações para os protocolos HTTP e HTTPs;

5.38 Deve realizar a identificação de ataques, contendo nome, campo atacado, quantidade de ataques, horário e endereços IPs envolvidos, através de relatórios históricos;

5.39 Deve realizar a identificação de dados sensíveis em páginas WEB, tais como senhas de acesso, por meio de campos de formulário, e o mascaramento, de forma a ocultar essa informação nos logs gerados;

5.40 Deve realizar a identificação e análise de tráfego de saída de aplicações, capaz de evitar vazamento de informações confidenciais, por meio da definição de padrões de formação, como, por exemplo, formato de CPF;

5.41 Implementar a criptografia entre o browser e o WAF de campos específicos, tais como credenciais, de forma que, além da criptografia do TLS, estes campos estejam protegidos por interceptações;

5.42 Deve realizar a detecção de ataques de força bruta;

5.43 Deve realizar a detecção de ataques de força bruta por meio da quantidade de transações por segundo (TPS), por endereço IP;

5.44 Deve realizar detecção de ataques do tipo força bruta que explorem controles de acesso da aplicação (Erro 401 – Unauthorized), solicitações repetidas ao mesmo recurso, em qualquer parte/URL da aplicação, e aplicações WEB que não retornam o erro 401, por meio da identificação de expressão regular, cabeçalho HTTP ou texto específico no retorno/página de erro da aplicação;

5.45 Suporta proteção contra mensagens XML e SOAP malformadas;

5.46 Deve realizar proteção contra ataques de Anonymous Proxy Vulnerabilities, Brute Force Login, Buffer Overflow, Cookie Injection, Cookie Poisoning, CSRF (Cross Site Request Forgery), XSS (Cross Site Scripting), Forceful Browsing, Form Field Tampering, Heartbleed, HTTP Denial of Service, HTTP Parameter Pollution, HTTP hidden field manipulation, HTTP request smuggling, Illegal Encoding; Malicious Robots, OS Command Injection, Poodle Attack, Sensitive Data Leakage, Session Hijacking, Site Reconnaissance, SQL Injection, WEB Scraping, WEB Services (XML) attacks;

5.47 Suporta a importação de arquivos swagger com a definição de API e configuração automática de regras de segurança;

5.48 Implementar mecanismos cotas para limitar a quantidade de requisições de um mesmo cliente a métodos de uma API, com limites de chamadas por período e limite de chamadas por rajada;

5.49 Proteger a aplicação web contra robôs sofisticados através da combinação de desafios enviados ao browser do usuário e técnicas avançadas de análise comportamental;

5.50 A solução de WAF Suporta HTTP/2.0 para inspeção de políticas, DoS camada 7 e proteção de Bot.

5.51 Proteger API contra ataques do tipo: Content scraping, Denial of service e ataques a API.

5.52 Implementar proteção por URI, método e atributos;

5.53 Implementar validação de métodos e atributos;

5.54 Prover proteção robusta contra robôs, a fim de proteger aplicações contra: Scanners de vulnerabilidade, robôs e outros vetores de ataques automatizados;

5.55 Deve possuir solução de segurança para a proteção de aplicações, contra ataques de bots e ataques automatizados, que obedecem às seguintes características:

5.56 A solução deve suportar análise comportamental e impressão digital para garantir que a transação seja feita por um ser humano;

5.57 Proteger as aplicações contra robôs através de técnicas de análise comportamental;

5.58 Deve aprender automaticamente o comportamento da aplicação e o comportamento heurístico do tráfego.

5.59 Assinaturas dinâmicas podem ser automaticamente criadas e implementadas em tempo real para proteção da aplicação;

5.60 Possuir uma proteção proativa contra ataques automatizados por robôs e outras ferramentas de ataque;

5.61 Deve prover inteligência para identificar e mitigar ataques sofisticados;

5.62 Possibilita o uso de múltiplas formas de logging remoto ao mesmo tempo para a mesma aplicação. Portanto dever ser possível por exemplo logar os requests válidos num servidor de SIEM e os requests inválidos em outro servidor de SIEM de outra marca e modelo;

5.63 A solução Permitir a integração com soluções de análise de vulnerabilidades (Scanner) de terceiros como por exemplo: Trustwave App Scanner (Cenzic), White Hat Sentinel, IBM AppScan, Qualys, Quotium Seeker, HP Webinspect;

6. Tratamento de SSL/TLS

6.1 Possuir suporte a seguintes cifras e protocolos SSL/TLS:

6.1.1 TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256

6.1.2 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

6.1.3 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

6.1.4 TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256

6.1.5 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

6.1.6 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

6.1.7 TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

6.1.8 TLS_DHE_RSA_WITH_AES_128_GCM_SHA256

6.1.9 TLS_CHACHA20_POLY1305_SHA256

6.1.10 TLS_AES_256_GCM_SHA384

6.1.11 TLS_AES_128_GCM_SHA256

6.2 Implementa aceleração em hardware específico de, no mínimo, os algoritmos DH, ECDH, 3DES, AES, AES-GCM, RSA, DSA, ECDSA, MD5, SHA e SHA2;

6.3 Suporta SSL forward secrecy como uma forma de melhorar a segurança nas transações SSL/TLS;

6.4 Implementa SSL offload, ou seja, realizar a encriptação e decriptação das sessões SSL;

6.5 Suporta o envio de tráfego, usando protocolo ICAP (Internet Content Adaptation Protocol), para dispositivos de inspeção;

6.6 Implementa a renegociação de sessão;

6.7 Implementa geração de chaves RSA, enrollment de certificado, importação e exportação de chaves, certificados de servidores;

6.8 A solução suporta protocolo TLS 1.3;

6.9 Possuir uma arquitetura de Proxy, ou seja, terminando as conexões do cliente e do servidor;

6.10 Através da arquitetura de Proxy Permitir negociar cifras e protocolos diferentes da comunicação do lado cliente e do lado servidor;

7. Gerência local

7.1 Permitir o gerenciamento de todas as funcionalidades por interface Web (HTTPS) ou linha de comando (interface console tipo serial e SSH);

7.2 Implementa autenticação, autorização e registro das operações dos administradores através dos protocolos TACACS+ e RADIUS;

7.3 Não deverão existir limitações de licenciamento quanto ao número de usuários, a não ser o limite operacional do equipamento;

7.4 Possuir MIB SNMP;

7.5 Permitir a configuração e gerenciamento de VLANs;

7.6 Possibilitar a coleta de dados de gerenciamento dos equipamentos utilizando os protocolos SNMPv2c e SNMPv3;

7.7 Permitir a configuração de endereços IPs para o envio de traps SNMP (alarmes);

7.8 Implementa mecanismos para criar usuários com no mínimo três conjuntos distintos de privilégios, sendo um deles somente leitura das configurações, para acesso às funções de gerenciamento dos equipamentos, via protocolos SSH, SNMP ou HTTPS;

7.9 Permitir a ativação e desativação de portas;

7.10 Permitir a ativação e desativação de servidores reais e virtuais;

7.11 Permitir a criação e exclusão de VIPs (Virtual IP);

7.12 Permitir a alteração do algoritmo de balanceamento;

7.13 Possuir suporte a MIB II;

7.14 Implementa a MIB privativa que forneça informações relativas ao funcionamento do equipamento;

7.15 Possuir descrição da MIB implementada no equipamento, inclusive a extensão privativa;

7.16 Implementa solução para coibir acesso ao gerenciamento do equipamento através de filtros de endereço IP;

7.17 Permitir o gerenciamento por uma ferramenta de gerência centralizada;

7.18 Suporta e Implementa APIs RESTful para gerenciamento, configuração, automação e integração com outros sistemas de gerenciamento;

7.19 Deverá ser disponibilizada documentação das API dos appliances que compõem a solução;

7.20 Possuir u integração com sistemas de gerenciamento de containers (ex: Kubernetes/Openshift), de modo a Permitir que mudanças dinâmicas na infraestrutura de microserviços sejam refletidas automaticamente no balanceamento de entrada, aumentando ou diminuindo a quantidade de pods, e ainda, inserindo ou removendo serviços;

7.21 Possuir integração com outros sistemas utilizando Ansible e Terraform para automação de configuração;

7.22 A solução é capaz de analisar a performance de aplicações web;

7.23 Possuir relatórios das aplicações;

7.24 Deve prover métricas de aplicações como: Transações por Segundo; Tempo de latência do cliente e servidor; Throughput de requisição e resposta; Sessões;

7.25 Implementa geração de informações para análises históricas e auxiliar nos processos de manutenções preventivas, de troubleshooting, de planejamento de capacidade e de análise da experiência dos usuários finais no acesso das aplicações;

7.26 As informações coletadas deverão permitir a análise dos dados por aplicações, por URL's, por clientes e por servidores, permitindo assim a identificação mais precisa dos eventuais ofensores do tráfego suportado pela solução;

7.27 Implementa geração de informações estatísticas de acesso identificando para cada aplicação os métodos de acesso HTTP (GET e Post), o tipo de sistema operacional utilizado pelos clientes, e os browsers utilizados;

7.28 A geração de informações históricas deverá permitir:

7.29 O detalhamento do tempo de resposta total de carregamento de uma URL e ou Página;

7.30 Permitir a correlação de métricas de uso de rede com o comportamento das aplicações.

8. Licenciamento

8.1 O Licenciamento deverá seguir o modelo Best, com a garantia de atualizações durante a vigência do contrato, abarcando todas as licenças necessárias às funções dos appliances, de acordo com os seguintes módulos:

8.1.1 *Local Traffic Manager* (LTM) - Balanceamento de aplicações, cache em RAM, Certificados SSL, Compressão de Dados, Network Firewall.

8.1.2 *Application Security Manager* (ASM) - Protege as aplicações com desempenho, flexibilidade, investigação, mitigação e relatórios baseado em políticas individualizadas ao nível de cada aplicação

8.1.3 *GTM – Global Traffic Manager* (DNS) - Verifica a saúde de toda a infraestrutura, eliminando os pontos únicos de falha e desviando o tráfego dos sites de baixa performance.

8.1.4 *Application Firewall Manager* (AFM) - Firewall FULL PROXY capaz de inspecionar todo o tráfego que passa através dele.

8.1.5 *Application Policy Manager* (APM) – VPN SSL e controle de acesso Single Sign-on e VPN SSL.

8.1.6 *IP Intelligence* (IPI) - Identifica endereços IP e categorias de segurança associadas a atividades maliciosas.

ANEXO IV – MODELO DE TERMO DE RECEBIMENTO PROVISÓRIO

O modelo abaixo é apenas exemplificativo, podendo sofrer alterações durante a execução do contrato.

Termo de Recebimento Provisório	
Contrato n°	Vigência:
Processo Administrativo nº:	
Contratada:	
Contratante:	
Ordem de Serviço:	
Data da Emissão:	
Objeto:	

Por este instrumento, atestamos, nos termos da Cláusula XX do contrato em epígrafe, que o objeto foi entregue em XX e a sua instalação concluída em XX. O objeto ora recebido provisoriamente não conclui o cumprimento da obrigação, ficando sujeito a posterior verificação de sua qualidade e quantidade.

Ressaltamos que o recebimento definitivo deste bem ocorrerá em até XX dias úteis, desde que não ocorram problemas técnicos ou divergências quanto às especificações constantes do Termo de Referência correspondente ao Contrato supracitado.

Rio de Janeiro, ___ de _____ de 20__.

Fiscal de Contrato 1	**Fiscal de Contrato 2**	**Fiscal de Contrato 3**
<Cargo>	<Cargo>	<Cargo>
<Setor>	<Setor>	<Setor>
<Id Funcional n°>	<Id Funcional n°>	<Id Funcional n°>

ANEXO V – MODELO DE TERMO DE RECEBIMENTO DEFINITIVO

O modelo abaixo é apenas exemplificativo, podendo sofrer alterações durante a execução do contrato.

Termo de Recebimento Definitivo	
Contrato n°	Vigência:
Processo Administrativo nº:	
Contratada:	
Contratante:	
Ordem de Serviço:	
Data da Emissão:	
Objeto:	

ESPECIFICAÇÃO DOS PRODUTOS / SERVIÇOS E VOLUMES DE EXECUÇÃO				
Item	Descrição de Produto e Serviço	Und	Qtd	Total
1				
2				
3				
4				
5				
			TOTAL DOS ITENS	

Por este instrumento, atestamos para fins de cumprimento do disposto na Cláusula XX do Contrato XX, que os serviços e os bens entregues, atendem às exigências especificadas no Termo de Referência do Contrato acima referenciado.

Rio de Janeiro, ___ de _____ de 20__.

Fiscal de Contrato 1	**Fiscal de Contrato 2**	**Fiscal de Contrato 3**
<Cargo>	<Cargo>	<Cargo>
<Setor>	<Setor>	<Setor>
<Id Funcional n°>	<Id Funcional n°>	<Id Funcional n°>

ANEXO VI – MODELO DE AUTORIZAÇÃO DE COMPRA ou ORDEM DE SERVIÇOS

Objeto: <Descrição do objeto>

1. REFERÊNCIA

1.1. Processo Licitatório nº:

1.2. Contrato nº:

1.3. Valor do Contrato: R$ xxxxxxx (valor por extenso).

1.4. Vigência Contratual:

Item	Descrição	Qtd	Und	Valor Unitário	Valor Global
1	Segmentação 1 - *Appliance* de solução integrada de segurança para interligação de redes	2	Unidade	R$	R$
2	Segmentação 2 - *Appliance* de solução integrada de segurança para interligação de internet	2	Unidade	R$	R$
3	Segmentação Concentrador - *Appliance* de solução integrada de segurança para interligação de internet	2	Unidade	R$	R$
4	Suporte técnico (24x7x365) por 12 (doze) meses	1	Serviço	R$	R$
5	Treinamento oficial para a solução F5 BIG-IP por aluno	4	Vaga	R$	R$

1.6. Prazo de entrega: Até o dia xx/xx/20xx

1.7. Responsável pelo recebimento e conferência da entrega:

Pela presente, autorizamos a <Descrever Contratada> a realizar a entrega dos itens na data de _____de _____de 20___, objeto do contrato acima epigrafado, celebrado entre a SECRETARIA DE ESTADO DE FAZENDA e a empresa <Descrever Contratada>.

Rio de Janeiro, _____ de _____de 20___.

Fiscal de Contrato 1	**Fiscal de Contrato 2**	**Fiscal de Contrato 3**
<Cargo>	<Cargo>	<Cargo>
<Setor>	<Setor>	<Setor>
<Id Funcional n°>	<Id Funcional n°>	<Id Funcional n°>

ANEXO VII – TERMO DE SIGILO E CONFIDENCIALIDADE

Os abaixo assinados, de um lado Secretaria de Fazenda do Estado do Rio de Janeiro, com sede na Av. Presidente Vargas Nº 670, doravante denominado SEFAZ-RJ, e de outro lado....., CNPJ Nº ...../0001-01, situada em ....., a Rua: ....., bairro....., doravante denominada CONTRATADA, tem entre si justa e acertada a celebração do presente TERMO DE SIGILO E CONFIDENCIALIDADE, através do qual a CONTRATADA aceita não divulgar sem autorização prévia e judicial segredos e informações sensíveis de propriedade da SEFAZ-RJ e se compromete a praticar procedimentos de segurança da informação, em conformidade com as seguintes cláusulas e condições:

CLÁUSULA PRIMEIRA - A CONTRATADA obriga-se a tratar como "Segredos comerciais e confidenciais" todos os produtos e subprodutos relativos aos serviços contratados.

CLÁUSULA SEGUNDA - Entregar, no momento da rescisão contratual, isto é, do aceite final do projeto, toda e qualquer documentação, material de propriedade do CONTRATANTE.

CLÁUSULA TERCEIRA - Destruir no final do contrato, ou quando for solicitada, toda e qualquer informação além dos produtos de propriedade do CONTRATANTE que estejam em seu poder, tais como bancos de dados, fontes e documentação de programas, fluxos de processo.

CLÁUSULA QUARTA - Não divulgar quaisquer informações a que tenha acesso em virtude dos trabalhos a serem executados, ou de que tenha tomado conhecimento em decorrência da execução do objeto, sem autorização por escrito do CONTRATANTE ou determinação judicial, sob pena de aplicação das sanções cabíveis, além do pagamento de indenização por perdas e danos de acordo com os termos constantes no presente documento.

CLÁUSULA QUINTA - Todas as informações obtidas ou extraídas pela CONTRATADA quando da execução dos serviços deverão ser tratadas como confidenciais, sendo vedada qualquer divulgação a terceiros. Devendo a CONTRATADA zelar por si e por seus sócios e empregados, pela manutenção do sigilo absoluto sobre os dados, informações, documentos, especificações técnicas e comerciais de que eventualmente tenham conhecimento ou acesso em razão dos serviços executados.

PARÁGRAFO ÚNICO – Caso seja constatada a necessidade de quebra de confidencialidade em relação a alguma informação específica, a CONTRATADA só poderá fazê-lo exclusivamente por meio de determinação judicial.

CLÁUSULA SEXTA - Qualquer falha na segurança da informação, identificada por qualquer

colaborador, deve ser imediatamente comunicada a SEFAZ-RJ para avaliação e determinação das ações que se fizerem necessárias.

CLÁUSULA SÉTIMA - Os acessos à rede de dados da SEFAZ-RJ são gerenciados em todos os tipos de conexão, devendo os profissionais ser identificados e ter acessos apenas às informações e aos recursos tecnológicos necessários ao desempenho de suas atividades.

CLÁUSULA OITAVA - A CONTRATADA responderá solidariamente com seus agentes empregados e prepostos, no caso de violação do compromisso de confidencialidade ora assumido, sujeitando-se a arcar com indenização por perdas e danos patrimoniais e morais e/ou lucros cessantes decorrentes da quebra do sigilo;

CLÁUSULA NONA - O acesso à Informação Confidencial será restrito ao profissional alocado para a execução dos SERVICOS. É vedado o controle exclusivo, por apenas um profissional, de um processo de negócio ou recurso.

CLÁUSULA DÉCIMA - Em caso de perda ou extravio de quaisquer informações confidenciais do CONTRATANTE, a CONTRATADA deverá notificar por escrito a CONTRATANTE imediatamente;

CLÁUSULA DÉCIMA PRIMEIRA - A não observância do disposto sobre Confidencialidade torna a PARTE infratora sujeita às sanções previstas nos artigos 86 e 87 da Lei nº 8.666/1993, apuração de responsabilidade criminal em processo administrativo ou judicial, apuração de responsabilidades de acordo com a Lei n° 8.429/1992 (Lei de Improbidade), sem prejuízo, igualmente, de o servidor público responder a processo administrativo disciplinar, com base no Decreto-Lei 220/1975 (Estatuto dos Funcionários Civis do Poder Executivo do Estado do Rio de Janeiro) ou em qualquer outra lei de regência específica das carreiras públicas, como a Lei Complementar nº 69/1990, para o caso dos Auditores Fiscais;

CLÁUSULA DÉCIMA SEGUNDA – A CONTRATADA deve assegurar que todos os seus colaboradores guardarão sigilo sobre as informações que porventura tiverem acesso, mediante a ciência de seus colaboradores em Termo próprio a ser firmado entre a CONTRATADA/colaboradores, no qual os mesmos comprometer-se-ão a informar, imediatamente, ao seu superior hierárquico, qualquer violação das regras de sigilo, por parte dele ou de qualquer pessoa, inclusive nos casos de violação não intencional.

PARÁGRAFO ÚNICO: A coleta dos Termos de Sigilo não exime a CONTRATADA das penalidades por violação das regras por parte de seus contratados.

CLÁUSULA DÉCIMA TERCEIRA – A CONTRATADA compromete-se a estar ciente e em conformidade com as regras estabelecidas na Política de Segurança da Informação da SEFAZ-RJ, devendo atender as seguintes normas:

I - a Lei no 9.983, de 14 de julho de 2000, que dispõe sobre a responsabilidade civil e criminal de usuários que cometam irregularidades em razão do acesso a dados, informações e sistemas informatizados da Administração Pública;

II - o Decreto no 3.505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades de Administração Pública Federal;

III - o Decreto no 4.553, de 27 de dezembro de 2002, que dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal;

CLÁUSULA DÉCIMA QUARTA - O atendimento deste Termo de Sigilo e Confidencialidade bem como da Política de Segurança da Informação da SEFAZ-RJ devem ser incorporados formalmente ao contrato de trabalho dos servidores da CONTRATADA que prestarem serviços a SEFAZ-RJ.

CLÁUSULA DÉCIMA QUINTA - O não cumprimento de quaisquer das cláusulas deste Termo implicará em responsabilização civil, criminal e administrativa, de acordo com a legislação vigente e as obrigações a que alude este instrumento perdurarão, inclusive, após a cessação do vínculo contratual entre a CONTRATADA e a SEFAZ-RJ e abrangem as informações presentes ou futuras, permanecendo as regras do sigilo fiscal.

CLÁUSULA DÉCIMA SEXTA – Fica eleito o Foro da Cidade do Rio de Janeiro, comarca da Capital, para dirimir qualquer litígio decorrente do presente Termo que não possa ser resolvido por meio amigável, com expressa renúncia a qualquer outro, por mais privilegiado que seja.

Rio de Janeiro, ____ de _____ 20xx.

_____ _____

SEFAZ-RJ Responsável do Contrato pela empresa