

TERMO DE REFERÊNCIA

AQUISIÇÃO DE PRODUTOS E SERVIÇOS PARA ATUALIZAÇÃO TECNOLÓGICA DE SOLUÇÃO DE SEGURANÇA, INCLUINDO FIREWALL DE APLICAÇÃO AVANÇADO PARA WEB E APIs (WAAP), PROTEÇÃO INTELIGENTE DE REPUTAÇÃO DE IP, BALANCEAMENTO DE CARGA AVANÇADO, PROTEÇÃO PARA APLICAÇÃO E PROTEÇÃO E ORQUESTRAÇÃO DE TRÁFEGO SSL DO FABRICANTE F5 NETWORKS, COMPOSTA POR EQUIPAMENTOS, SOFTWARES, LICENCIAMENTO E INSUMOS, INCLUINDO INSTALAÇÃO, CONFIGURAÇÃO, SUPORTE, GARANTIA E MANUTENÇÃO.

junho de 2026.

1. DO OBJETO

- 1.1. A presente licitação tem por objeto a aquisição de produtos e serviços para atualização tecnológica de solução de segurança, incluindo Firewall de Aplicação Avançado para Web e APIs (WAAP), Proteção Inteligente de Reputação de IP, Balanceamento de Carga Avançado, Proteção para Aplicação e Proteção e Orquestração de tráfego SSL do fabricante F5 Networks, composta por equipamentos, softwares, licenciamento e insumos, incluindo instalação, configuração, suporte, garantia e manutenção. A solução tem como objetivo a atualização e modernização da solução de proteção da F5 Networks atualmente instalada e operacional na camada interna da infraestrutura computacional da IPLANRIO. Os itens deste documento estão caracterizados e especificados neste Termo de Referência.
- 1.2. O objeto descrito neste Termo de Referência é caracterizado como comum, sendo cabível a utilização da modalidade de licitação denominada Pregão, tendo em vista que foi objetivamente definido neste documento por meio de especificações usuais do mercado.
- 1.3. Trata-se de objeto disponível em mercado próprio, fornecido habitualmente, independentemente da demanda da Administração, de forma padronizada, sem a exigência de atendimento de qualquer especificidade ou variantes de adequação.
- 1.4. Todos os itens necessários para a instalação dos novos equipamentos e a integração ao ambiente atualmente operacional, encontram-se no item 2, tabela 1, a seguir, incluindo os equipamentos, cabos, interfaces, softwares, licenças e serviços de suporte técnico.
- 1.5. A solução deve incluir todos os cabos e acessórios necessários para as conexões dos equipamentos ao ambiente atualmente em operação.

2. DA DESCRIÇÃO DOS SERVIÇOS, MATERIAIS/EQUIPAMENTO (S)

LOT E	ITEM	PARTNUMBER	DESCRIÇÃO	QTD.
1	1	F5-F5-BIG-LTM-R5600_BND-014	SOLUTION: 1X F5-BIG-LTM-R5600, 1X F5-UPG-AC-R5XXX	2

	2	F5-F5-SVC-BIG-PRE-HW369	BIG-IP SERVICE PREMIUM CAT HW369	4
	3	F5-F5-ADD-BIG-R56R58	BIG-IP R5600 TO R5800 LICENSE UPGRADE	2
	4	F5-F5-SVC-BIG-PRE-SW102	BIG-IP SERVICE PREMIUM CAT SW102	4
	5	F5-F5-ADD-BIG-GBT-R58XX	BIG-IP LOCAL TRAFFIC MANAGER TO BEST BUNDLE UPGRADE FOR R5800	2
	6	F5-F5-SVC-BIG-PRE-SW472	BIG-IP SERVICE PREMIUM CAT SW472	4
	7	F5-F5-SBS-BIG-TC-2-1YR	BIG-IP THREAT CAMPAIGNS LICENSE FOR R5X00 I7X00 I5X00 ADVANCED WEB APPLICATION FIREWALL 1-YEAR SUBSCRIPTION	4
	8	F5-F5-SBS-BIG-IPI-5-1YR	BIG-IP IP INTELLIGENCE LICENSE FOR R5X00 I5X00 1-YEAR SUBSCRIPTION	4
	9	F5-F5-ADD-BIG-SSLOR5XXX	BIG-IP SSL ORCHESTRATOR LICENSE FOR R5XX0	2
	10	F5-F5-SVC-BIG-PRE-SW512	BIG-IP SERVICE PREMIUM CAT SW512	4
	11	F5-F5-UPG-SFP+-R	F5: FIELD UPGRADE SFP FIBER CONNECTOR 10G-LC850NM ROHS	8
	12	SERVIÇOS	SERVIÇOS DE SUPORTE TÉCNICO ESPECIALIZADO 24 x 7.	24 MESES
2	13	SERVIÇOS	SERVIÇOS DE MONTAGEM, INSTALAÇÃO E CONFIGURAÇÃO	1

Tabela 1

Obs: os lotes são apenas para uma divisão prática e de entendimento entre produtos e serviços, não se tratando de lotes divisíveis para fins de contratação;
Obs 2: o serviço de montagem manutenção, instalação e configuração se dá em momento único e por isso a quantidade 1, não será dividido em meses, visto que seu pagamento se dará após a sua conclusão e em pagamento único.

2.1. ESPECIFICAÇÕES TÉCNICAS

2.1.1. O fabricante F5 Networks separa os itens de equipamentos (hardwares), softwares, licenças e subscrições em diferentes partes em seu catálogo e alguns itens precisam ser compostos por partes oferecidas com duração de 1 (um) e 2 (dois) anos para atingir os 2 (dois) anos de atualizações e suporte previstos para a solução:

2.2. LOTE 1 – ITEM 1 – SOLUTION: 1X F5-BIG-LTM-R5600, 1X F5-UPG-AC-R5XXX – 2 (duas) unidades

2.2.1. Este item corresponde aos appliances F5 BIG-IP r5600, fornecidos em formato de solução integrada, incluindo fonte de alimentação AC adicional, destinados a operar

em cluster redundante (alta disponibilidade), garantindo continuidade de serviço, balanceamento de carga, segurança e desempenho para aplicações críticas.

2.3. LOTE 1 – ITEM 2 – BIG-IP Service Premium CAT HW369 – 4 (quatro) unidades

2.3.1. Fornecimento de suporte técnico premium oficial do fabricante F5 Networks, com cobertura de hardware para os appliances BIG-IP r5600, em regime 24x7x365, incluindo atendimento avançado, substituição de peças e acesso ao TAC do fabricante.

2.4. LOTE 1 – ITEM 3 – BIG-IP r5600 to r5800 License Upgrade – 2 (duas) unidades

2.4.1. Licenciamento de upgrade de plataforma, permitindo a elevação dos appliances BIG-IP da linha r5600 para r5800, assegurando maior capacidade de processamento, escalabilidade e aderência às evoluções tecnológicas da solução.

2.5. LOTE 1 – ITEM 4 – BIG-IP Service Premium CAT SW102 – 4 (quatro) unidades

2.5.1. Fornecimento de suporte técnico premium oficial do fabricante F5 Networks para software, contemplando atualizações, correções, novos releases e acesso ao suporte especializado, em regime 24x7x365, para os appliances da solução.

2.6. LOTE 1 – ITEM 5 – BIG-IP Local Traffic Manager to Best Bundle Upgrade for r5800 – 2 (duas) unidades

2.6.1. Licenciamento do tipo Best Bundle, ampliando as funcionalidades dos appliances F5 BIG-IP, contemplando, entre outros recursos, balanceamento de carga avançado, DNS, proteção contra ataques DDoS e recursos adicionais de segurança e performance.

2.7. LOTE 1 – ITEM 6 – BIG-IP Service Premium CAT SW472 – 4 (quatro) unidades

2.7.1. Este item corresponde ao suporte técnico premium oficial do fabricante F5 Networks para o ciclo de vida do software associado ao Best Bundle, garantindo acesso contínuo a atualizações, melhorias e suporte especializado, em regime 24x7x365.

- 2.8. **LOTE 1 – ITEM 7 – BIG-IP Threat Campaigns License – 1-Year Subscription – 4 (quatro) unidades**
- 2.8.1. Licenciamento por subscrição de Threat Campaigns, voltado à proteção contra campanhas de ataques conhecidos e emergentes, integrando inteligência de ameaças à solução de Web Application Firewall (WAF), pelo período de 1 (um) ano.
- 2.9. **LOTE 1 – ITEM 8 – BIG-IP IP Intelligence License – 1-Year Subscription – 4 (quatro) unidades**
- 2.9.1. Licenciamento por subscrição do módulo IP Intelligence, permitindo o bloqueio proativo de acessos provenientes de endereços IP maliciosos, com base em reputação global mantida pelo fabricante, pelo período de 1 (um) ano.
- 2.10. **LOTE 1 – ITEM 9 – BIG-IP SSL Orchestrator License for r5XX0 – 2 (duas) unidades**
- 2.10.1. Licenciamento do módulo SSL Orchestrator, responsável pela inspeção, orquestração e gerenciamento do tráfego criptografado, possibilitando integração com soluções de segurança e garantindo visibilidade e controle sobre comunicações SSL/TLS.
- 2.11. **LOTE 1 – ITEM 10 – BIG-IP Service Premium CAT SW512 – 4 (quatro) unidades**
- 2.11.1. Fornecimento de suporte técnico premium oficial do fabricante F5 Networks específico para os módulos de segurança e orquestração SSL, incluindo atualizações, novos releases e suporte avançado, em regime 24x7x365.
- 2.12. **LOTE 1 – ITEM 11 – Field Upgrade SFP Fiber Connector 10G-LC850nm ROHS – 8 (oito) unidades**
- 2.12.1. Equipamentos do tipo SFP+ (GBIC), conectores ópticos de 10Gb, destinados à interconexão dos appliances F5 ao ambiente de rede existente, garantindo alta taxa de transferência e compatibilidade com a infraestrutura instalada.
- 2.13. **LOTE 2 – ITEM 12 – Serviços de suporte técnico especializado**
- 2.13.1. Serviços de suporte técnico especializado, pelo período de 24 (vinte e quatro) meses, destinados à sustentação operacional do ambiente descrito no Lote 1, incluindo apoio técnico, troubleshooting, ajustes e orientações

especializadas.

2.14. LOTE 2 – ITEM 13 – Serviços de montagem, instalação e configuração

- 2.14.1. Prestação de serviços especializados de montagem, instalação e configuração da solução descrita no Lote 1, incluindo integração ao ambiente atualmente em operação, seguindo as melhores práticas do fabricante F5 Networks.

3. CARACTERÍSTICAS GERAIS DA SOLUÇÃO

- 3.1. A solução deverá ser composta de hardware e software licenciado, do fabricante F5 Networks, com o objetivo de manter a compatibilidade e padronização da solução atualmente instalada e operacional nas dependências da IPLANRIO, modernizando-a para atender às novas e futuras necessidades;
- 3.2. Serão aceites apenas os produtos listados na tabela 1, ou superiores, com no mínimo as mesmas funções e capacidades detalhadas no descritivo técnico (datasheet) dos produtos, parte integrante deste documento, caso o fabricante lance produtos atualizados compatíveis em substituição aos listados na tabela 1.
- 3.3. Todos os componentes de hardware devem ser próprios para montagem em rack “19” e deverão ser fornecidos pela Contratada, incluindo kit tipo trilho para adaptação, cabos de alimentação, suportes, gavetas e braços, se necessário;
- 3.4. Na data da proposta, nenhum dos modelos ofertados poderá estar/ser listado no site do fabricante em listas de end-of-life, end-of-support e/ou end-of-sale;

4. DO FORNECIMENTO E LOCAL DE ENTREGA DOS OBJETOS

- 4.1. Os equipamentos, softwares e licenças deverão ser entregues na IPLANRIO, no endereço Rua Afonso Cavalcanti, 455, Bloco II, sala 307 do prédio CASS (Centro Administrativo São Sebastião), Cidade Nova, Rio de Janeiro, RJ, em até 60 (sessenta) dias contados da data da assinatura do contrato, em parcela única, dispensando cronograma de execução física e financeira.
- 4.2. Deverão ser entregues os acessórios necessários à instalação dos produtos, incluindo kit tipo trilho para adaptação, cabos de alimentação, suportes, gavetas e braços, se necessário;

- 4.3. Os itens deverão ser entregues novos, sem uso, lacrados, sem avarias, acompanhados de suas notas fiscais e documentos legais necessários.

5. DO PARCELAMENTO DO OBJETO

- 5.1. Embora no descritivo contenha descrição de funcionalidades específicas, não é possível que a contratação dos equipamentos e licenças do lote 1 seja feita de forma parcelada, dado o conceito de solução, integração, administração e gestão;
- 5.2. Os itens do lote 1 não podem ser divididos em sub-lotes, por se tratar de um conjunto de equipamentos e licenças de software para uma mesma solução, com características modulares. Trata-se da atualização e modernização da atual solução já existente, com inclusão de novas funcionalidades necessárias para se elevar a segurança do ambiente como um todo.
- 5.3. Produtos similares de outros fabricantes não se integrariam completamente à solução existente, sendo o custo de aquisição, treinamento e esforço administrativo de migração do atual ambiente e aquisição de todos os produtos necessários, muito maior, sem contar o tempo de implantação.
- 5.4. O suporte centralizado também ficaria inviabilizado caso partes de uma mesma solução tivessem de ser atendidas por diferentes fornecedores;

6. QUANTITATIVOS ESTIMADOS

- 6.1. Conforme disposto trata-se de solução composta por dois Lotes, em quantidade de 13 itens no total.
- 6.2. A solução deve atender às quantidades estimadas para cada um dos itens, conforme descrito na tabela 1 do item 2.

7. PRAZO DA CONTRATAÇÃO

- 7.1. O prazo de vigência inicia-se com a assinatura do contrato e encerra-se 120 (cento e vinte) dias após, sem prejuízo da garantia, assistência e suporte técnico dos bens.
- 7.2. O prazo de garantia dos serviços será durante toda a vigência do contrato, contados a partir da emissão do aceite definitivo destes pela Comissão de Fiscalização da CONTRATANTE.

8. FUNDAMENTOS DA CONTRATAÇÃO E JUSTIFICATIVA

Justifica-se a Aquisição em três aspectos fundamentais: a justificativa da necessidade de aquisição do objeto; a razão do quantitativo demandado; a motivação para as especificações técnicas exigidas - os quais passamos a apresentar:

8.1. JUSTIFICATIVA DA NECESSIDADE

8.1.1. Considerando a portaria Nº 123, de 28 de maio de 2010, e;

8.1.2. Considerando a deliberação Nº 001 de 28 de março de 2018, e;

8.1.3. Considerando o decreto Rio Nº 53.700 de 8 de dezembro de 2023, que determinam, entre outras obrigações:

8.1.3.1. Que a manutenção de níveis adequados de segurança das informações tratadas pela Administração Pública Municipal é requisito imprescindível à consolidação de sua credibilidade junto ao cidadão.

8.1.3.2. Que é crucial a manutenção da integridade, disponibilidade, confidencialidade e autenticidade das informações tratadas pelos órgãos e entidades municipais visando garantir a confiabilidade de seus processos e serviços.

8.1.3.3. Que as informações são armazenadas em diferentes formas, veiculadas em diferentes meios, sejam físicos ou digitais, sendo, portanto, vulneráveis a incidentes como desastres naturais, acessos não autorizados, mau uso, falhas de equipamentos, extravio e furto.

8.1.3.4. Que existe a necessidade de aprimoramento contínuo das ações de governança e gestão de Segurança da Informação visando à sua compatibilização aos cenários de risco cibernético continuamente em evolução.

8.1.3.5. Que as informações são ativos de propriedade do Município, devendo, portanto, ser tomadas as medidas necessárias para protegê-las de alteração, destruição e divulgação não autorizadas, quer seja acidental ou intencional.

8.1.4. Tendo como referência as camadas de segurança cibernética expressas no despacho da Presidência da IPLANRIO (expediente de 17/08/2022: constante do diário oficial de 18/08/2022), visando à atualização da camada "Gestão da Infraestrutura de Rede", considerando a justificativa descrita abaixo, solicito a contratação de solução para ambientes da Data Center em conformidade

com todos os requisitos descritos no Termo de Referência que segue em anexo.

- 8.1.5. A Prefeitura do Rio disponibiliza aos servidores e aos cidadãos diversos sistemas corporativos e departamentais, tendo como política de qualidade assegurar a melhoria contínua da prestação dos serviços, propiciando um atendimento mais acessível, rápido e efetivo aos cidadãos e usuário internos.
- 8.1.6. A IPLANRIO tem como missão institucional garantir a disponibilidade, integridade e confidencialidade dos citados sistemas, essenciais ao funcionamento da Prefeitura do Rio.
- 8.1.7. O papel da Tecnologia como instrumento indutor do desenvolvimento social e econômico é cada vez mais fundamental. A Tecnologia da Informação vem assumindo uma importância cada vez maior para que se possa ampliar o acesso ao conhecimento e facilitar a comunicação, de forma cada vez mais efetiva com o cidadão;
- 8.1.8. Ao longo dos anos a IPLANRIO tem investido em recursos de tecnologia da informação e comunicação, de forma a assegurar o desempenho de suas atividades institucionais, possibilitando o tratamento de um grande e variado conjunto de informações;
- 8.1.9. Atualmente, mais de noventa por cento de todo o tráfego da Internet é criptografado por meio dos protocolos SSL/TLS para que a comunicação entre um cliente e um servidor ocorra de forma segura. Entretanto muitos cibercriminosos fazem o uso da criptografia para ocultar conteúdo malicioso ou extrair informações sigilosas de pessoas ou corporações podendo comprometer a integridade, a disponibilidade e a confidencialidade das informações. O desencapsulamento do tráfego SSL pelo BIG-IP para a posterior inspeção aumenta significativamente a segurança da rede da PREFEITURA ao possibilitar a análise desse tipo de tráfego permitindo a entrada e a saída apenas do tráfego benigno e desejado;
- 8.1.10. O balanceamento de carga do sistema BIG-IP é necessário para distribuir de forma igualitária as requisições a uma mesma aplicação hospedada em dois ou mais hosts servidores resultando em um melhor aproveitamento dos recursos de hardware e da rede e

ainda, em conjunto com o Firewall Chek-Point, priorizar o tráfego das aplicações que são de maior relevância para a PREFEITURA, por meio de configurações aplicadas de qualidade de serviço (QoS) otimizando a utilização dos links de internet contratados junto a operadora de telecomunicações;

- 8.1.11. A universalização dos sistemas e dos serviços a partir de plataforma tecnológica homogênea, tecnicamente apta a operar nos padrões do ecossistema digital, caracterizado pela abundância de dados abertos e transparentes e por fortes oscilações elásticas no consumo de infraestrutura. Diante deste contexto, verifica-se a necessidade premente de atualização e modernização dos equipamentos e serviços que ofereçam respostas efetivas e imediatas às demandas de negócio programadas e repentinas, bem como ofereça níveis de segurança ativa e passiva, garantindo a continuidade das ofertas dos sistemas e serviços da PREFEITURA. A aquisição em pauta objetiva realizar a atualização tecnológica e a modernização da Solução de Proteção à camada de aplicação da PREFEITURA;
- 8.1.12. Um dos trabalhos primordiais de um equipamento de rede é o de fornecer acesso às aplicações e serviços aos usuários. Porém, conforme o crescimento das necessidades da Instituição, a infraestrutura fica cada vez mais complexa e a demanda aumenta na mesma velocidade. A forma mais eficiente de dar conta das tarefas diárias e de novas demandas é avançar o balanceamento de carga e ampliar o monitoramento para ajudar a acrescentar mais servidores e a direcionar o tráfego sem interrupções;
- 8.1.13. Entretanto os equipamentos possuem ciclo de vida e obsolescência tecnológica de hardware e software e necessitam de atualizações pontuais ao longo da vida;
- 8.1.14. Novas matrizes de hardware e funcionalidades avançadas são adicionadas constantemente em resposta ao avanço da quantidade e complexidade dos ciberataques;
- 8.1.15. Os diversos incidentes de segurança reportados diariamente nos noticiários têm mostrado que, uma vez transpostas as defesas de perímetro, praticamente não haverá mais resistência à continuidade dos ataques. Com isso, faz-se necessária a atualização e modernização da solução empregada dando continuidade à proteção destas ameaças que podem estar em qualquer lugar (incluindo o

perímetro da rede).

- 8.1.16. Independentemente dos motivadores e dos artifícios utilizados pelos atacantes (hackers) durante um ataque cibernético, suas ações costumam seguir um padrão estruturado e gradual composto por algumas fases.
- 8.1.17. As primeiras fases tratam essencialmente do reconhecimento do ambiente a ser atacado (alvo) e a identificação de suas vulnerabilidades. Uma vulnerabilidade é uma fragilidade presente ou associada a um ativo (ex. uma falha no sistema operacional que permite que um atacante possa realizar ações não autorizadas no equipamento, uma estação de trabalho que não possui antivírus instalado), por esta razão são necessárias atualizações constantes e a manutenção da arquitetura atualmente utilizada na PREFEITURA, que se mostrou ser efetiva para enfrentar os desafios desse tipo de ataque.
- 8.1.18. Diante do cenário de risco cibernético potencial trazido pela presença das vulnerabilidades nos ativos de Tecnologia da Informação e Comunicação (TIC), uma vez que são "a porta de entrada" para as ameaças, principalmente em organizações com grande quantitativo de ativos de TIC, torna-se crucial a presença de uma solução automatizada que possa suportar um processo contínuo e eficiente de identificação, análise e tratamento de vulnerabilidades, visando à redução dos riscos de comprometimento destes ativos e, por consequência, dos processos, serviços e informações que estes estejam suportando.
- 8.1.19. Também há o aumento dos ataques às aplicações, que por algum fator possuam alguma vulnerabilidade em seu código, seja por necessidade de compatibilidade com sistemas legados ou pelo surgimento de novas vulnerabilidades. Para estes casos entra em ação os módulos de defesa WAAP (Web Application and Api Protection), ou proteção de aplicações web e APIs.
- 8.1.19.1. O WAAP É um conceito mais amplo que engloba o WAF (Web Application Firewall), mas oferece proteção adicional a APIs, que são interfaces de comunicação entre aplicações, extensamente utilizadas pelos sistemas da PREFEITURA.
- 8.1.19.2. O WAAP ainda conta com proteção contra BOTs, que são programas automatizados que simulam ações humanas ao acessar uma aplicação, eliminando este

risco, pois os BOTs são largamente utilizados como vetores de ataques cibernéticos.

8.1.19.3. O WAAP ajuda ainda a mitigar os ataques DDoS, ajudando a absorver e redirecionar o tráfego malicioso de ataques DDoS evitando que sua aplicação fique indisponível.

8.1.20. A Prefeitura através da IPLANRIO possui hoje uma solução cluster de firewalls e balanceadores de carga do fabricante F5 Networks, mais especificamente do modelo BIG-IP i5800, atualmente instalados e operacionais em seu Datacenter, que cumprem algumas funções relacionadas a proteção e segurança do ambiente de aplicações on premises.

8.1.21. Ocorre que tais equipamentos atingiram o ciclo máximo de vida não sendo mais comercializados, conforme podemos observar em link de conhecimento público (f5.com/article/K000133583), disponibilizado pelo fabricante do equipamento, impossibilitando assim que o mesmo seja atualizado e capacitado com novas funcionalidades.

8.1.22. O Cenário proposto, trata da atualização da camada de proteção das aplicações WEB e APIs com balanceamento avançado, agregando novas funcionalidades como licenciamento por subscrição para Threat Campaigns, voltado à proteção contra campanhas de ataques conhecidos e emergentes, licenciamento para subscrição do módulo IP Intelligence, permitindo o bloqueio proativo de acessos provenientes de endereços IP maliciosos, com base em reputação global mantida pelo fabricante F5 Networks e licenciamento do módulo SSL Orchestrator, responsável pela inspeção, orquestração e gerenciamento do tráfego criptografado, possibilitando integração com soluções de segurança e garantindo visibilidade e controle sobre comunicações SSL/TLS.

8.2. CENÁRIO PROPOSTO:

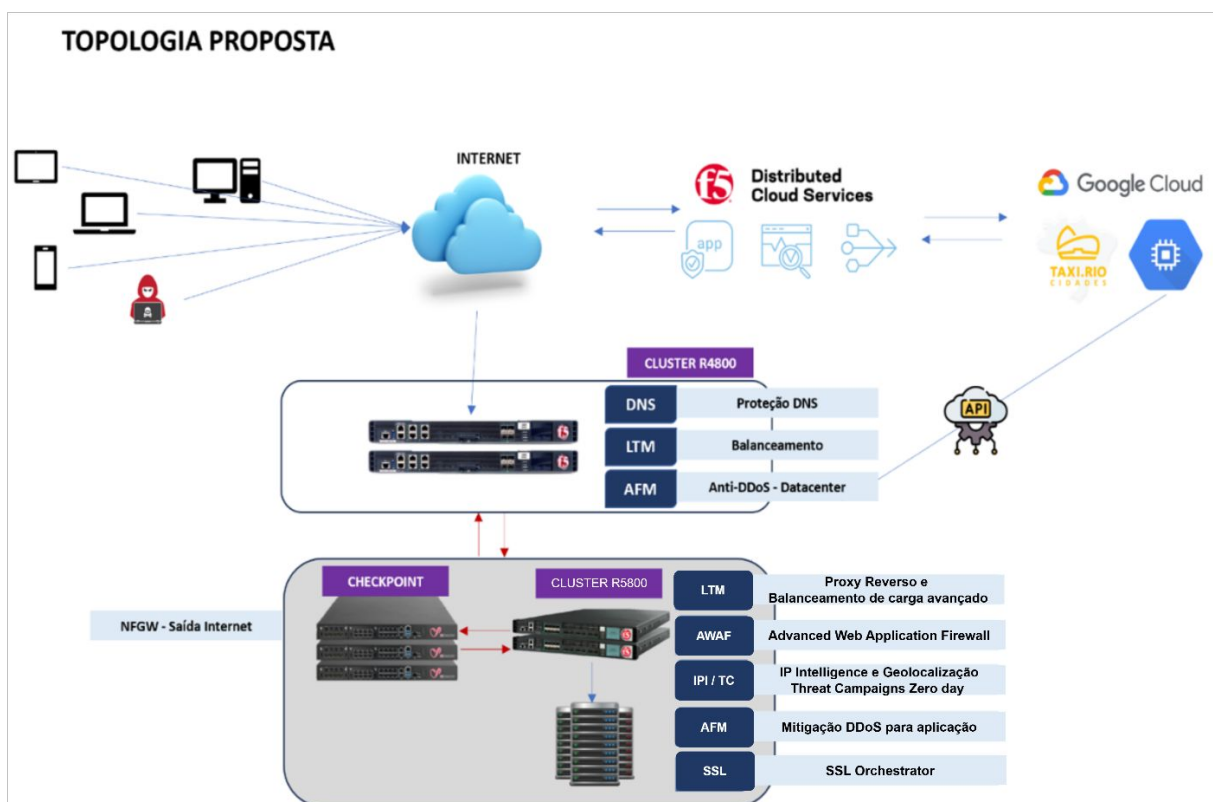


Figura 1

8.2.1. Com a atualização dos equipamentos será possível manter as camadas de segurança atuais, garantido os mesmos níveis de serviço, além de agregar novas características de proteção e novas funcionalidades, como por exemplo, Orquestração do tráfego SSL.

8.2.2. Benefícios da Proteção de Segurança em Camadas:

8.2.2.1. **Defesa mais abrangente:** A combinação de diferentes tipos de firewalls pode ajudar a proteger contra uma variedade mais ampla de ataques.

8.2.2.2. **Maior flexibilidade:** Cada camada de firewall pode ser configurada para atender às necessidades específicas da organização.

8.2.2.3. **Melhor desempenho:** As diferentes camadas de firewall podem ser distribuídas em diferentes dispositivos, o que pode ajudar a melhorar o desempenho da rede.

8.2.2.4. **Maior segurança:** A proteção de segurança de firewalls em camadas é uma estratégia que utiliza diferentes tipos de firewalls em conjunto para fornecer uma defesa mais abrangente contra ameaças à segurança da rede. Cada camada de firewall oferece um conjunto específico

de recursos de segurança, e a combinação de diferentes firewalls pode ajudar a proteger contra uma variedade mais ampla de ataques.

- 8.2.2.5. **Maior tempo para resposta aos ataques:** cada camada de firewall é uma barreira a ser derrubada pelo invasor, o que proporciona um tempo precioso para que as equipes de segurança detectem e tomem ação já na primeira camada, garantindo o ambiente seguro pela segunda camada, enquanto se mitiga ou elimina a ameaça.

8.3. JUSTIFICATIVA DOS QUANTITATIVOS

- 8.3.1. Os quantitativos especificadas na tabela 1, no item 2, foram dimensionadas pela equipe técnica da IPLANRIO, com base nas melhores práticas de mercado e das necessidades atuais e futuras, considerando:
- 8.3.1.1. Se faz necessário que cada componente possua uma redundância, visando manter a continuidade dos serviços em casos de falhas isoladas de componentes, eliminando desta forma os pontos únicos de falhas;
- 8.3.2. São necessárias redundâncias nas conexões de fibra óptica e demais cabos, visto que são usadas para gerar redundância e aumentar a banda de conexão dos dados;
- 8.3.3. São necessários os licenciamentos dos softwares que atuarão nas camadas de proteção em nuvem, visando atender à demanda das aplicações WEB.

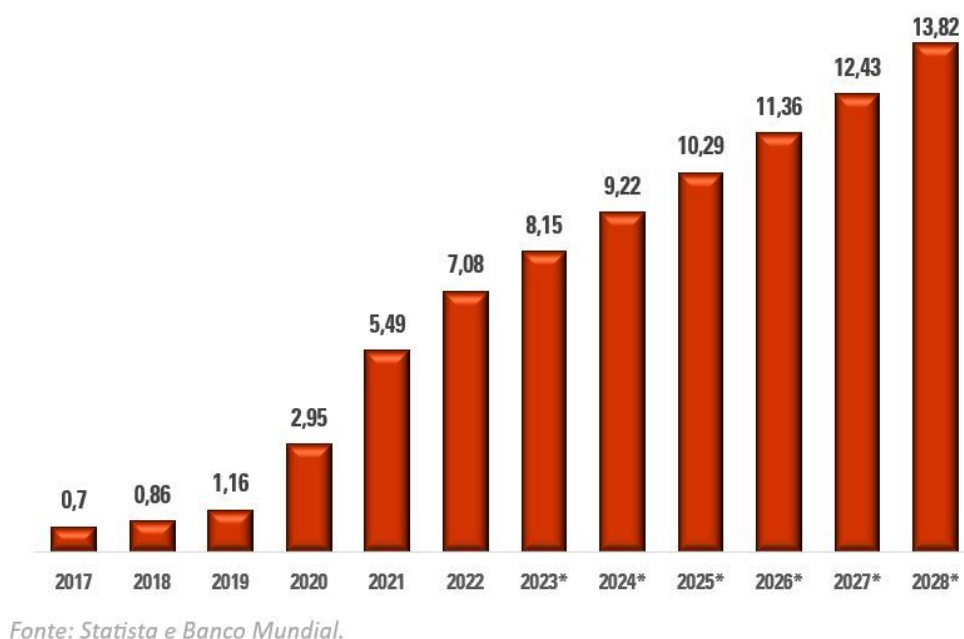
8.4. MOTIVAÇÃO PARA AS ESPECIFICAÇÕES TÉCNICAS

- 8.4.1. A IPLANRIO hospeda inúmeros sistemas, com dados sigilosos e sensíveis, que necessitam de proteção, integridade, confiabilidade e disponibilidade, para serem acessados e utilizados por quem necessitar e possuir os direitos de acesso, conforme rege a atual legislação.
- 8.4.2. Para atingir estes objetivos, e com o crescente aumento de sistemas digitais disponibilizados à população, se faz necessário que a infraestrutura esteja apta a manter os sistemas protegidos, com total disponibilidade, sem pontos únicos de falhas, e com capacidade suficiente para atender as atuais e futuras demandas.
- 8.4.3. As especificações técnicas foram elaboradas com base nas atuais necessidades da PREFEITURA, tendo em vista a enorme necessidade de proteção contra ataques DDoS,

ataques às APIs e às aplicações propriamente ditas.

- 8.4.4. Abaixo gráfico demonstrativo com base em estudos do Banco Mundial sobre aumento dos custos associados aos aumentos dos ataques cibernéticos:

Custo Estimado dos Crimes Cibernéticos no Mundo 2017-2028
Trilhões US Dólares



9. OBJETIVOS A SEREM ALCANÇADOS:

- 9.1. Aprimoramento da solução atual, incluindo as seguintes funcionalidades:

9.1.1. **Proteção abrangente:** A combinação de diferentes firewalls em camadas oferece uma defesa mais robusta contra uma variedade de ameaças, como ataques de rede, malware, phishing e DDoS, incluindo estas funcionalidades nos ambientes de cloud;

9.1.2. **Visibilidade e controle granulares:** Cada camada fornece informações específicas sobre o tráfego de rede, permitindo um controle mais preciso sobre o que entra e sai do datacenter e da cloud;

9.1.3. **Segmentação de rede aprimorada:** As camadas de firewall serão usadas para segmentar a rede em zonas com diferentes níveis de segurança, limitando o acesso a recursos críticos e protegendo dados confidenciais, criando uma camada de proteção à frente do perímetro;

9.1.4. **Escalabilidade e flexibilidade:** As soluções de firewall em camadas serão dimensionadas para atender às necessidades específicas do ambiente, permitindo adicionar ou remover firewalls conforme

necessário, utilizando contextos virtualizados;

- 9.1.5. **Alta disponibilidade e resiliência:** As camadas de firewall serão configuradas para redundância, garantindo que a rede permaneça protegida mesmo em caso de falha de um dispositivo, aumentando a robustez da infraestrutura de segurança;

10. DA DESCRIÇÃO DA SOLUÇÃO DE TIC COMO UM TODO

- 10.1. Trata-se da aquisição de produtos e serviços para atualização tecnológica de solução de segurança constituída de um cluster com appliances físicos em alta disponibilidade, incluindo Firewall de Aplicação Avançado para Web e APIs (WAAP), Proteção Inteligente de Reputação de IP, Balanceamento de Carga Avançado, Proteção Anti DDoS para Aplicação e Proteção e Orquestração de tráfego SSL do fabricante F5 Networks, composta por hardwares, softwares, licenciamento e insumos, incluindo instalação, configuração, suporte, garantia e manutenção, visando a atualização e modernização da solução de proteção da F5 Networks atualmente instalada e operacional na camada interna da infraestrutura computacional da IPLANKRIO pelo prazo de 24 (vinte e quatro) meses de acordo com as especificações e condições constantes neste documento.

11. ESPECIFICAÇÃO TÉCNICA DETALHADA DOS ITENS

11.1. CARACTERÍSTICAS ESPECÍFICAS DO APPLIANCE:

- 11.1.1. Cada appliance deve possuir a capacidade mínima para tratar 95 Gbps processando em camada 4 (L4);
- 11.1.2. Possuir capacidade mínima para tratar 85 Gbps processando em camada 7 (L7) sem inspeção de WAF habilitada;
- 11.1.3. Possuir capacidade mínima para tratar ~3,3 milhões (três milhões e trezentos mil) de requisições em L7 com WAF habilitado (capacidade de requisições por segundo já contemplada nos RPS máximos);
- 11.1.4. Possuir capacidade de compressão de 40 (quarenta) Gbps;
- 11.1.5. Possuir capacidade de manter, no mínimo, 85.000.000 (oitenta e cinco milhões) de conexões simultâneas na camada 4;
- 11.1.6. Ter capacidade de tratar ~1.400.000 (um milhão e quatrocentos mil) novas conexões em L4 por segundo;

- 11.1.7. Ter capacidade de tratar 80.000.000 (oitenta milhões) de SYN Cookies por segundo;
- 11.1.8. Ter capacidade de tratar ~3.300.000 (três milhões e trezentos mil) requisições em camada 7 por segundo;
- 11.1.9. Possuir capacidade de processar 45 (quarenta e cinco) Gbps de throughput de tráfego SSL bulk (com RSA 2048 bits);
- 11.1.10. Processar ~80.000 (oitenta mil) transações por segundo TLS com RSA 2K;
- 11.1.11. Processar ~50.000 (cinquenta mil) transações por segundo TLS com ECDHE-ECDSA P-256;
- 11.1.12. Deve possuir no mínimo 02 (duas) portas QSFP+ 40 G / QSFP28 100G;
- 11.1.13. Deve possuir no mínimo 08 (oito) portas SFP28/SFP+ 25G/10G;
- 11.1.14. Cada appliance deve vir acompanhado de seus respectivos módulos, sendo, no mínimo, 04 (quatro) módulos SFP+ 10GBASE-SR;
- 11.1.15. Deve possuir uma interface 1000BASE-T UTP RJ45 dedicada para gerenciamento;
- 11.1.16. Possuir uma interface USB 3.0 para transferência de arquivos;
- 11.1.17. Possuir interface serial para gerenciamento;
- 11.1.18. Não serão aceitos equipamentos servidores e SO genéricos, somente appliance dedicado;
- 11.1.19. Permitir a criação de, pelo menos, 18 (dezoito) instâncias isoladas (tenants) com planos de dados/controle independentes;
- 11.1.20. Possuir disco interno com tecnologia SSD (1 TB M.2);
- 11.1.21. Possuir fontes internas redundantes (Dual PSU);
- 11.1.22. Possuir altura máxima de 01 (um) RU compatível com rack 19”;
- 11.1.23. A solução deve permanecer operante após fim de garantia sem interrupção de tráfego ou funcionalidades, sendo permitida apenas a cessação de atualizações de assinaturas/bases.

11.2. REQUISITOS GERAIS

- 11.2.1. Suportar IPv4 e IPv6;

- 11.2.2. Suportar múltiplas tabelas de roteamento independentes em IPv4 e IPv6;
- 11.2.3. Suportar VXLAN para integração com o ambiente de virtualização;
- 11.2.4. Suportar configuração de endereçamento IP estático e dinâmico (DHCP/BOOTP) para o gerenciamento;
- 11.2.5. Suportar implementação em alta disponibilidade,
- 11.2.6. Implementar modo ativo/standby;
- 11.2.7. Suportar modo ativo/ativo para, pelo menos, as funções de balanceamento de servidores. Aceita-se como ativo/ativo a utilização de dois endereços virtuais, onde cada endereço fica ativo em um elemento e standby no outro;
- 11.2.8. Permitir a sincronização das configurações de forma automática e manual, forçando a sincronização quando necessário;
- 11.2.9. Permitir utilizar qualquer endereçamento IP, inclusive os definidos na RFC 1918, para criação de cluster, heartbeat e sincronização entre os equipamentos;
- 11.2.10. Fornecer todos os recursos de redundância da solução sem nenhuma despesa com licenças adicionais;
- 11.2.11. Permitir expansão do cluster adicionando novos equipamentos inclusive de modelos diferentes;
- 11.2.12. Possuir interface gráfica via web e interface via CLI por SSH e console para administração, gerenciamento e monitoramento do equipamento;
- 11.2.13. Implementar o SNTP (Simple Network Time Protocol) ou NTP (Network Time Protocol);
- 11.2.14. Permitir habilitar e desabilitar acesso administrativo via SSH por qualquer interface do equipamento;
- 11.2.15. Manter internamente múltiplos arquivos de configurações do sistema;
- 11.2.16. Utilizar SCP ou HTTPS como mecanismo de transferência de arquivos de configuração e sistema operacional;
- 11.2.17. Possuir recurso de autocompletar nos comandos na CLI, com ajuda contextual;
- 11.2.18. Permitir a configuração de múltiplas contas locais de administradores;
- 11.2.19. Implementar controles de acesso por nível, os quais podem ser atribuídos a usuários ou grupos de usuários

para fazer cumprir a separação por perfil de privilégios;

- 11.2.20. Possuir, no mínimo, três níveis de usuários na GUI: administrador, analista e somente-leitura;
- 11.2.21. Suportar autenticação e autorização externa de usuários administradores através de RADIUS, LDAP, Active Directory e TACACS+;
- 11.2.22. A interface gráfica deve permitir a atualização do sistema operacional, atualização de componentes e instalação de patches;
- 11.2.23. Permitir selecionar pela interface gráfica a versão do sistema operacional para inicialização do equipamento;
- 11.2.24. Possuir um comando, via CLI, que mostre o tráfego de utilização das interfaces (bps e pps);
- 11.2.25. Suportar a rollback de configuração e imagem;
- 11.2.26. Possuir o registro local de eventos relevantes do sistema e suportar o envio via syslog de eventos relevantes ao sistema, com capacidade de configuração de múltiplos servidores de syslog;
- 11.2.27. Implementar rate limit da taxa logs enviados para servidores externos, com o objetivo de prevenir a sobrecarga e perda de logs por motivos de alta utilização de CPU, memória ou uso de banda;
- 11.2.28. Permitir reiniciar o equipamento pela interface gráfica e por CLI;
- 11.2.29. Implementar SNMPv1, SNMPv2c e SNMPV3;
- 11.2.30. Implementar traps SNMP;
- 11.2.31. Permitir a criação de MIBs customizadas;
- 11.2.32. Possuir suporte a monitoração utilizando RMON através de pelo menos 4 (quatro) grupos: statistics, history, alarms e events
- 11.2.33. Possuir agente integrado de coleta e exportação de métricas de desempenho e eventos:
 - 11.2.33.1. Coleta de métricas de desempenho compatível com Prometheus;
 - 11.2.33.2. Coleta de métricas de desempenho em formato JSON utilizando cliente HTTP;
 - 11.2.33.3. Exportação de métricas de desempenho compatíveis com, pelo menos, os sistemas AWS CloudWatch e S3, Azure Log Analytics e Application Insights, Elasticsearch, Fluentd, GCP Cloud Monitoring e

Logging, Graphite, Kafka, Splunk e StatsD;

- 11.2.33.4. Exportação de métricas de desempenho em formato JSON para um servidor HTTP;
- 11.2.34. Permitir definir critérios de inclusão e exclusão de coleta e exportação de métricas;
- 11.2.35. Deve incluir métricas de desempenho relacionadas a servidores virtuais, pool e pool members;
- 11.2.36. Deve incluir métricas de throughput, conexões, bits, pacotes, disponibilidade;
- 11.2.37. Deve incluir métricas de requisições, respostas;
- 11.2.38. Deve incluir métricas de criptografia, incluindo cifras, algoritmos, versão, conexões, bytes criptografados, bytes descriptografados;
- 11.2.39. Deve incluir métricas de certificados digitais, incluindo data de expiração, issuer e subject;
- 11.2.40. Deve incluir métricas relacionadas a CPU, memória, discos e interfaces;
- 11.2.41. Deve incluir métricas de desempenho dos scripts de manipulação de tráfego, incluindo total de execuções, média de ciclos, máximo e mínimo de ciclos e falhas;
- 11.2.42. Deve incluir informações de inventário (hostname, id, versão, localização, plataforma, chassi, módulos provisionados);
- 11.2.43. Deve incluir métricas do cluster, incluindo data de sincronização;
- 11.2.44. Deve incluir informações de data da última configuração aplicada;
- 11.2.45. Deve possuir documentação pública do fabricante contendo informações de configurações, exemplos de configuração e modelos de mensagens;
- 11.2.46. Implementar debugging utilizando CLI via console e SSH;
- 11.2.47. Possuir ferramenta interna nativa de captura de tráfego de rede com informações contextuais da solução inseridas em cada pacote/frame;
- 11.2.48. Permitir a exportação de informações de diagnóstico, logs, configurações, desempenho para análises externas sem interferência na solução em produção. A análise deve ser feita em ferramenta, disponível sem custo adicional, online via web ou via aplicação para Windows, Linux ou

MacOS;

- 11.2.49. Deve possuir suporte a Link Layer Discovery Protocol (LLDP), com, pelo menos, as informações: Port ID, TTL, Port Description, System Name, System Description, Management Address, Port VLAN ID, Port and Protocol VLAN ID, VLAN Name, Protocol Identity, Link Aggregation, Maximum Frame Size
- 11.2.50. Suportar exportação de informações de fluxos através sFlow, NetFlow, IPFIX ou outro protocolo similar;
- 11.2.51. Permitir a criação de códigos ou scripts capazes de manipular o tráfego, incluindo descartar, redirecionar, alterar, substituir e comparar valores e atributos, a partir de informações extraídas da conexão, sessão e protocolos;
- 11.2.52. Permitir utilizar listas de dados como fonte de dados por um script para validar se as conexões a serem estabelecidas obedecem a um dos critérios contidos nessa base de dados;
- 11.2.53. Implementar roteamento IPv4 e IPv6 estático e dinâmico;
- 11.2.54. Suportar a criação de múltiplos domínios de roteamento, com tabelas de rotas isoladas, em IPv4 e IPv6, BGP, OSPF e RIP em IPv4 e IPv6;
- 11.2.55. Permitir que cada domínio de roteamento utilize BGP, OSPF e RIP em IPv4 e IPv6;
- 11.2.56. Suportar integração via BGP para divulgação de prefixos;
- 11.2.57. Deve garantir que o retorno do tráfego seja encaminhado para o mesmo host que enviou o tráfego inicialmente para a solução, independente da configuração de rotas do equipamento. Por exemplo, no caso de múltiplos roteadores com acesso à Internet, a solução deve enviar o tráfego de retorno para o cliente sempre para o mesmo roteador que encaminhou o tráfego do cliente inicialmente para a solução;
- 11.2.58. Suportar Equal Cost Multipath (ECMP);
- 11.2.59. Implementar Bidirectional Forward Detection (BFD);

11.3. ENTREGA DE APLICAÇÕES E BALANCEAMENTO DE CARGA

- 11.3.1. Suportar os protocolos HTTP/1.0, HTTP/1.1, HTTP/2 e HTTP/3, para comunicação com o cliente e comunicação

com o servidor;

- 11.3.2. Implementar a reutilização de conexões entre a solução e os servidores, para diferentes clientes e diferentes requisições;
- 11.3.3. Suportar os métodos de balanceamento round robin, least connections, weighted (por peso), tempo de resposta mais rápida baseado no tráfego real, baseado em parâmetros dinâmicos coletados via SNMP ou WMI;
- 11.3.4. Implementar criptografia de cookies;
- 11.3.5. Implementar persistência com pelo menos os métodos por cookie inserindo um novo cookie na sessão, por cookie utilizando um valor do cookie da aplicação, sem adição de cookie, por endereço IP destino, por endereço IP origem, por sessão SSL, parâmetros da URL acessada, parâmetro no header HTTP, qualquer informação do payload camada 7;
- 11.3.6. Permitir configuração de grupos de servidores secundários que devem ser utilizados para balanceamento somente quando uma quantidade mínima especificada de servidores estiver disponível no grupo primário. Caso o número de servidores disponíveis fique menor do que o especificado, a solução deve automaticamente distribuir o tráfego para o próximo grupo. Caso o número de servidores disponíveis volte ao valor mínimo, a solução deve automaticamente voltar a utilizar o grupo primário de servidores;
- 11.3.7. Permitir a replicação do tráfego destinado a servidores virtuais, permitindo habilitar a cópia do tráfego entre o cliente e a solução e entre a solução e o servidor;
- 11.3.8. Implementar pelo menos monitores de servidores de servidores via ICMP, conexões TCP e UDP pela respectiva porta no servidor e HTTP e HTTPS, incluindo HTTP/2;
- 11.3.9. Suportar balanceamento de carga de servidores SIP para VoIP;
- 11.3.10. Permitir limitar o número de conexões estabelecidas com cada servidor real;
- 11.3.11. Permitir limitar o número de conexões estabelecidas com cada servidor virtual;
- 11.3.12. Implementar Network Address Translation (NAT) do IP do servidor;
- 11.3.13. Implementar Network Address Translation (NAT) do IP do cliente;

- 11.3.14. Implementar proteção contra Denial of Service (DoS) em camada 3, 4 e 7;
- 11.3.15. Implementar proteção contra SYN floods;
- 11.3.16. Suportar servidores virtuais com endereço IPv4 e os servidores reais com endereços IPv6;
- 11.3.17. Suportar multiplexação TCP e reuso de sessão para reaproveitamento e uso eficiente de conexões entre a solução de balanceamento de aplicações e os servidores balanceados;
- 11.3.18. Suportar Stream Control Transmission Protocol (SCTP);
- 11.3.19. Implementar aceleração de TLS com instalação do certificado digital na solução, troca de chaves e criptografia dos dados;
- 11.3.20. Permitir recriptografar a conexão entre a solução e o servidor;
- 11.3.21. Permitir espelhamento de tráfego de conexões TLS;
- 11.3.22. Suportar diversas cifras e protocolos SSL/TLS, incluindo TLS 1, 1.1, 1.2, 1.3, Forward Secrecy/Perfect Forward Secrecy, RSA, ECDSA, DHE, ECDHE, AES-128, AES-256, CBC/GCM, Camellia128, Camellia256, SHA, SHA2 (SHA256/384) e ChaCha20-Poly1305;
- 11.3.23. Em relação ao tráfego TLS, deve suportar:
 - 11.3.23.1. Autenticação do servidor pelo cliente, apresentando um certificado previamente configurado;
 - 11.3.23.2. Autenticação do cliente pela solução, através da solicitação e verificação do certificado fornecido pelo cliente;
 - 11.3.23.3. Autenticação mútua (mTLS), quando ambas as autenticações acima mencionadas ocorrem. Durante a autenticação com mTLS, a solução deve apresentar para o servidor um certificado de cliente com atributos extraídos do certificado original obtido do cliente, preservando a autenticação mútua fim a fim;
 - 11.3.23.4. Encaminhar ao servidor real via cabeçalho HTTP todo o certificado utilizado pelo cliente para se autenticar;
 - 11.3.23.5. Encaminhar ao servidor real via cabeçalho HTTP atributos específicos do certificado utilizado pelo cliente;
- 11.3.24. Suportar os algoritmos para sessões TLS:

- 11.3.24.1. SSL session cache Timeout;
- 11.3.24.2. Session Ticket;
- 11.3.24.3. OCSP (Online Certificate Status Protocol) Stapling;
- 11.3.24.4. Dynamic Record Sizing;
- 11.3.24.5. ALPN (Application Layer Protocol Negotiation);
- 11.3.25. Perfect Forward Secrecy;
- 11.3.26. Suportar múltiplos certificados digitais no mesmo servidor virtual, com identificação via SNI (Server Name Indication);
- 11.3.27. Suportar importação de certificados digitais e chaves privadas;
- 11.3.28. Possuir alertas visuais na interface web de certificados com vencimento próximo;
- 11.3.29. Implementar limpeza de cabeçalho HTTP;
- 11.3.30. Implementar compressão de conteúdo HTTP, suportar os algoritmos gzip e deflate e permitir definir compressão especificamente para certos tipos de objetos;
- 11.3.31. Permitir a criação de políticas para classificação de tráfego através de parâmetros da aplicação, incluindo informações de geolocalização IP, cabeçalhos de autenticação HTTP, cookies e operações de cookie, cabeçalhos HTTP, host, método, Referer, Status Code e URI;
- 11.3.32. Permitir as ações para o tráfego classificado: bloqueio, reescrita e manipulação de URL, adicionar cabeçalho HTTP, redirecionar o tráfego para um servidor específico, escolher uma política de proteção web, logging do tráfego;
- 11.3.33. Suportar log de todas as sessões e permitir a customização do formato, incluindo endereço IP de origem, Porta TCP e UDP de origem, endereço IP de destino, porta TCP e UDP de destino, protocolo de camada 4 (TCP ou UDP), data e hora da mensagem, URL acessada;
- 11.3.34. Permitir utilizar diferentes configurações de envio de eventos de uma mesma aplicação, de forma que eventos válidos sejam enviados para um servidor e eventos de violações de segurança sejam enviados para outro servidor;
- 11.3.35. Permitir exportar eventos de acesso para servidores externos com configuração das informações exportadas;

- 11.3.36. Permitir a configuração de autenticação e autorização de clientes HTTP, através de base LDAP, RADIUS e certificados digitais;
- 11.3.37. Implementar integração com ambientes de orquestração de containers para criação dinâmica de serviços de entrega de aplicações e balanceamento de carga na solução, modificando a configuração de forma dinâmica e automática a partir de configurações feitas na plataforma de orquestração;
- 11.3.38. Suportar, pelo menos, as plataformas Kubernetes “Vanilla”, Red Hat OpenShift e VMware Tanzu;
- 11.3.39. Permitir a configuração através de ConfigMaps;
- 11.3.40. Permitir a configuração através de CustomResourceDefinition (CRD) da solução;
- 11.3.41. Permitir a configuração através de objetos de serviço (Service) do tipo LoadBalancer na plataforma;
- 11.3.42. Permitir a configuração através de objetos Ingress na plataforma;
- 11.3.43. Permitir a configuração através de objetos Route no OpenShift;
- 11.3.44. Permitir incluir serviços de entrega de aplicações da solução, tais como SSL Offload e proteção de aplicações;
- 11.3.45. O ADC deverá receber em tempo real as alterações do ambiente e atualizar automaticamente o pool de pods ou nodes disponíveis para o serviço publicado de acordo com a integração realizada;
- 11.3.46. Suportar o protocolo FTP com, pelo menos, as seguintes características:
 - 11.3.46.1. Determinar os comandos FTP permitidos;
 - 11.3.46.2. Requests FTP anônimos;
 - 11.3.46.3. Validar conformidade com o protocolo FTP;
 - 11.3.46.4. Proteger contra ataques de força bruta nos logins;
- 11.3.47. Suportar o protocolo SMTP com, pelo menos, as seguintes características:
 - 11.3.47.1. Limitar o número de mensagens;
 - 11.3.47.2. Validar registro SPF do DNS;
 - 11.3.47.3. Determinar quais métodos SMTP podem ser utilizados;

11.4. PROTEÇÃO DE APLICAÇÕES NO NÍVEL DE REDE E PROTOCOLO

- 11.4.1. Permitir implementação no modo que todo o tráfego seja bloqueado com exceções explícitas em regras de permissões e no modo que todo tráfego é permitido com exceções explícitas em regras de bloqueio;
- 11.4.2. Proteger de ataques DDoS nas camadas de rede e de sessão;
- 11.4.3. Proteger de ataques DDoS que utilizem SSL;
- 11.4.4. A solução deve permitir a criação de regras com, no mínimo, os parâmetros:
 - 11.4.4.1. Endereço IP de destino;
 - 11.4.4.2. Endereço IP de origem;
 - 11.4.4.3. Porta de destino;
 - 11.4.4.4. Porta de origem;
 - 11.4.4.5. VLAN;
 - 11.4.4.6. Protocolo;
 - 11.4.4.7. Ação;
 - 11.4.4.8. Horário;
 - 11.4.4.9. Log;
 - 11.4.4.10. Permitir definir agendamento para ativação da regra;
 - 11.4.4.11. Permitir criar regras com base em zonas de segurança e por interface ou VLAN;
- 11.4.5. Implementar a descoberta automática de serviços presentes em objetos monitorados;
- 11.4.6. Permitir definir, no mínimo, as seguintes ações no tráfego:
 - 11.4.6.1. Permitir: os pacotes são aceitos e passam pela solução;
 - 11.4.6.2. Rejeitar: os pacotes são rejeitados e ocorre envio de pacotes de destino inatingível ou similar a origem do tráfego;
 - 11.4.6.3. Descartar: onde os pacotes são descartados sem o envio de qualquer notificação a origem do tráfego;
- 11.4.7. Deve ser possível criar regras que sejam aplicadas em diferentes hierarquias, incluindo, no mínimo:
- 11.4.8. Global, regras válidas para todo o tráfego, independente da interface de ingresso;

- 11.4.9. Domínio de roteamento, regras válidas para todo o tráfego daquele domínio, independente da interface de ingresso;
- 11.4.10. Objeto, regras válidas para objetos específicos;
- 11.4.11. Deve possuir criptografia IPSEC para comunicação entre sites;
- 11.4.12. Permitir a configuração de alertas que informem automaticamente sobre ataques e anomalia de tráfego, através de limiares baseados no perfil de rede ou através de limites de tráfego atingido;
- 11.4.13. Permitir a restauração das configurações de proteções originais;
- 11.4.14. Deve permitir criar lista de exceção de regras por endereço IP específico ou faixa de sub-rede;
- 11.4.15. Permitir a criação de códigos ou scripts para customizar e aumentar o nível de segurança contra DDoS;
- 11.4.16. Permitir o consumo de listas externas de IPs para bloqueio com base em destino e origem, com atualização automática e ajuste manual da frequência de atualização;
- 11.4.17. Permitir o acionamento via API do descarte de conexões (shun) para integração com terceiros, tais como SIEM, IPS, IDS e outros;
- 11.4.18. Permitir a criação de regras de filtragem através de API REST declarativa;
- 11.4.19. A documentação da API deve ser pública;
- 11.4.20. Exibir uma lista de proteções ativas juntamente com estatísticas resumidas sobre as quantidades de tráfego descartado e aceito
- 11.4.21. Incluir informações estatísticas sobre o tráfego total e o total bloqueado por cada tipo de prevenção;
- 11.4.22. Implementar proteção contra pacotes inválidos, incluindo verificação para DNS malformed, Bad ICMP Frame, Bad ICMP Checksum, ICMP Frame too Large, BadIGMP 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, DNS Water-torture e fornecer estatísticas para os pacotes descartados;

- 11.4.23. Implementar descarte de sessões TCP ociosas se o cliente não enviar uma quantidade de dados dentro de um período configurável;
- 11.4.24. Limitar o número de consultas DNS por segundo através da configuração de limiares;
- 11.4.25. Mitigar, no mínimo, os tipos de ataques ICMP/UDP/TCP Flood, TCP Flag Abuse, GET/POST Flood, SYN Flood, UDP Bandwidth Attack, Smurfing, NTP Reflection Attack, TCP/UDP Bandwidth Attack, Fragging Attack, Slowloris, Connection Attack e Fragmentation Attacks;
- 11.4.26. Possuir recurso de bloqueio automático e temporário de atacantes, devendo ser possível especificar o tempo mínimo para iniciar o bloqueio e o tempo de bloqueio;
- 11.4.27. Suportar envio de SNMP traps para cada ataque DoS detectado;
- 11.4.28. Possuir uma ferramenta de teste de pacotes, através da qual deve ser possível realizar testes de pacotes;
- 11.4.29. Deve possuir a funcionalidade de limiares automático para vetores de DoS;
- 11.4.30. Essa funcionalidade deve valer tanto para proteção geral como também para proteção de serviços específicos.
- 11.4.31. Os limiares automáticos serão construídos pelo próprio sistema e aplicados aos diversos vetores de ataques selecionados;
- 11.4.32. Permitir configurar o sistema para detectar e mitigar assinaturas dinâmicas, capaz de detectar possíveis ameaças de DoS baseado no histórico e comportamento do tráfego e mitigar automaticamente essas ameaças;
- 11.4.33. Suportar integração com serviço de tratamento de DDoS externo através do compartilhamento de informação de vetores e sinalização de ataques em andamento para redirecionamento de tráfego via BGP e limpeza do tráfego em centros de limpezas externos;

11.5. **PROTEÇÃO PARA APLICAÇÕES WEB E API**

- 11.5.1. Possuir tecnologia para mitigação de DDoS em camada 7 a partir de análises comportamentais;
- 11.5.2. Implementar ajustes automáticos e adaptativos de limiares de DoS;
- 11.5.3. Permitir a captura automática do tráfego relativo a ataques DoS em camada 7, web scraping e força bruta;

- 11.5.4. Implementar proteção para aplicações web contra ameaças listadas no OWASP Top 10 2021;
- 11.5.5. Implementar modelo positivo de segurança de aplicações web;
- 11.5.6. Implementar modelo negativa de segurança, ou seja, adotar assinatura de ataques, ameaças e exploração de vulnerabilidade, de aplicações web;
- 11.5.7. Possuir conjuntos de configurações de segurança pré-definidas para configuração rápida de políticas;
- 11.5.8. Permitir a criação de políticas diferenciadas por aplicação e por URL, onde cada aplicação e URL poderão ter políticas totalmente diferentes;
- 11.5.9. Permitir configurar de forma granular, por aplicação protegida, restrições de métodos HTTP permitidos, tipos ou versões de protocolos, tipos de caracteres e versões utilizadas de cookies;
- 11.5.10. Permitir desativar a inspeção para URL específicas;
- 11.5.11. Implementar identificação do usuário da aplicação web, mantendo a identificação até que o usuário tenha deixado o aplicativo;
- 11.5.12. Permitir a integração com firewall de banco de dados;
- 11.5.13. Suportar aplicações que utilizam protocolo WebSocket;
- 11.5.14. Suportar os protocolos HTTP/1.0, HTTP/1.1 e HTTP/2.0, para comunicação com o cliente e comunicação com o servidor, sem a necessidade de downgrade de versão;
- 11.5.15. Implementar proteção contra:
 - 11.5.15.1. Acesso por força bruta;
 - 11.5.15.2. DoS e DDoS em camada 7;
 - 11.5.15.3. Buffer Overflow;
 - 11.5.15.4. Cross Site Request Forgery (CSRF);
 - 11.5.15.5. Cross-Site Scripting (XSS);
 - 11.5.15.6. Server-Side Request Forgery (SSRF);
 - 11.5.15.7. SQL Injection;
 - 11.5.15.8. Parameter tampering;
 - 11.5.15.9. Cookie poisoning;
 - 11.5.15.10. HTTP Request Smuggling;
 - 11.5.15.11. Manipulação de campos escondidos (hidden input);

- 11.5.15.12. Manipulação de cookies;
- 11.5.15.13. Roubo de sessão através de manipulação de cookies;
- 11.5.15.14. Sequestro de sessão;
- 11.5.15.15. Validação de consistência de formulários;
- 11.5.15.16. Validação do cabeçalho do "user-agent" para identificar clientes inválidos;
- 11.5.16. Permitir especificar quais URLs devem ser utilizadas para proteção contra CSRF (Cross-Site Request Forgery);
- 11.5.17. Suportar codificação HTML "application/x-www-form-urlencoded";
- 11.5.18. Suportar HTTP Batched Request com proteções e assinaturas considerando individualmente URIs, cabeçalhos e conteúdo;
- 11.5.19. Suportar codificação fragmentada (chunked encoding);
- 11.5.20. Suportar validações de protocolo:
 - 11.5.20.1. Restrição de métodos;
 - 11.5.20.2. Restrição de protocolos e versões;
 - 11.5.20.3. Validação de conformidade com RFCs;
 - 11.5.20.4. Validação de caracteres URL-encoded;
 - 11.5.20.5. Validação de codificação fora de padrão %uXXYY.
- 11.5.21. Suportar validações de HTML com nome de parâmetros, tamanho e tipo dos valores de parâmetros e combinação de nome, tipo e tamanho de parâmetros;
- 11.5.22. Possuir técnicas de detecção de evasões:
 - 11.5.22.1. URL-decoding;
 - 11.5.22.2. Terminação Null Byte String;
 - 11.5.22.3. Paths autorreferenciados;
 - 11.5.22.4. Case de caracteres misturados;
 - 11.5.22.5. Uso excessivo de espaços em branco;
 - 11.5.22.6. Decodificação de entidades HTML;
 - 11.5.22.7. Caracteres de escape;
- 11.5.23. Permitir a inspeção externa de arquivos enviados por usuários (upload) para os servidores de aplicação utilizando Internet Content Adaptation Protocol (ICAP);
- 11.5.24. Capacidade de filtrar cabeçalhos, corpo e status de

respostas;

- 11.5.25. Permitir o uso do parâmetro HTTP X-Forwarded-For como parte da política de controle;
- 11.5.26. Implementar validação de URL;
- 11.5.27. Validação de métodos HTTP utilizados (GET, POST, HEAD, OPTIONS, PUT, TRACE, DELETE, CONNECT) por URL;
- 11.5.28. Implementar proteção de aplicações web que utilizam chamadas de API, protegendo tanto a aplicação como a API, com a visibilidade que se trata da mesma sessão de usuário;
- 11.5.29. Suportar aplicações Single-Page Application (SPA);
- 11.5.30. Permitir a customização da resposta de bloqueio;
- 11.5.31. Permitir a configuração de lista de exceções temporárias ou permanentes de endereços IP bloqueados;
- 11.5.32. Permitir adicionar, automaticamente e manualmente, em uma lista de bloqueio, os endereços IP de origem que ultrapassarem limites estabelecido, por um período configurável;
- 11.5.33. Implementar as proteções:
- 11.5.34. Proteção contra exposição de informações do ambiente e servidores internos como, sistema operacional e servidor web;
- 11.5.35. Ocultar qualquer mensagem de erro HTTP dos usuários;
- 11.5.36. Remover as mensagens de erro às páginas que serão enviadas aos usuários;
- 11.5.37. Suportar políticas por geolocalização para restrição de acesso a determinados países;
- 11.5.38. Implementar aprendizado automático para identificação da estrutura da aplicação, incluindo URLs, parâmetros URLs, campos de formulários, tipo de dado, tamanho de caracteres, cookies;
- 11.5.39. O aprendizado deve ser capaz de diferenciar atributos com o mesmo nome, mas presentes em URLs diferentes;
- 11.5.40. Implementar aprendizado automático de XML;
- 11.5.41. Permitir a importação de arquivo de esquema XML;
- 11.5.42. Implementar aprendizado automático de JSON;
- 11.5.43. Permitir a importação de arquivo de esquema JSON;

- 11.5.44. Permitir a criação automática de políticas, onde a política de segurança é criada e atualizada automaticamente baseando-se no tráfego real;
- 11.5.45. O perfil aprendido de forma automatizada pode ser ajustado, editado ou bloqueado;
- 11.5.46. Implementar detecção e mitigação de ameaças e ataques com base em assinaturas de ataques, com atualização periódica e automática da base de assinaturas;
- 11.5.47. As assinaturas devem ser atualizadas durante o período do contrato, sem custo adicional;
- 11.5.48. Não serão aceitas soluções que definem assinaturas como sendo uma base de reputação de IP;
- 11.5.49. A atualização deve ser relacionada apenas as assinaturas, não sendo aceitas soluções que demanda a atualização do sistema operacional para atualização de cada nova versão da base de assinaturas;
- 11.5.50. Permitir a configuração automática de assinaturas com base em uma lista interna de tecnologias utilizadas pela aplicação;
- 11.5.51. Permitir desabilitar assinaturas específicas para determinados parâmetros, se comportando como exceção da configuração geral da política;
- 11.5.52. Permitir configurar um período de adaptação de novas assinaturas, quando nenhuma requisição que viole a assinatura deve ser bloqueada, apenas informada em relatório. Este processo deve ser automático, não sendo necessário a criação de regras específicas a cada atualização de assinatura;
- 11.5.53. Possuir assinaturas de ataques para conteúdo em JSON e XML;
- 11.5.54. Possuir proteções contra XML Bomb;
- 11.5.55. Possuir proteção para WebServices, suportar WS-I Basic Profile, importação de WSDL e aplicação de controles, criptografar e descriptografar partes das mensagens SOAP, assinar digitalmente e verificar de partes das mensagens SOAP;
- 11.5.56. Possuir integração com soluções externas de análise vulnerabilidade para importação de relatórios e configuração de políticas de segurança, indicando quais vulnerabilidades podem ser resolvidas e quais devem ser resolvidas manualmente externamente;

- 11.5.57. Implementar detecção de DoS na camada 7, através de análise comportamental, com aprendizado automático do comportamento da aplicação e combinação com nível de carga do servidor;
- 11.5.58. Permitir apenas registrar o ataque, sem tomar nenhuma ação de bloqueio;
- 11.5.59. Implementar detecção com base no número de requisições por segundo enviados a uma URL específica;
- 11.5.60. Implementar detecção com base no número de requisições por segundo enviados de um IP específico;
- 11.5.61. Implementar detecção com base na validação do cliente através de código executado no navegador para identificação de bots;
- 11.5.62. Implementar detecção com base no aumento de um determinado percentual do número de transações por segundo (TPS);
- 11.5.63. Implementar detecção com base no aumento de carga e latência do servidor de aplicação;
- 11.5.64. Implementar detecção com base no número máximo de transações por segundo de um determinado IP;
- 11.5.65. Implementar mitigações para ataques DoS, incluindo resolução de CAPTCHA, descarte de todas as requisições de um determinado IP, descarte por geolocalização IP, injeção de um desafio JavaScript para detectar se é um usuário legítimo ou bots;
- 11.5.66. Implementar mitigação de ataques DDoS através de assinaturas dinâmicas em tempo real para proteção da aplicação;
- 11.5.67. Implementar detecção e mitigação de ataques de força bruta de usuário/senha em páginas de login, com configuração da quantidade máxima de tentativas e tempo de mitigação;
- 11.5.68. Identificar ataques com diferentes usuários e mesma origem;
- 11.5.69. Identificar ataques com diferentes origens e mesmo usuário;
- 11.5.70. Identificar ataques de forma global, considerando a quantidade de tentativas e implementando contramedidas de forma global para a política;
- 11.5.71. Possuir funcionalidade para integração com listas externas de credenciais expostas para mitigar ataques

Credential Stuffing e Password Sprawl;

- 11.5.72. Implementar mitigação através de listas de bloqueio dinâmica de endereços IPs após validação sem sucesso de desafios e permitir a configuração do tempo de bloqueio;
- 11.5.73. Implementar mitigação através de listas de bloqueio dinâmica de endereços IPs que ultrapassem um número máximo de violações por minuto e permitir a configuração do tempo de bloqueio;
- 11.5.74. Implementar detecção e mitigação para proteção contra bots através da combinação de desafios enviados ao navegador do usuário e técnicas avançadas de análise;
- 11.5.75. Não serão aceitas soluções que utilizam apenas o user-agent para detecção de bots;
- 11.5.76. Implementar proteção proativa de ataques automatizados por bots e outras ferramentas, como web scrapers.
- 11.5.77. Possuir atualização automática de definição de bots;
- 11.5.78. Permitir a configuração de bloqueio e permissão de bots benignos conhecidos, como Google, Yahoo! e Microsoft Bing;
- 11.5.79. Permitir a criação de definições de bots;
- 11.5.80. Implementar proteção de APIs através da imposição de regras de endpoint e métodos permitidos;
- 11.5.81. Permitir a configuração de quotas e rate limits para chamadas em APIs de forma global na política;
- 11.5.82. Permitir a configuração de quotas e rate limits para chamadas em APIs por endpoint;
- 11.5.83. Permitir configurar exceções as regras de rate limits para chamadas na API;
- 11.5.84. Implementar proteção de conteúdo no formato JSON (JavaScript Object Notation);
- 11.5.85. Suportar proteção de conteúdo de mensagens no formato GraphQL, incluindo assinaturas de ataques, profundidade de query, GraphQL batching, inspeção de conteúdo JSON em mensagens POST e GET;
- 11.5.86. Suportar importação de especificação de API compatível com OpenAPI v2 e v3, nos formatos YAML ou JSON, com suporte a parâmetros no path e importação de respostas;
- 11.5.87. Implementar funcionalidade de autenticação e

autorização de clientes de API utilizando, pelo menos, os métodos HTTP Basic e OAuth 2.0;

- 11.5.88. Implementar funcionalidade para prevenir vazamento de informações, dados sensíveis e outros tipos de dados confidenciais, sigilosos ou restrito, através do bloqueio ou remoção dos dados confidenciais;
- 11.5.89. Implementar funcionalidades para prevenir vazamento de dados sensíveis em mensagens de erro HTTP, códigos das aplicações, entre outros, retirando os dados ou mascarando a informação nas páginas enviadas aos usuários;
- 11.5.90. Implementar funcionalidade para ocultar erros de aplicação ou infraestrutura do usuário;
- 11.5.91. Permitir a configuração de fluxo de navegação da aplicação, de forma que um usuário só pode alcançar determinada URL se passar por outras anteriormente;
- 11.5.92. Permitir a correção de um falso positivo através da aceitação da requisição e atualização da política de forma automática;
- 11.5.93. Possuir um nível severidade de violação de múltiplos níveis para fácil identificação de violações de maior e menor prioridade;
- 11.5.94. Implementar um identificador único para cada requisição tratada pela solução;
- 11.5.95. Permitir o armazenamento local de eventos e exportação para servidores externos;
- 11.5.96. Permitir configurar a retenção dos eventos por tempo e volume;
- 11.5.97. Implementar a detecção, remoção ou codificação de dados sensíveis dos eventos como, por exemplo, números de cartão de crédito, CPF e senhas;
- 11.5.98. Implementar a criptografia de parâmetros específicos da aplicação, tais como credenciais e dados sensíveis, sem a necessidade de atualizar a aplicação. Esta criptografia de dados deve ser implementada no payload do HTTP, ou seja, nos dados propriamente ditos e não apenas via protocolo de transporte/túnel (TCP/TLS);
- 11.5.99. Implementar a ofuscação do nome de um parâmetro sensível da aplicação utilizando caracteres aleatórios, devendo ser mudado frequentemente pela solução para dificultar ataques direcionados;

- 11.5.100. Possuir API REST para configuração de servidores virtuais, políticas de segurança, parâmetros, perfis e demais configurações;
- 11.5.101. Permitir exportar as políticas de segurança para arquivos texto, JSON ou XML;
- 11.5.102. Possuir integração com esteiras de automação que permita que as configurações sejam realizadas de forma automática e dinâmica, de forma declarativa, por ferramentas de automação e orquestração, permitindo que a solução seja integrada ao ciclo de desenvolvimento;
- 11.5.103. Suportar integração com funcionalidade de gestão avançada de tráfego automatizado para detecção e mitigação de ataques, abusos e fraudes, com detecção de tráfego gerado por usuários, bots benignos e malignos, através de telemetria de uso coletada da aplicação, sem a utilização de CAPTCHAs ou desafios para o navegador;
- 11.5.104. Implementar funcionalidade de forma nativa na solução ou possuir integração com serviço em nuvem do mesmo;
- 11.5.105. Implementar proteção de aplicações web, de dispositivos móveis e APIs;

11.6. IMPLEMENTAR BASES DE INTELIGÊNCIA DE AMEAÇAS ATUALIZADAS

- 11.6.1. A solução deve implementar a atualização das bases de inteligência de ameaças para proteção de DoS/DDoS, serviços de DNS, de visibilidade de tráfego e de proteção de aplicações web e API durante a vigência do contrato;
- 11.6.2. As fontes de inteligência devem ser fornecidas diretamente pelo fabricante da solução ou parceiro homologado através de assinaturas de serviços próprios;
- 11.6.3. As fontes de inteligência devem ser atualizadas frequentemente pela duração do contrato sem custo adicional;
- 11.6.4. Deve dispor de bases de inteligência de IP, incluindo IPv4 e IPv6, classificados e categorizados em, pelo menos, as categorias fontes de ataques web, redes e hosts de botnets, scanners de websites, fontes de phishing, servidores proxies, redes e hosts que exploram vulnerabilidades em Windows, redes e hosts de negação de serviço e redes e hosts com baixa reputação;

- 11.6.5. Permitir que sejam criados filtros utilizando as categorias de IP nas funções de proteção de DDoS e serviços de DNS, de visibilidade de tráfego e de proteção de aplicações web e API;
- 11.6.6. Permitir utilizar a base de inteligência de IP durante consultas de DNS, permitir ações diferentes configuradas de acordo com a categoria e alterar a resposta antes de ser enviada para o cliente na solução de proteção de DDoS e serviços de DNS;
- 11.6.7. Permitir utilizar a base de inteligência de IP para classificar e selecionar uma cadeia de serviço na solução de visibilidade de tráfego;
- 11.6.8. Permitir que sejam criados filtros onde se verifica o endereço de origem no cabeçalho X-Forwarded-For (XFF) com base na classificação de endereços IP na solução de proteção de aplicações web e API;
- 11.6.9. Dispor de base de inteligência de ameaças relacionados a campanhas e ataques a aplicações web, correlacionando diversas fontes de inteligência e ameaças encontradas diariamente no mundo real;
- 11.6.10. As regras de proteção e assinaturas derivadas desta base de inteligência devem ser habilitadas automaticamente, sem precisar de um ciclo de aprendizagem na solução;
- 11.6.11. A base de inteligência deve implementar detecção e mitigação de ataques com baixo índice de falso-positivo;
- 11.6.12. Este serviço é complementar a atualização de assinaturas de ataques da solução de proteção de aplicações web e API, portanto, as informações disponibilizadas pela base de inteligência não devem ser limitada a apenas indicar qual assinatura do WAF for acionada, devendo disponibilizar informações contextuais incluindo, por exemplo, a capacidade de informar que um agente conhecido de ameaça usou uma exploração específica de vulnerabilidade mais recente (por exemplo, um CVE) em uma tentativa de implantação de uma ameaça como, por exemplo, um software de mineração de criptomoedas;
- 11.6.13. Devem ser automáticas e frequentes as atualizações de regras, políticas, configurações e demais ajustes que dependem do serviço de inteligência, sem interrupção do serviço, sem necessidade de atualização do sistema operacional e nem reiniciar o equipamento a cada atualização;

11.7. IMPLEMENTAR MÓDULO DE IDENTIFICAÇÃO E ACESSO

11.7.1. Deverá implementar as funcionalidades de Single Sign-on e VPN-SSL, com no mínimo os seguintes recursos:

11.7.1.1. Deve possuir o modo “Portal” onde a solução se comporta como proxy reverso, buscando o conteúdo Web dos portais internos e apresentando-os como links seguros no portal do usuário;

11.7.1.2. Deve possuir o modo “Network”, onde um usuário se conecta efetivamente à rede interna, obtendo um endereço IP roteável pela rede interna.

11.7.1.3. Deverá possuir ativo o controle de, no mínimo, 500 usuários concorrentes, e deverá vir com todo o licenciamento necessário para ativação desses 500 usuários;

11.7.1.4. Deverá possuir cliente VPN SSL para pelo menos os sistemas operacionais Windows, Linux e MacOS;

11.7.1.5. Deverá possuir validação da estação de trabalho do usuário, para pelo menos: Sistema Operacional, Antivírus e Firewall.

11.7.2. Deverá ser capaz de autenticar usuários em, pelo menos, bases de dados:

11.7.2.1. LDAP;

11.7.2.2. Radius;

11.7.2.3. TACACS+;

11.7.2.4. Active Directory;

11.7.3. Deve possuir capacidade para realizar múltiplos métodos de autenticação remotos, incluindo pelo menos:

11.7.3.1. Radius;

11.7.3.2. LDAP;

11.7.3.3. Active Directory;

11.7.3.4. TACACS+;

11.7.3.5. Kerberos;

11.7.4. Deve possuir capacidade para permitir a troca da senha dos usuários que tenham expirado;

11.7.5. Deve possuir capacidade para definir lease pool que contenha endereços IP a serem designados aos usuários com acesso a rede;

- 11.7.6. Deve possuir capacidade de redirecionar tráfego HTTP para HTTPs para um determinado servidor virtual;
- 11.7.7. Deve possuir capacidade para definir ACLs estáticas e dinâmicas;
- 11.7.8. Deve possuir capacidade para realizar Single Sign On (SSO) utilizando:
 - 11.7.8.1. NTLM;
 - 11.7.8.2. Basic;
 - 11.7.8.3. HTTP Forms;
 - 11.7.8.4. Kerberos;
 - 11.7.8.5. OAM;
- 11.7.9. Deve possuir capacidade de utilizar JSON Web Token (JWT) para autorizar e autenticar acesso as aplicações e APIs;
- 11.7.10. Deve possuir a capacidade de utilizar JWE, onde o JWT será criptografado e decritografado utilizando, pelo menos, chaves RSA;
- 11.7.11. Deve possuir capacidade para, graficamente, criar e manter as políticas de acesso como diagrama de fluxo;
- 11.7.12. Suportar visibilidade e inspeção de tráfego criptografado SSL/TLS, com capacidade de descriptografia e recriptografia centralizada;

11.8. ORQUESTRAÇÃO DE TRÁFEGO CRIPTOGRAFADO SSL/TLS

- 11.8.1. Suportar inspeção de tráfego criptografado SSL/TLS de entrada (inbound) e saída (outbound);
- 11.8.2. Suportar atuação como SSL Forward Proxy e SSL Reverse Proxy;
- 11.8.3. Suportar os protocolos TLS 1.0, TLS 1.1, TLS 1.2 e TLS 1.3;
- 11.8.4. Suportar algoritmos criptográficos amplamente utilizados, incluindo RSA, ECDSA, DHE, ECDHE, AES, GCM, CBC e ChaCha20-Poly1305;
- 11.8.5. Suportar Forward Secrecy e Perfect Forward Secrecy;
- 11.8.6. Suportar controle e aplicação de políticas de criptografia SSL/TLS, incluindo versões de protocolo e cipher suites;
- 11.8.7. Suportar descriptografia e recriptografia de tráfego

SSL/TLS para inspeção por dispositivos de segurança integrados;

- 11.8.8. Suportar orquestração de tráfego criptografado entre múltiplas soluções de segurança por meio de security service chaining;
- 11.8.9. Suportar operação independente de porta TCP para descriptografia SSL/TLS;
- 11.8.10. Suportar bypass seletivo de tráfego SSL/TLS com base em políticas definidas pelo administrador;
- 11.8.11. Suportar exceções de descriptografia para tráfego sensível, conforme políticas de segurança e conformidade;
- 11.8.12. Suportar inspeção baseada em informações do handshake SSL/TLS, incluindo Server Name Indication (SNI);
- 11.8.13. Suportar geração dinâmica de certificados para interceptação SSL/TLS;
- 11.8.14. Suportar uso de Autoridade Certificadora (CA) interna para assinaturas de certificados de inspeção;
- 11.8.15. Suportar importação e gerenciamento de certificados digitais X.509;
- 11.8.16. Suportar validação de certificados apresentados durante o handshake SSL/TLS;
- 11.8.17. Suportar integração com infraestrutura de chaves públicas (PKI);
- 11.8.18. Suportar integração com módulos de segurança de hardware (HSM) para proteção de chaves criptográficas;
- 11.8.19. Suportar HSMs compatíveis com padrões de mercado;
- 11.8.20. Suportar armazenamento seguro de chaves privadas e certificados;
- 11.8.21. Suportar aplicação centralizada de políticas SSL/TLS;
- 11.8.22. Suportar alta disponibilidade e sincronização de configurações SSL/TLS entre dispositivos;
- 11.8.23. Suportar registro (logging) de eventos SSL/TLS para auditoria e troubleshooting;
- 11.8.24. Suportar integração com sistemas externos de monitoramento e análise de eventos de segurança.

12. DOS REQUISITOS DA CONTRAÇÃO

12.1. REQUISITOS DA SOLUÇÃO DE TIC

- 12.1.1. Independente da Proposta Comercial, o Part Number é único para todos os produtos, de forma que identifica exatamente as características necessárias para cada item.
- 12.1.2. Part Number (PN, P/N, #NUMBER) é um código padronizado de identificação de componentes, que permite a múltiplos fabricantes venderem o mesmo item sem gerar problemas de compatibilidade. Trata-se de uma sequência de números e algarismos impressos de forma idêntica em todas as unidades.
- 12.1.3. Os itens necessários, com os números de catálogo (Part Number) do fabricante, com a respectiva descrição são listados na Tabela 1, no item 2.

13. SUPORTE TÉCNICO 24x7x365, INSTALAÇÃO E MANUTENÇÃO.

13.1. DO SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO DA SOLUÇÃO

- 13.1.1. O serviço especializado de instalação, configuração e migração entre as soluções deverá ser prestado por profissional certificados pelo fabricante da solução a ser disponibilizado à época da assinatura do contrato;
- 13.1.2. Compreende a instalação e customização dos equipamentos, montagem física dos equipamentos, e todos os componentes, bem como a configuração lógica de todos os equipamentos e softwares envolvidos na solução ofertada, de acordo com a topologia definida pela CONTRATANTE;
- 13.1.3. A CONTRATADA deverá apresentar sua equipe de trabalho, composta pelo Gerente de Projeto e sua equipe técnica, conforme o serviço a ser executado, na data da 1ª reunião de acompanhamento da execução do Contrato, a ser definida pelo CONTRATANTE, após a assinatura do mesmo;
- 13.1.4. Deverá ser apresentado plano de ação das atividades e cronograma de implantação, em até 60 (sessenta) dias úteis, contados da assinatura do contrato, incluindo as etapas de Kick-off, levantamento, topologia, montagem dos equipamentos, instalação, configuração, migração, testes e operação assistida da solução ofertada;
- 13.1.5. Cabe à CONTRATANTE, manter a topologia atual efetuando a substituição dos equipamentos, conforme

topologia representada pela figura 1, no item 8.2;

- 13.1.6. A equipe da CONTRATADA que irá executar a instalação deverá trabalhar sob a orientação e supervisão do profissional responsável (gerente de projeto) e pela coordenação das atividades de implantação e migração, e com o acompanhamento do profissional técnico indicado pelo CONTRATANTE. Caberá ao gerente de projeto coordenar e orientar todo o processo de planejamento, instalação, configuração, integração, migração e teste da solução, acompanhando o cumprimento dos prazos e atestando a qualidade dos entregáveis;
- 13.1.7. Deverá disponibilizar, no momento da assinatura do contrato, técnico especializado certificado na solução ofertada pelo período necessário para realizar a instalação, configuração, parametrização, otimização para pleno funcionamento da solução;
- 13.1.8. Deverá instalar, configurar e otimizar a solução ofertada com todos os componentes da solução em pleno funcionamento;
- 13.1.9. Deverá haver repasse de conhecimento de toda a solução implementada para a equipe designada como responsável técnica, com apresentações sobre a solução ofertada em local definido pela CONTRATANTE;
- 13.1.10. A janela de instalação, configuração, manutenção, será acordada com a CONTRATANTE, que poderá optar em ser executadas em finais de semana, feriados e fora do expediente, e em horário noturno, para evitar indisponibilidade;
- 13.1.11. Os eventuais custeios com deslocamentos técnicos, despesas de transportes, diárias, seguro ou quaisquer custos envolvidos ficam a cargo da CONTRATADA;
- 13.1.12. A CONTRATADA deve emitir relatórios das atividades da implementação e migração, deverão ser apresentados em via impressa ou em meio digital, serão considerados como efetivamente entregues e aceitos somente após a validação pela equipe técnica da CONTRATANTE;

13.2. DO SUPORTE TÉCNICO ESPECIALIZADO

- 13.2.1. Prestar suporte especializado na solução contratada para garantir a manutenção emergencial, preventiva, corretiva, melhoria contínua e realizar as atualizações das licenças e assinaturas da solução;

- 13.2.2. Disponibilizar técnico especializado na solução ofertada, durante o período de vigência do contrato, para garantir o perfeito funcionamento da solução;
- 13.2.3. Os serviços contratados poderão ser executados após o expediente, em finais de semana ou feriados, a critério da CONTRATANTE e acordado com a CONTRATADA;
- 13.2.4. O suporte técnico da CONTRATANTE deverá ser prestado para cada componente da solução adquirida e será acionada em caso de qualquer indisponibilidade da solução;
- 13.2.5. Os serviços de manutenção preventiva e corretiva deverão ser executados no ambiente da CONTRATANTE;
- 13.2.6. As manutenções serão solicitadas através de chamado ou por notificação automática de detecção de alarme, inoperância, falhas que possam ocasionar a indisponibilidade do serviço;
- 13.2.7. Deverá implantar novas versões, aplicar patches de atualização, documentar e prestar suporte técnico especializado durante a vigência do contrato;
- 13.2.8. Toda atividade executada pela CONTRATADA, caso seja solicitado, deverá ser entregue documentação a CONTRATANTE, em até 7 (sete) dias, após a demanda para aceite;
- 13.2.9. Responder, formalmente, dentro de 03 (três) dias úteis, a todas as correspondências emitidas pela CONTRATANTE, prestando todos os esclarecimentos solicitados;
- 13.2.10. A CONTRATADA será responsável por todas as atividades referentes ao reposicionamento lógico e físico da solução de proteção de perímetro (ex. migração de posicionamento externo para interno, modificação na topologia de rede etc.), sempre que demandada pela CONTRATANTE;
- 13.2.11. A CONTRATADA deverá prestar todo o apoio necessário para garantir o funcionamento das soluções a partir da abertura de chamado, através de Central de Atendimento (número telefônico e site na Internet), fornecendo, no momento da abertura do chamado, o número, data e hora, devendo possibilitar a indicação do nível de prioridade para o mesmo. Este será considerado o início para contagem dos prazos estabelecidos nos itens seguintes;
- 13.2.12. No caso da central de chamados da CONTRATADA encontrar-se fora do município do Rio de Janeiro, esta

deverá oferecer número de telefone de Discagem Direta Gratuita (DDG);

- 13.2.13. A CONTRATADA deverá possuir “web site” na INTERNET, com visão para os profissionais indicados pela CONTRATANTE, com os recursos mínimos de: acompanhamento do status do chamado, medidas tomadas, pendências e emissão de relatórios de chamados técnicos;
- 13.2.14. Todos os chamados com referência aos componentes, deverão seguir as seguintes premissas:
 - 13.2.14.1. Os chamados poderão ser abertos durante todo o período do dia, incluindo sábados, domingos e feriados, no regime de 24 (vinte e quatro) horas do dia, nos 7 (sete) dias da semana;
- 13.2.15. A CONTRATADA se obrigará a resolver problemas técnicos, on-site, caso seja necessário, dentro dos prazos estipulados no Acordo de Nível de Serviço deste TR, com todos os ônus para deslocamento e de hospedagem ser da CONTRATADA, quando ocorrer indisponibilidade da solução adquirida e inviabilidade de solução remota;
- 13.2.16. A CONTRATADA se obrigará a informar as atualizações de softwares, em até 48 horas após disponibilização pelo fabricante, para análise de criticidade, que definirá o modelo de manutenção preventiva a ser seguido, e acordado com a CONTRATANTE;
- 13.2.17. Os serviços de garantia, manutenção e suporte técnico, para a solução, devem ser prestados durante 24 (vinte e quatro) meses, contados a partir do término das atividades de implantação, para atualização de softwares e listas de categorização e suporte a todos os itens de software e hardware da solução, em conformidade com os itens que seguem:
 - 13.2.17.1. O primeiro atendimento deverá ser efetuado pelo fornecedor e não diretamente pelo fabricante.
- 13.2.18. A Contratada deverá manter em seu quadro de funcionários, durante toda a duração do contrato, ao menos dois analistas técnicos com certificação válidas oficial fornecida pela F5 Networks abaixo, sendo no mínimo:
 - 13.2.18.1. F5 Certified BIG-IP Administrator (F5-CA).
- 13.2.19. As certificações listadas no item 13.2.18.1 garantem o expertise necessário para administrar e sanar possíveis incidentes no ambiente complexo dos produtos BIG IP F5

Networks, bem como prestar o suporte de alto nível que é necessário.

- 13.2.20. A Contratada deverá prover serviços de Suporte Técnico da Solução F5 Networks no período de 24 (vinte e quatro) meses contados a partir do término das atividades de implantação.
- 13.2.21. A IPLANRIO, no papel de administradora da solução Contratada, será a responsável pelas solicitações de suporte, garantia e manutenção junto à Contratada.
- 13.2.22. A Contratada deverá fornecer também suporte técnico sempre que solicitado pela IPLANRIO, seja para casos de mal funcionamento de software e hardware, implementação de funcionalidades ou necessidade de apoio técnico quanto ao produto.
- 13.2.23. A Contratada deverá fornecer Suporte Técnico e Atualização de versões para a solução Contratada.
- 13.2.24. A Contratada deverá fornecer Serviços Profissionais de Suporte da Fabricante, incluindo suporte técnico, migrações, consultoria, ajustes e otimizações do ambiente.

13.3. **ACORDO DE NÍVEIS DE SERVIÇOS (ANS) PARA SUPORTE TÉCNICO**

- 13.3.1. Para o fim aqui previsto, define-se como “Caracterização do Chamado” a data e horário a partir da qual a Contratada comprovadamente seja acionada, através de: contato telefônico ou pela INTERNET (página Web).
- 13.3.2. Tabela dos prazos máximos, contados em horas corridas a partir do chamado:

Severidade	Critério de Classificação do Contratante	Tempo de Resposta	Tempo de Solução
Alto Impacto	Serviço indisponível ou seriamente comprometido	Até 2 horas	Até 8 horas
Médio Impacto	Operando com Restrições	Até 4 horas	Até 12 horas
Impacto reduzido	Restrição pontual em funcionalidade	Até 8 horas	Até 24 horas

o			
---	--	--	--

- 13.3.3. Em caso de PARALISAÇÃO TOTAL dos produtos sob suporte (Falha Crítica/alto impacto), a Contratada, deverá comprometer-se, enquanto estiver solucionando o problema, a tomar todas as medidas paliativas que estiverem ao seu alcance e disponíveis na melhor técnica existente, de forma a amenizar o problema indicado pela IPLANRIO, fornecendo, se for o caso, solução alternativa compatível à Contratada, até o restabelecimento total da solução.
- 13.3.4. No caso de descumprimento do ANS a contratada estará sujeita as sanções administrativas conforme disposições do item 22 deste Termo de Referência.
- 13.3.5. O ANS poderá ser revisto durante a execução do contrato e sofrer alterações mediante acordo entre as partes, sempre que o novo sistema se mostrar mais eficiente para garantir a qualidade dos serviços para a Prefeitura e desde que não haja prejuízos para a Contratada.
- 13.3.6. A Contratada deverá designar um técnico qualificado para acompanhar presencialmente a instalação, cabeamento e ativação dos equipamentos.
- 13.3.7. A Contratada deverá realizar, em conjunto com a IPLANRIO, a configuração de software necessária para o completo funcionamento da Solução, considerando a integração com a infraestrutura administrativa da solução, já existente no ambiente da IPLANRIO.
- 13.3.8. A CONTRATANTE deverá informar as pessoas autorizadas a abrir e fechar chamados junto à CONTRATADA, bem como o meio pelo qual a autorização de fechamento será formalizada;
- 13.3.9. A CONTRATANTE poderá efetuar um número ilimitado de chamados de suporte técnico durante a vigência do contrato. A CONTRATADA deverá disponibilizar garantia técnica prestada pelo fabricante dos produtos oferecidos, a fim de garantir os serviços à CONTRATANTE;
- 13.3.10. A CONTRATADA deverá disponibilizar, quando da formalização da contratação, um gerente de serviço, responsável técnico por realizar o acompanhamento periódico dos serviços prestados, com visitas para promover interações com o responsável técnico da CONTRATANTE, atuando preventivamente, com o acompanhamento dos serviços prestados, identificando

necessidades, fornecendo feedbacks para melhoria do serviço prestado;

- 13.3.11. A CONTRATADA deve comunicar, imediatamente, por escrito, quaisquer dificuldades encontradas pelos técnicos alocados para execução dos serviços que, eventualmente, possam prejudicar a boa e pontual execução dos trabalhos, pactuando-se como INEXISTENTE as dificuldades não formalizadas de imediato.

14. DAS OBRIGAÇÕES DA CONTRATADA E DA CONTRATANTE

14.1. SÃO OBRIGAÇÕES DA CONTRATADA:

- 14.1.1. Executar os serviços conforme especificações do Termo de Referência e de sua proposta, como perfeito cumprimento das cláusulas contratuais, além de fornecer os materiais e equipamentos, ferramentas e utensílios inerentes à execução do objeto do Contrato;
- 14.1.2. Reparar, corrigir, remover ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do Contrato, os serviços efetuados em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;
- 14.1.3. Responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com os artigos 14 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990), ficando o Contratante autorizado a descontar da garantia o valor correspondente aos danos sofridos;
- 14.1.4. Utilizar empregados habilitados e com conhecimento dos serviços a serem executados, em conformidade com as normas e determinações em vigor;
- 14.1.5. Relacionar os trabalhadores que executarão os serviços na sede do Contratante, além de provê-los conforme as exigências de segurança do trabalho, se for o caso;
- 14.1.6. Responsabilizar-se por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas na legislação específica, cuja inadimplência não transfere responsabilidade ao Contratante;
- 14.1.7. Instruir os trabalhadores que eventualmente executarem os serviços na sede do Contratante quanto à necessidade de acatar as normas internas da Administração;
- 14.1.8. Relatar ao Contratante toda e qualquer irregularidade verificada no decorrer da prestação dos serviços.

- 14.1.9. Não permitir a utilização de qualquer trabalho do menor de 16 (dezesesseis) anos, exceto na condição de aprendiz para os maiores de 14 (quatorze) anos; nem permitir a utilização do trabalho do menor de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre;
- 14.1.10. Manter durante toda a vigência do Contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas no Termo de Referência;
- 14.1.11. Manter atualizado os seus dados no Cadastro Unificado de Fornecedores, conforme legislação vigente;
- 14.1.12. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do Contrato;
- 14.1.13. Indicar preposto para representá-la durante a execução do contrato;
- 14.1.14. Cumprir o Acordo de Nível de Serviços (ANS);
- 14.1.15. No caso de descumprimento do ANS a contratada estará sujeita as sanções administrativas conforme disposições do item 22 deste Termo de Referência;

14.1.16.SÃO OBRIGAÇÕES DA CONTRATANTE:

- 14.1.17. Receber o objeto no prazo e condições estabelecidas no Edital, e seus anexos;
- 14.1.18. Exigir o cumprimento de todas as obrigações assumidas pela Contratada, de acordo com as cláusulas contratuais e os termos de sua proposta;
- 14.1.19. Verificar minuciosamente, no prazo fixado, a conformidade do objeto recebido provisoriamente, com as especificações constantes do Edital e da proposta, para fins de aceitação e recebimento definitivo;
- 14.1.20. Comunicar à Contratada, por escrito, as imperfeições, falhas ou irregularidades verificadas, fixando prazo para a sua correção;
- 14.1.21. Acompanhar e fiscalizar o cumprimento das obrigações da Contratada, através de comissão ou de servidores especialmente designados;
- 14.1.22. Efetuar o pagamento à Contratada no valor correspondente ao fornecimento do objeto, no prazo e forma estabelecidos no Edital e seus anexos;
- 14.1.23. Efetuar as eventuais retenções tributárias devidas sobre o valor da nota fiscal e fatura fornecida pela Contratada, no

que couber;

- 14.1.24. Prestar as informações e os esclarecimentos que venham a ser solicitados pela Contratada;

15.DA SUBCONTRATAÇÃO

- 15.1. Não será admitida a subcontratação para o objeto deste edital.

16.DA FUNDAMENTAÇÃO LEGAL DA CONTRATAÇÃO

- 16.1. A presente contratação tem fundamento na Lei 13.303/2016, Decreto Municipal n.º 44.698/2018 e Regulamento de Licitações e Contratos da Contratante.

17.DA QUALIFICAÇÃO TÉCNICA DA LICITANTE

- 17.1. Prova de aptidão da empresa licitante para desempenho de atividade pertinente e compatível com o objeto da licitação, por meio de certidão(ões) ou atestado(s), fornecido(s) por pessoa jurídica de direito público ou privado.
- 17.2. A empresa licitante deverá possuir credencial de parceria com o fabricante F5 Networks, no mínimo no nível Gold, nível este que comprova oficialmente que a licitante possui as qualificações técnicas necessárias para prestar os serviços de suporte técnico, bem como possui relação comercial com o fabricante, estando assim autorizada a fornecer os produtos e serviços citados neste documento.
- 17.3. A empresa licitante deverá apresentar carta do fabricante F5 Networks atestando sua capacidade em prestar suporte aos produtos que compõe a solução.
- 17.4. Considera-se compatível com o objeto da licitação o fornecimento de 50% do Lote 1 e ter prestado os serviços do Lote 2 constante na tabela 1 do item 12 deste Termo de Referência, em números compatíveis com o ambiente da CONTRATANTE.
- 17.5. Não será admitida a apresentação de atestado de capacidade técnica emitido por empresa ou empresas do mesmo grupo econômico em favor da licitante participante, no caso desta também pertencer ao grupo econômico.
- 17.6. Será admitida a soma dos atestados ou certidões apresentadas pelas licitantes, desde que os mesmos sejam tecnicamente pertinentes e compatíveis em características, quantidades e prazos com o objeto da licitação.

- 17.7. Não serão aceitos atestados de capacidade técnica com objetos incompatíveis com o objeto desta licitação, como instalação e suporte de computadores, servidores, notebooks, instalação de pontos de redes físicos ou lógicos, ou outros serviços diversos.

18.DO LOCAL DE PRESTAÇÃO DOS SERVIÇOS E DE ENTREGA DO(S) MATERIAL (IS)/EQUIPAMENTO (S)

- 18.1. O (s) serviço (s) deverá (ão) ser prestado (s) e a entrega do (s) material (is)/equipamento (s) deverão ser realizados no seguinte endereço: R. Afonso Cavalcanti 455 - Anexo - Sala 307 - Cidade Nova - Rio de Janeiro - RJ - CEP 20211-110.

19.DA GARANTIA CONTRATUAL

- 19.1. A CONTRATADA prestará garantia de 2% (dois por cento) do valor total do Contrato, como determina o art. 457 do RGCAF, a ser prestada antes do ato de assinatura, em uma das modalidades previstas no art. 445 do RGCAF e no art. 81 do Decreto Municipal n.º 44.698/2018. Seus reforços poderão ser igualmente prestados nas mesmas modalidades. Caso o fornecedor escolha a modalidade seguro- garantia, esta deverá incluir a cobertura das multas eventualmente aplicadas, e, caso escolha a modalidade carta-fiança, deverá observar as regras descritas na legislação municipal aplicável a cada CONTRATANTE.
- 19.2. A CONTRATANTE se utilizará da garantia para assegurar as obrigações associadas à contratação, podendo recorrer a esta inclusive para cobrar valores de multas eventualmente aplicadas e ressarcir-se dos prejuízos que lhe forem causados em virtude do descumprimento das referidas obrigações. Para reparar esses prejuízos, poderá a CONTRATANTE ainda reter créditos.
- 19.3. Os valores das multas impostas por descumprimento das obrigações assumidas na contratação serão descontados da garantia caso não venham a ser quitados no prazo de 03 (três) dias úteis, contados da ciência da aplicação da penalidade. Se a multa aplicada for superior ao valor da garantia prestada, além da perda desta, responderá a CONTRATADA pela diferença, que será descontada dos pagamentos eventualmente devidos pela Administração ou cobrada judicialmente.
- 19.4. Em caso de rescisão decorrente de falta imputável à CONTRATADA, a garantia reverterá integralmente à

CONTRATANTE, que promoverá a cobrança de eventual diferença que venha a ser apurada entre o importe da garantia prestada e o débito verificado.

- 19.5. Na hipótese de descontos da garantia a qualquer título, seu valor original deverá ser integralmente recomposto no prazo de 7 (sete) dias úteis, exceto no caso da cobrança de valores de multas aplicadas, em que esse será de 48 (quarenta e oito) horas, sempre contados da utilização ou da notificação pela CONTRATANTE, o que ocorrer por último, sob pena de rescisão administrativa do Contrato.
- 19.6. Caso o valor da contratação seja alterado, de acordo com o art. 92 do Decreto Municipal 44.698/2018, a CONTRATADA deverá complementar o valor da garantia para que seja mantido o percentual de 2% (dois por cento) do valor do Contrato.
- 19.7. Sempre que houver reajuste ou alteração do valor da contratação, a garantia será complementada no prazo de 7 (sete) dias úteis do recebimento, pela CONTRATADA, do correspondente aviso, sob pena de aplicação das sanções previstas no RGCAF.
- 19.8. A garantia contratual só será liberada ou restituída com o integral cumprimento da contratação, mediante ato liberatório da autoridade contratante, de acordo com o art. 465 do RGCAF e, quando em dinheiro, atualizada monetariamente.

20.DA FISCALIZAÇÃO E ACEITE DO OBJETO

- 20.1. A CONTRATADA submeter-se-á a todas as medidas e procedimentos de Fiscalização. Os atos de fiscalização, inclusive inspeções e testes, executados pela CONTRATANTE e/ou por seus prepostos, não eximem a CONTRATADA de suas obrigações no que se refere ao cumprimento das normas, especificações e projetos, nem de qualquer de suas responsabilidades legais e contratuais.
- 20.2. A Fiscalização da execução do (s) serviço (s) e da entrega dos bens caberá à comissão designada por ato da autoridade competente no âmbito da CONTRATANTE. Incumbe à Fiscalização a prática de todos os atos que lhe são próprios nos termos da legislação em vigor, respeitados o contraditório e a ampla defesa.
- 20.3. A CONTRATADA declara, antecipadamente, aceitar todas as decisões, métodos e processos de inspeção, verificação e controle adotados pela CONTRATANTE, se obrigando a fornecer os dados, elementos, explicações, esclarecimentos e comunicações de que este necessitar e que forem

considerados necessários ao desempenho de suas atividades.

- 20.4. A CONTRATADA se obriga a permitir que o pessoal da fiscalização da CONTRATANTE acesse quaisquer de suas dependências, possibilitando o exame das instalações e também das anotações relativas aos equipamentos, pessoas e materiais, fornecendo, quando solicitados, todos os dados e elementos referentes à execução do contrato.
- 20.5. Compete à CONTRATADA fazer minucioso exame das especificações do (s) serviço (s) e dos bens, de modo a permitir, a tempo e por escrito, apresentar à Fiscalização, para o devido esclarecimento, todas as divergências ou dúvidas porventura encontradas e que venham a impedir o bom desempenho do Contrato. O silêncio implica total aceitação das condições estabelecidas.
- 20.6. A atuação fiscalizadora em nada restringirá a responsabilidade única, integral e exclusiva da CONTRATADA no que concerne aos serviço (s) contratado (s) e bens adquiridos, à sua execução e à entrega e às consequências e implicações, próximas ou remotas, perante a CONTRATANTE, ou perante terceiros, do mesmo modo que a ocorrência de eventuais irregularidades na execução contratual não implicará corresponsabilidade da CONTRATANTE ou de seus prepostos.
- 20.7. A aceitação do objeto deste Termo de Referência se dará mediante a avaliação de Comissão de Fiscalização designada pela autoridade competente no âmbito da CONTRATANTE, e constituída na forma do art. 501, do RGCAF, que constatará se os serviços executados e os bens fornecidos atendem a todas as especificações contidas neste Termo de Referência ou no processo que ensejou a presente contratação.
- 20.8. O objeto do presente Termo de Referência será recebido em tantas parcelas quantas forem às relativas ao pagamento.
- 20.9. Os serviços e bens cujos padrões de qualidade estejam em desacordo com a especificação deste Termo de Referência e seus anexos deverão ser recusados pela Comissão responsável pela fiscalização do contrato, que anotarà em registro próprio as ocorrências e determinará o que for necessário à regularização das faltas ou defeitos observados. No que exceder à sua competência, comunicará o fato à autoridade superior, em 5 (cinco) dias, para ratificação.
- 20.10. Na hipótese de recusa de aceitação, por não atenderem às exigências da CONTRATANTE, a CONTRATADA deverá reexecutar ou substituir quaisquer serviços e bens defeituosos ou qualitativamente inferiores, passando a contar os prazos para pagamento e demais compromissos da CONTRATANTE da

data da efetiva aceitação. Caso a CONTRATADA não reexecute os serviços não aceitos no prazo assinado ou substitua os bens não aceitos no prazo assinado, a CONTRATANTE se reserva o direito de providenciar sua execução ou seu fornecimento às expensas da CONTRATADA, sem prejuízo das penalidades cabíveis.

- 20.11. O Aceite Provisório ficará a cargo da Comissão de Fiscalização, que emitirá Termo de Aceitação Provisória em até 05 (cinco), após a entrega da Solução instalada e configurada.

21. DAS CONDIÇÕES DE PAGAMENTO

- 21.1. Em relação aos itens do Lote 1 da tabela 1, no item 2 de termo de referência, o pagamento será efetuado integralmente à CONTRATADA após a regular liquidação da despesa, nos termos do art. 63 da Lei Federal nº 4.320/64, observada a regras de recebimento do objeto contidas no RLC IPLANKRIO e neste Termo de Referência. O prazo para pagamento será de 30 (trinta) dias, contados da data do protocolo do documento de cobrança no setor competente do(a) CONTRATANTE e obedecido o disposto na legislação.
- 21.2. O pagamento à CONTRATADA será realizado em razão do efetivo fornecimento realizado e aceito, sem que a CONTRATANTE esteja obrigado(a) a pagar o valor total do contrato caso todo o quantitativo do objeto não tenha sido regularmente entregue e aceito.
- 21.3. Em relação ao Item 12 do Lote 2 da tabela 1, no item 2 deste documento, o(s) pagamento(s) será(ão) efetuado(s) mensalmente à CONTRATADA após a regular liquidação da despesa, nos termos do art. 63 da Lei Federal nº 4.320/64, observada a regras de recebimento do objeto neste Termo de Referência. O prazo para pagamento será de 30 (trinta) dias, contados da data do protocolo do documento de cobrança no setor competente do(a) CONTRATANTE e obedecido o disposto na legislação.
- 21.4. Em relação ao Item 13 do Lote 2 da tabela 1, no item 2 deste documento, o pagamento será efetuado 30 dias após a instalação dos equipamentos e aceite dos serviços de instalação.
- 21.5. Para fins de medição, se for o caso, e faturamento, o período-base de medição do serviço prestado será de um mês, considerando-se o mês civil, podendo no primeiro mês e no último, para fins de acerto de contas, o período se constituir em fração do mês, considerado para esse fim o mês com 30 (trinta) dias.

- 21.6. O pagamento à CONTRATADA será realizado em razão dos serviços efetivamente prestados e aceitos no período-base mencionado no item anterior sem que o(a) CONTRATANTE esteja obrigado(a) a pagar o valor total do Contrato.
- 21.7. A CONTRATADA deverá apresentar juntamente com o documento de cobrança, os comprovantes de recolhimento do FGTS e INSS de todos os empregados atuantes no contrato, assim como Certidão Negativa de Débitos Trabalhistas - CNDT ou Certidão Positiva de Débitos Trabalhistas com efeito negativo válida, declaração de regularidade trabalhista, na forma do Anexo do Edital.
- 21.8. O valor dos pagamentos eventualmente efetuados com atraso, desde que não decorra de fato ou ato imputável à CONTRATADA, sofrerá a incidência de juros calculados de acordo com a variação da Taxa Selic, pro rata die entre o 31º (trigésimo primeiro) dia da data do protocolo do documento de cobrança no setor competente da CONTRATANTE e a data do efetivo pagamento, limitado ao percentual de 12% (doze por cento) ao ano.
- 21.9. O valor dos pagamentos eventualmente antecipados será descontado à taxa de 1% (um por cento) ao mês, calculada pro rata die, entre o dia do pagamento e o 30º (trigésimo) dia da data do protocolo do documento de cobrança no setor competente do (a) CONTRATANTE.
- 21.10. O pagamento será efetuado à CONTRATADA através de crédito em conta bancária do fornecedor cadastrado junto à Coordenação do Tesouro Municipal.

22. DAS SANÇÕES ADMINISTRATIVAS

- 22.1. Sem prejuízo de indenização por perdas e danos, a CONTRATANTE poderá impor ao contratado, pelo descumprimento total ou parcial das obrigações a que esteja sujeito, as seguintes sanções, observado o Regulamento Geral do Código de Administração Financeira e Contabilidade Pública do Município do Rio de Janeiro – RGCAF, o Decreto Municipal n.º 44.698/2018 e o Regulamento de Licitações e Contratos da CONTRATANTE, garantida a defesa prévia ao contratado:
- a. Advertência;
 - b. Multa de mora de até 1% (um por cento) por dia útil sobre o valor do Contrato ou do saldo não atendido do Contrato;
 - c. Multa de até 20% (vinte por cento) sobre o valor do Contrato ou do saldo não atendido do Contrato, conforme o caso, e, respectivamente, nas hipóteses de descumprimento total ou parcial da obrigação, inclusive nos casos de rescisão por culpa da CONTRATADA;
 - d. Suspensão temporária do direito de licitar e impedimento de contratar com a Administração Municipal;

- 22.2. As sanções previstas nos incisos I e IV do subitem 22.1 poderão ser aplicadas juntamente com as dos incisos II e III, devendo a defesa prévia do interessado, no respectivo processo, ser apresentada no prazo de 10 (dez) dias úteis e não excluem a possibilidade de rescisão unilateral do contrato;
- 22.3. Do ato que aplicar a pena prevista no inciso IV do subitem 22.1, a autoridade competente no âmbito da CONTRATANTE dará conhecimento aos demais órgãos e entidades municipais interessados, na página oficial desta empresa pública na internet.
- 22.4. A sanção prevista no inciso IV do subitem 22.1 poderá também ser aplicada às empresas ou aos profissionais que, em razão dos contratos regidos pelo Decreto Municipal n.º 44.698/2018:
- I - tenham sofrido condenação definitiva por praticarem, por meios dolosos, fraude fiscal no recolhimento de quaisquer tributos;
 - II - tenham praticado atos ilícitos visando a frustrar os objetivos da licitação;
 - III - demonstrem não possuir idoneidade para contratar com a CONTRATANTE em virtude de atos ilícitos praticados.
- 22.5. As multas previstas nos incisos II e III do subitem 22.1 não possuem caráter compensatório, e, assim, o pagamento delas não eximirá a CONTRATADA de responsabilidade pelas perdas e danos decorrentes das infrações cometidas.
- 22.6. A multa aplicada será depositada em conta bancária indicada pela IplanRio, descontada dos pagamentos eventualmente devidos, descontada da garantia ou cobrada judicialmente.
- 22.7. As multas aplicadas poderão ser compensadas com valores devidos à CONTRATADA mediante requerimento expresso nesse sentido.
- 22.8. Ressalvada a hipótese de existir requerimento de compensação devidamente formalizado, nenhum pagamento será efetuado à CONTRATADA antes da comprovação do recolhimento da multa ou da prova de sua relevação por ato da Administração, bem como antes da recomposição do valor original da garantia, que tenha sido descontado em virtude de multa imposta, salvo decisão fundamentada da autoridade competente que autorize o prosseguimento do processo de pagamento.

23.DA MATRIZ DE RISCOS

- 23.1. Para a presente contratação foram identificados os principais riscos conhecidos na Matriz constante do Anexo I deste Termo de Referência, bem como estabelecidos os respectivos responsáveis e descritas suas respostas sugeridas.
- 23.2. É vedada a celebração de aditivos decorrentes de eventos supervenientes alocados na Matriz de Riscos como sendo de responsabilidade da CONTRATADA.
- 23.3. Sempre que atendidas as condições do contrato e mantidas as disposições da Matriz de Risco, considera-se mantido o equilíbrio econômico-financeiro.
- 23.4. A proposta comercial deverá ser elaborada levando em consideração a natureza e a extensão dos riscos relacionados

na Matriz de Risco.

24. DA PROPOSTA DE PREÇOS

- 24.1. A pretensa CONTRATADA deverá apresentar proposta de preços de acordo com as especificações deste Termo de Referência e nos moldes praticados pelo Município do Rio de Janeiro.
- 24.2. Os preços propostos deverão estar de acordo com os praticados no mercado, em moeda nacional (Reais) e neles deverão estar inclusos todos os impostos, taxas, fretes, material, mão de obra, instalações e quaisquer outras despesas necessárias e não especificadas neste Termo de Referência, mas julgadas essenciais ao cumprimento do objeto desta contratação.

25. DO TIPO DE LICITAÇÃO

- 25.1. O tipo de licitação será o menor preço Global.

26. DA PROTEÇÃO DE DADOS PESSOAIS

- 26.1. Havendo tratamento de dados pessoais no desenvolvimento de quaisquer atividades relacionadas com o objeto, as Partes observarão a Legislação de Privacidade e de Proteção de Dados Pessoais, em especial, a Lei 13.709/2018 (LGPD).

Rio de Janeiro, 22 de junho de 2026.

Leonardo Cavalieri
IPLANRIO/Gerência de Segurança Cibernética

Jorge Francisco Antunes da Silva
IPLANRIO/Diretor de Operações

ANEXO I – MATRIZ DE RISCO

ANEXO I - MATRIZ DE RISCOS PARA O TR Prestação de serviço para atualização das licenças, assistência técnica dos equipamentos "Appliance", suporte técnico especializado "Premium" da Solução de balanceamento BIG-IP F5 existente no Datacenter da IPLANRIO, pelo prazo de 24 (vinte e quatro) meses										
Identificação dos Riscos				Análise Qualitativa				Resposta aos Riscos (Tratamento)		
Id.	Tipo	Risco	Categoria	Sub Categoria	P	I	P x I	Estratégia	Resposta Sugerida	Responsável
R001	Ameaça	Devido a variação cambial, pode haver aumento dos custos dos produtos importados	Aquisições	Bem ou SW	8	8	64	Mitigar	A contratada deverá considerar a variação cambial em sua proposta de preço	Contratada
R002	Ameaça	Devido ao calendário orçamentário da PCRJ, pode haver atraso no pagamento do contrato	Aquisições	Geral	7	9	63	Mitigar	A contratada deverá manter fluxo de caixa para cobrir o período descoberto	Contratada

R007	Ameaça	Devido à logística da contratada, pode haver atraso na entrega de produtos prejudicando o cumprimento do contrato	Aquisições	Entrega	5	8	40	Aceitar Ativamente	A contratada deverá ter planos alternativos para cumprimento do contrato	Contratada
R004	Ameaça	Devido a alteração da política econômico-financeira, pode haver aumento nos tributos após a contratação	Aquisições	Geral	4	5	20	Aceitar Ativamente	A contratada deverá buscar alternativas para cumprimento do contrato	Contratada
R005	Ameaça	Devido a retirada da Solução do mercado, este pode não ser entregue	Aquisições	Aquisição	3	3	9	Aceitar Ativamente	A contratada deverá fornecer produto com especificação igual ou superior ao definido no contrato	Contratada
R006	Ameaça	Falta de peças de reposição do equipamento	Aquisições	Reposição	1	3	3	Aceitar Ativamente	A comissão de fiscalização deverá	Contratante