

TERMO DE REFERÊNCIA

AQUISIÇÃO DE SOLUÇÃO DE OBSERVABILIDADE AVANÇADA DE TRÁFEGO DE REDE DE DADOS COM E SEM CRIPTOGRAFIA, COMPOSTA POR EQUIPAMENTOS, SOFTWARES, LICENÇAS E ACESSÓRIOS, INCLUINDO SERVIÇOS DE INSTALAÇÃO, CONFIGURAÇÃO, SUPORTE TÉCNICO E GARANTIA.

julho de 2026.

1. DO OBJETO

- 1.1. A presente licitação tem por objeto a aquisição de solução de observabilidade avançada de tráfego de rede de dados com e sem criptografia, composta por equipamentos, softwares, licenças e acessórios, incluindo serviços de instalação, configuração, suporte técnico e garantia.
- 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.

2. DA DESCRIÇÃO DOS SERVIÇOS, MATERIAIS / EQUIPAMENTOS

ITEM	DESCRIÇÃO	UND	QTD
1	Módulo de Observabilidade Decriptada SSL (Hardware)	UND	1
2	Módulo de Observabilidade Decriptada SSL (Software)	UND	1
3	Módulo de Observabilidade e Privacidade (Hardware)	UND	1
4	Módulo de Observabilidade e Privacidade (Software)	UND	1
5	Voucher Treinamento Oficial	UND	4
6	Suporte técnico	Meses	24

Tabela 1

3. ESPECIFICAÇÕES TÉCNICAS – DETALHAMENTO

3.1. ITENS 1 E 2 – MÓDULO DE OBSERVABILIDADE DECRYPTADA SSL

CARACTERÍSTICAS GERAIS

- 3.1.1. O equipamento deve ser baseado em Appliance suportando montagem em rack (bastidor) de 19" (dezenove polegadas), com utilização de no máximo 1-RU (uma unidade de bastidor) de altura, com fornecimento dos respectivos conjuntos de fixação;
- 3.1.2. Os equipamentos ofertados deverão possuir funcionalidades e hardware específicos para este propósito de agregação, regeneração, filtragem e modificação/transformação do tráfego, não sendo aceita soluções similares, como: Switches, Roteadores, Firewalls, Balanceadores, Servidores, soluções Híbridas etc.;
- 3.1.3. A solução deverá ser composta por único fabricante, incluindo os itens de Agregador, módulos e GBICs, com vista a não desperdício de recursos técnicos e facilidade de integração;
- 3.1.4. Deverá possibilitar a configuração dinâmica de portas por software, permitindo a definição de portas de "Rede", "Rede Inline", "Ferramenta" e portas de "Ferramenta Inline";
- 3.1.5. Entende-se por portas de Rede, todas as portas que serão responsáveis por receber a cópia do tráfego através dos TAPs/SPANs;
- 3.1.6. Entende-se por portas de Ferramenta, todas as portas que serão responsáveis por encaminhar o tráfego, seja ele já filtrado e/ou modificado, para as ferramentas que serão conectadas a solução de NPB;
- 3.1.7. Entende-se por portas de Rede Inline, todas as portas que serão responsáveis por se conectar de forma Inline a rede de produção;
- 3.1.8. Entende-se por portas de Ferramenta Inline, todas as portas que serão responsáveis por encaminhar o tráfego de produção, selecionado através dos filtros ou não, para as ferramentas Inline que serão conectadas a solução de NPB;

- 3.1.9. A solução deverá suportar interfaces de 1 Gbps, 10Gbps, 25Gbps, 40Gbps e 100 Gbps através da adição ou substituição módulos/licenças, sem causar impacto no desempenho dos equipamentos ofertados;
- 3.1.10. O equipamento deverá possuir a capacidade de processamento de, no mínimo, 1.8Tbps (um ponto oito) Tbps de tráfego agregado para aplicação dos filtros (regras) descritos nesta especificação;
- 3.1.11. O equipamento deve estar em conformidade com o padrão RoHS;
- 3.1.12. Deverá possuir módulos de ventilação hot swappable;
- 3.1.13. Possuir ventilação "front-to-back", ou seja, a saída de ar quente deve acontecer pela traseira do equipamento;
- 3.1.14. Deverá possuir fonte de alimentação interna que trabalhe em 100V-240V, 50/60 Hz, com detecção automática de tensão e frequência, hot-swappable;
- 3.1.15. Deverá possuir fonte de alimentação AC redundante interna, hot-swappable;
- 3.1.16. Deverá realizar automaticamente o deploy do Network Packet Broker com o mínimo de intervenção do usuário, mediante utilização de ZTP (Zero Touch Provisioning), assegurando que após reset de fábrica ou instalação inicial o dispositivo se autoconfigure por meio de arquivo previamente definido;
- 3.1.17. Deverá suportar simultaneamente em sua memória Flash (ou semelhante), duas imagens do sistema operacional entregue com o equipamento;
- 3.1.18. São apresentadas, a seguir, as especificações técnicas mínimas a serem ofertadas referentes ao objeto. Os termos "possuir", "permite/permitir", "implementar" e "é" implicam no fornecimento de todos os elementos necessários à adoção da tecnologia ou funcionalidade citada. O termo "ou" implica que a especificação técnica mínima dos serviços pode ser atendida por somente uma das opções. O termo "e" implica que a especificação técnica mínima dos serviços deve ser atendida englobando todas as opções;
- 3.1.19. A solução é definida como um Network Packet Broker, ou seja, realiza características de um broker a nível de pacotes de rede. Uma solução específica caracterizada como SSL Decryption ou com funcionalidade de SSL Inspection realiza apenas uma das múltiplas funções de um Network Packet Broker. Desta forma, não serão aceitas soluções como Firewalls UTM, Next-Generation Firewall (NGFW), Load Balancers com funcionalidade de SSL Offloading;
- 3.1.20. Com o intuito de garantir a homologação do equipamento ofertado, no que tange o seu padrão de qualidade, de segurança, de compatibilidade eletromagnética, de não agressão ao meio ambiente e de funcionalidade técnica regulamentada, deverá ser anexada a sua certificação oficial ANATEL para o network packet broker;
- 3.1.21. Os componentes de Hardware da solução devem possuir garantia do fabricante de, no mínimo, 36 (trinta e seis meses).

GERENCIAMENTO DO NETWORK PACKET BROKER

- 3.1.22. Deverá permitir configuração customizada baseadas nos perfis de acesso (RBAC - Role Base Access Control);
- 3.1.23. Deverá implementar os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps;
- 3.1.24. Deverá possuir suporte a MIB II;

- 3.1.25. Deverá implementar a MIB privativa que forneça informações relativas ao funcionamento do equipamento;
- 3.1.26. Deverá suportar SNMP trap sobre IPv6;
- 3.1.27. Deverá suportar configuração total da solução através de console local RS-232 ou RJ-45, bem como deverá permitir configurar total da solução através de interface de linha de comando (CLI);
- 3.1.28. Deverá permitir a atualização remota do sistema operacional e arquivos de configuração utilizados no equipamento via interface de gerenciamento;
- 3.1.29. Deverá permitir a gravação de log externo (syslog);
- 3.1.30. Deverá permitir o armazenamento de sua configuração em memória não volátil, podendo, numa queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior à queda de alimentação;
- 3.1.31. Deverá possuir ferramentas para depuração e gerenciamento em primeiro nível, tais como estatísticas de utilização e log de eventos;
- 3.1.32. Deverá suportar configuração total da solução através de console local RS-232 ou RJ-45;
- 3.1.33. Deverá possuir gerenciamento através de interface Web (HTTPS) ou CLI;
- 3.1.34. Deverá implementar o protocolo NTP (Network Time Protocol);
- 3.1.35. Deverá implementar mecanismo de autenticação para acesso local ou remoto ao equipamento baseada em um Servidor de Autenticação/Autorização do tipo TACACS/TACACS+, RADIUS e LDAP;
- 3.1.36. Deverá suportar IPv6 para TACACS+;
- 3.1.37. Deverá implementar o protocolo SSHv2 para acesso à interface de linha de comando;
- 3.1.38. Deverá proteger a interface de comando do equipamento através de senha;
- 3.1.39. Possuir gerenciador em um único ponto central para orquestrar todo os elementos físicos, virtuais, em nuvem e containers que compõem o projeto. A solução deve permitir o gerenciamento de todos os componentes da solução, incluindo appliances físicos e virtuais, nuvem e containers;

FILTROS (REGRAS)

- 3.1.40. A solução deverá implementar as seguintes configurações para agregação e encaminhamento de pacotes das portas de Rede para as portas de Ferramentas, tanto para os fluxos Out-of-Band (Cópia de Tráfego) quanto para Inline, respectivamente:
 - 3.1.40.1. Uma para uma;
 - 3.1.40.2. Uma para Várias - Com suporte a balanceamento;
 - 3.1.40.3. Várias para uma;
 - 3.1.40.4. Várias para Várias - Com suporte a balanceamento;
- 3.1.41. Deverá permitir criar filtros (regras) baseados em, no mínimo, os seguintes campos:
 - 3.1.41.1. Endereços MAC de origem e destino;
 - 3.1.41.2. Endereço IPv4 de origem/destino;
 - 3.1.41.3. Portas TCP e UDP de origem e destino;

- 3.1.41.4. VLAN ID;
- 3.1.41.5. Ethertype;
- 3.1.41.6. IPFrag;
- 3.1.41.7. TTL;
- 3.1.41.8. TOS;
- 3.1.41.9. Protocol;
- 3.1.41.10. TCP Control Mask/Bits;
- 3.1.41.11. DSCP;
- 3.1.41.12. Versão do Protocolo IPv4 e IPv6;
- 3.1.41.13. Endereço IPv6 de origem/destino;
- 3.1.42. Deverá suportar a reescrita de endereços IPs ou MAC Address para proteger a confidencialidade dos endereços IP reais;
- 3.1.43. A solução deverá suportar, no mínimo, 35.000 (trinta e cinco mil) filtros (regras);
- 3.1.44. Deverá permitir a inserção e remoção de novos filtros (regras) sem a necessidade de reiniciar o(s) equipamento(s), ou seja, a aplicação destes filtros (regras) deverá acontecer em tempo real;
- 3.1.45. Deve suportar overlapping de filtros (regras), ou seja, utilização conjunta de filtros de entrada (ingress) e filtros de saída (egress);
- 3.1.46. A solução deverá implementar funcionalidade Mesh/Cluster;
- 3.1.47. O Mesh/Cluster deverá permitir a configuração e gerenciamento de 2 (dois) ou mais agregadores como um único equipamento lógico. Não serão aceitas soluções em cascata para o atendimento desta funcionalidade;
- 3.1.48. A solução deverá suportar, no mínimo, 30 agregadores em modo Mesh/Cluster;
- 3.1.49. O Mesh/Cluster deverá permitir a configuração de todos os Agregadores a partir de uma única interface WEB (HTTPS) e CLI;
- 3.1.50. A funcionalidade de Mesh/Cluster deverá suportar a criação de 1 (um) ou mais filtros (regras) que se utilizem de portas de Rede em um equipamento físico e direcionem este tráfego para portas de Ferramenta localizadas em outro equipamento físico, independentemente da quantidade de equipamentos entre estes equipamentos. Não serão aceitas soluções em cascata para o atendimento deste item;
- 3.1.51. A funcionalidade de Mesh/Cluster deve suportar arquitetura conhecida como Spine/Leaf, permitindo balanceamento do tráfego entre os Leafs e os Spines e adicionando redundância a solução em caso de falha de um dos equipamentos;
- 3.1.52. Deve suportar o conceito de FABRIC que permite a criação de filtros que se estendem por múltiplos agregadores ou mesh/clusters de agregadores;
- 3.1.53. Deve permitir a configuração de circuitos entre mesh/clusters de agregadores, permitindo que o tráfego recebido em um cluster seja entregue para uma ferramenta em outro cluster;

FUNCIONALIDADES INLINE

- 3.1.54. O equipamento deve implementar instalação sem necessidade de reconfiguração de roteadores e switches, quando utilizado no modo de operação Inline;

- 3.1.55. O equipamento deve implementar, de forma simultânea e em interfaces distintas, os modos:
- 3.1.55.1. TAP/SPAN (Cópia de Tráfego);
 - 3.1.55.2. Inline (Tráfego de Produção);
- 3.1.56. A solução deverá ser capaz de configurar a sequência das ferramentas Inline (Serial), quando possuir 2 (duas) ou mais ferramentas, pela qual os pacotes deverão ser encaminhados sequencialmente quando o agregador funcionar de forma Inline;
- 3.1.57. A solução deverá ser capaz de configurar um grupo de ferramentas Inline (Paralelo), quando possuir 2 (duas) ou mais ferramentas, pela qual os pacotes deverão ser balanceados entre as ferramentas quando o agregador funcionar de forma Inline;
- 3.1.58. A solução deverá permitir a configuração conjunta das funcionalidades Serial e Paralelo, permitindo criar uma sequência serial de ferramentas que estão em Paralelo;
- 3.1.59. A solução deverá permitir que ferramentas inline em modo standalone, serial e paralelo, possam ter a flexibilidade de receber somente o tráfego de interesse, sem impacto entre elas e sem a necessidade de solução de contorno físico. Por exemplo, a ferramenta 1 precisa receber todo o tráfego e a ferramenta 2 necessita receber apenas tráfego WEB, nesse tipo de cenário as ferramentas devem receber o tráfego desejado sem necessidade de arranjos físicos e sem impactar o tráfego da outra;
- 3.1.60. Implementar funcionalidade conhecida como Fail-Safe através do uso de bypass, que mesmo em caso de perda de energia, os links interceptados da rede continuem ativos, não gerando indisponibilidade de rede;
- 3.1.61. Não é permitido composição com bypass externo, este deve ser obrigatoriamente do mesmo fabricante do restante da solução não é permitido composição com bypass OEM ou de terceiros;
- 3.1.62. A solução deve suportar Heartbeat para monitoramento da saúde das ferramentas, quando utilizadas de forma Inline, permitindo detectar e remover somente a ferramenta que apresentar falha, sem causar impacto no fluxo de dados das outras ferramentas e no tráfego de rede;
- 3.1.63. A solução deve suportar Heartbeat Negativo, que permite utilizar um pacote específico para a geração do tráfego de checagem, no entanto, este pacote deve ser bloqueado pela ferramenta inline, não retornando novamente para a solução de NPB. Caso este pacote retorne a ferramenta inline será considerada com falha e deverá ser removida sem impacto na rede e nos fluxos de dados;
- 3.1.64. A solução, quando utilizada em modo Inline, deve permitir remover uma ou mais ferramentas da sequência do tráfego sem causar impacto no tráfego da rede. Esta funcionalidade tem como principal objetivo remover ferramentas para atualização e para fins de troubleshooting, sem causar interrupção de rede;
- 3.1.65. A solução deve permitir a alteração do modo de operação sem causar interrupção de rede da ferramenta inline para “simulação inline” sem causar interrupção de rede, de modo que a ferramenta entenda que está inline mas está recebendo apenas uma cópia dos dados que foram encaminhados para rede.

INTERFACES

- 3.1.66. A solução deverá suportar, no mínimo, 32 (trinta e duas) interfaces 1Gb;

- 3.1.67. A solução deverá suportar, no mínimo, 72 (setenta e duas) interfaces 10/25Gb;
- 3.1.68. A solução deverá implementar, no mínimo, 8 (oito) interfaces 1/10/25Gb SFP28. Todas as portas devem ser fornecidas com transceivers de 10Gb SFP+ LC MM;
- 3.1.69. A solução deverá implementar, no mínimo, 4 (quatro) interfaces 40/100Gb QSFP28. Todas as portas devem ser fornecidas com transceivers de 100Gb Q28 SR4 MM MPO12;
- 3.1.70. A solução deverá implementar, no mínimo, 6 (seis) pares de interfaces BPS em fibra para 1G/10G com conectores LC;
- 3.1.71. Não serão aceitas soluções com Bypass externo ao agregador;
- 3.1.72. Não serão aceitas soluções que utilizam baterias para manter o funcionamento do bypass;
- 3.1.73. Todas as licenças devem ser fornecidas com vigência e suporte por trinta e seis (36) meses;
- 3.1.74. Todas as portas físicas do equipamento fornecido deverão estar habilitadas e devidamente licenciadas para captura de pacotes, encontrando-se prontas para uso imediato em fábrica, independentemente de terem sido ou não explicitamente especificadas neste Termo de Referência, não sendo admitida qualquer forma de licenciamento parcial, expansão progressiva, ativação futura ou aquisição adicional de licenças.

FUNCIONALIDADES AVANÇADAS

- 3.1.75. Deve implementar a funcionalidade SSL Decryption através de função Man-In-The-Middle e somente cópia do tráfego;
- 3.1.76. Deve implementar a funcionalidade SSL Decryption Inline e Out-Of-Band;
- 3.1.77. O equipamento deve implementar um throughput exclusivo de tráfego criptografado de, no mínimo, 7.4 (sete ponto quatro) Gbps;
- 3.1.78. A descryptografia deve ser baseada no handshake SSL/TLS e não através de portas pré-definidas.
- 3.1.79. O equipamento deve permitir importação de no mínimo 1.000 (um mil) certificados em formato PKCS #12 ou PEM;
- 3.1.80. Suportar o mínimo de 10 (dez) mil novas conexões SSL por segundo, utilizando cifra 'TLS_RSA_WITH_AES_128_CBC_SHA256' e criptografia RSA de 2048 bits;
- 3.1.81. implementar no mínimo 100 mil conexões SSL simultâneas utilizando criptografia de 2048 bits;
- 3.1.82. O equipamento deve implementar, no mínimo, os seguintes algoritmos de troca de chaves com autenticação:
 - 3.1.82.1. RSA;
 - 3.1.82.2. DHE;
 - 3.1.82.3. DHE_RSA;
 - 3.1.82.4. ECDHE com PFS (Perfect Forward Secrecy)
 - 3.1.82.5. ECDHE_RSA;
 - 3.1.82.6. ECDHE_ECDSA;

- 3.1.83. O equipamento deve implementar, no mínimo, os seguintes métodos de autenticação de mensagens:
- 3.1.83.1. SHA;
 - 3.1.83.2. SHA256;
 - 3.1.83.3. SHA384;
 - 3.1.83.4. POLY1305;
- 3.1.84. O equipamento deve implementar, no mínimo, os seguintes algoritmos PQC Post-Quantum Cryptography:
- 3.1.84.1. KEM;
 - 3.1.84.2. ML-KEM (CRYSTALS-KYBER) em variantes mlkem512, mlkem768, mlkem1024;
 - 3.1.84.3. Combinações Hybrid X25519_MLKEM768, SecP256r1_MLKEM768, SecP384r1MLKEM1024;
 - 3.1.84.4. ML-DSA (CRYSTALS-DILITHIUM) em variantes mldsa44, mldsa65, mldsa87;
- 3.1.85. Deverá implementar Host Categorization, permitindo selecionar tráfegos que não serão descryptografados, como dados financeiros por exemplo;
- 3.1.86. Deverá ser capaz de descryptografar tráfego TLS/SSL e integrá-lo via ICAP com ferramentas, tais como DLP, para inspeção de conteúdo em texto claro;
- 3.1.87. A funcionalidade SSL Decryption deve implementar, no mínimo, os seguintes protocolos:
- 3.1.87.1. SSL 3;
 - 3.1.87.2. TLS 1.0;
 - 3.1.87.3. TLS 1.1;
 - 3.1.87.4. TLS 1.2;
 - 3.1.87.5. TLS 1.3;
 - 3.1.87.6. mTLS;
- 3.1.88. Deve implementar chaves de 1024 bits, 2048 bits e 4096 bits;
- 3.1.89. O equipamento deve implementar, no mínimo, as seguintes cifras de criptografia:
- 3.1.89.1. AES_128_CBC;
 - 3.1.89.2. AES_256_CBC;
 - 3.1.89.3. AES_256_GCM;
 - 3.1.89.4. CHACHA20;
 - 3.1.89.5. Camellia128;
 - 3.1.89.6. Camellia256;
 - 3.1.89.7. DES_CBC;
 - 3.1.89.8. 3DES_EDE_CBC;
 - 3.1.89.9. SEED;

- 3.1.89.10. IDEA;
- 3.1.89.11. Chacah20-Poly1305.

GERENCIA CENTRALIZADA

- 3.1.90. Deverá ser fornecido um software capaz de controlar, administrar, gerenciar e monitorar a solução de Visibilidade;
- 3.1.91. O software deverá estar licenciado para, no mínimo, 5 ativos físicos da solução de Visibilidade, e permitir upgrades através da aquisição de licença adicional;
- 3.1.92. Possuir gerenciador único em um único ponto central para orquestrar todo os elementos físicos, virtuais, em nuvem e containers que compõem o projeto. A solução deve permitir o gerenciamento de todos os componentes da solução, incluindo appliances físicos e virtuais, nuvem e containers;
- 3.1.93. A solução deve possuir uma interface gráfica e intuitiva com API abertas para simples customização de aplicações e integração com produtos de terceiros;
- 3.1.94. A solução deve implementar Automação com Ansible e uso de API REST;
- 3.1.95. O dispositivo pode ser fornecido em forma de servidor físico instalados, configurados e possuindo todos os softwares necessários para prover os requisitos técnicos especificados, inclusive o sistema operacional, sem qualquer ônus adicional;
- 3.1.96. O dispositivo também pode ser fornecido em forma de appliance virtual compatível com hypervisors VMware e Hyper-V;
- 3.1.97. No caso de servidores, a solução poderá adotar hardwares padrão de mercado, desde que atendam aos requisitos recomendados pela última versão do manual de instalação dos softwares utilizados, no momento da assinatura do contrato;
- 3.1.98. Para ambos os casos deverá possuir altura máxima de 1RU;
- 3.1.99. Todo hardware que compõe a solução deverá possuir alimentação elétrica de 110/240 V, 47 a 63 Hz, com chaveamento automático;
- 3.1.100. A solução deve ser capaz de visualizar e gerenciar os dados e métricas coletadas em múltiplos segmentos monitorados em uma única console (centralizada), permitindo desta forma integração, maior segurança, escalabilidade, robustez e disponibilidade da solução;
- 3.1.101. Possuir interface gráfica para a criação dos filtros (regras), onde é possível selecionar as portas de Rede e as portas de Ferramentas, independentemente do equipamento físico. Os filtros (regras) criados para estes tráfegos deverão ser aplicados através desta mesma interface Web (HTTPS), facilitando a operação e entendimento dos fluxos;
- 3.1.102. A solução deve possibilitar a configuração de diferentes perfis de administradores. Deve ser possível ainda criar usuários com perfil de administração e outros de apenas visualização;
- 3.1.103. Deve permite gerar um token somente se você for um usuário autenticado e com base em seus privilégios de acesso a Gerência;
- 3.1.104. A solução deve permitir que os usuários façam “drill down” a partir de visões de alto nível, orientadas a serviços, até visões técnicas com dados detalhados, que auxiliem na análise da causa raiz do problema;
- 3.1.105. Deve permitir a criação de topologias da solução de Visibilidade para todos os

equipamentos ativos e gerenciáveis;

- 3.1.106. Deve permitir a identificação do status das portas dos dispositivos up ou down, tecnologia e velocidade das portas;
- 3.1.107. A solução deve permitir o inventário detalhado de atributos dos ativos da solução, atendendo, no mínimo, números seriais, módulos instalados, status do equipamento e versão de software instalado;
- 3.1.108. A solução deve permitir o armazenamento das configurações dos dispositivos;
- 3.1.109. A ferramenta deve permitir o agendamento da função de armazenamento de configuração de determinados elementos da rede. O agendamento deve ter periodicidade mínima de um dia;
- 3.1.110. Deve permitir o upgrade do sistema operacional ou Boot Prom dos dispositivos, unitariamente e para um grupo de dispositivos, inclusive podendo agendar um dia e horário para que este upgrade aconteça automaticamente;
- 3.1.111. A ferramenta deve permitir a execução do reset dos dispositivos;
- 3.1.112. A ferramenta deve permitir restaurar a configuração armazenada. Deve ser possível ainda aplicar essa configuração em um equipamento em processo de substituição;
- 3.1.113. Deve permitir a instalação dos TAPs virtuais a partir da console de gerência;
- 3.1.114. Deve possuir integração via API com a VMware, para permitir cópia do tráfego entre as VMs mesmo em caso de mobilidade das VMs;
- 3.1.115. A solução deverá ser capaz de criar e configurar os filtros (regras) virtuais, ou seja, os filtros (regras) que serão aplicados dentro da solução virtual para que seja espelhado para fora do servidor somente o tráfego desejado;
- 3.1.116. A solução deverá possuir dashboards com, no mínimo, as seguintes informações:
 - 3.1.116.1. Total de portas que estão perdendo pacotes;
 - 3.1.116.2. Total de portas acima do limite de utilização, tanto portas de Rede como portas de Ferramenta;
 - 3.1.116.3. TOP portas com maior utilização;
- 3.1.117. Visualização simplificada de todos os filtros (regras) aplicados, indicando as portas de Redes e Ferramentas;
- 3.1.118. Requisitos de Logs:
 - 3.1.118.1. A solução deve possuir ferramenta para acompanhamento e análise de eventos de logs;
 - 3.1.118.2. Deve permitir a geração de log externo (syslog) para integração com soluções de SIEM;
 - 3.1.118.3. A solução deverá gerar e armazenar trilhas de auditoria que permitam o rastreamento de ações efetuadas em todos os seus componentes. Os registros de logs devem conter a identificação do evento, data e hora, identificação do usuário, identificação do dispositivo e endereço IP do dispositivo ou permitir que estas informações sejam correlacionadas com o mecanismo de SIEM como por exemplo QRadar IBM e Splunk;
- 3.1.119. Deve apresentar dashboards de estatísticas de Inline SSL;

- 3.1.119.1. Novas conexões/handshakes por segundo;
- 3.1.119.2. Número de conexões concorrentes;
- 3.1.119.3. Totais sessões interceptadas;
- 3.1.119.4. Média de CPU;
- 3.1.119.5. Versão TLS Client/Server;
- 3.1.119.6. Média de decryption por engine;
- 3.1.119.7. Taxa de tráfego; e
- 3.1.119.8. Sessões descriptografadas.
- 3.1.119.9. Volume total (Bytes);
- 3.1.119.10. Throughput Client e Server (bps);
- 3.1.119.11. Distribuição dos Modos do SSL Outbound, Inbound e Não SSL;
- 3.1.119.12. Top 10 URLs e categorias acessadas pelo inline ssl;
- 3.1.119.13. Top 10 Cifras;

INSTALAÇÃO E CONFIGURAÇÃO MÓDULO DE OBSERVABILIDADE DECRYPTADA SSL

- 3.1.120. Os serviços de instalação física, configuração e documentação, deverão ser executados por equipe técnica da CONTRATADA;
- 3.1.121. O(s) profissional(is) técnico(s) da CONTRATADA responsável(is) pelos serviços descritos neste ITEM deve(m) possuir os certificados dos fabricantes das soluções respectivas;
- 3.1.122. A implantação deverá contemplar as seguintes fases:
 - 3.1.122.1. **Planejamento:** nesta etapa a Contratada deverá realizar o planejamento do projeto, onde serão definidos os prazos por atividade, as pessoas, a estratégia de implantação do serviço, o plano de testes, a localização dos equipamentos na arquitetura da rede do órgão, bem como quaisquer outros itens que sejam necessários para a implantação do projeto. Devem-se considerar as janelas de manutenção do órgão, plano de rollback e o escopo definido. Os responsáveis técnicos do órgão acompanharão e aprovarão o planejamento.
 - 3.1.122.2. **Documentação do projeto:** Deverá ser entregue a documentação do projeto, conforme descrita a seguir, em formato e quantidade a serem acordados entre as partes e nos momentos especificados.
 - 3.1.122.3. **Plano de Requisitos de Infraestrutura:** A CONTRATADA, antes de iniciar a execução das instalações deve levantar as necessidades de infraestrutura necessárias para instalação da configuração (espaço em rack, energização, refrigeração, tipo de conectorização, entre outros).
 - 3.1.122.4. **Plano de Implementação:** A CONTRATADA, antes de iniciar a execução das configurações, deverá elaborar uma documentação técnica fundamentando todas as configurações que serão realizadas.
 - 3.1.122.5. **Plano de Migração:** A CONTRATADA, antes de iniciar a execução das configurações, deverá analisar o ambiente do órgão para avaliar como será realizada a integração e a migração do ambiente atual de Produção.

3.1.123. Após a aprovação do planejamento deverá ser iniciado o processo de implantação, levando-se em consideração a disponibilidade das equipes envolvidas e cumprimento dos prazos pactuados, contemplando:

- 3.1.123.1. Instalação física dos equipamentos;
- 3.1.123.2. Configuração;
- 3.1.123.3. Instalação em ambiente;
- 3.1.123.4. Etapa de testes e de funcionamento experimental;
- 3.1.123.5. Migração;
- 3.1.123.6. Validação do funcionamento em ambiente de produção;
- 3.1.123.7. Documentação Final.

3.2. ITENS 3 E 4 – MÓDULO DE OBSERVABILIDADE E PRIVACIDADE

CARACTERÍSTICAS GERAIS

- 3.2.1. O equipamento deve ser baseado em Appliance suportando montagem em rack (bastidor) de 19" (dezenove polegadas), com utilização de no máximo 1-RU (uma unidade de bastidor) de altura, com fornecimento dos respectivos conjuntos de fixação;
- 3.2.2. Os equipamentos ofertados deverão possuir funcionalidades e hardware específicos para este propósito de agregação, regeneração, filtragem e modificação/transformação do tráfego, não sendo aceita soluções similares, como: Switches, Roteadores, Firewalls, Balanceadores, Servidores, soluções Híbridas etc.;
- 3.2.3. A solução deverá ser composta por único fabricante, incluindo os itens de Agregador, módulos e GBICs, com vista a não desperdício de recursos técnicos e facilidade de integração;
- 3.2.4. Deverá possibilitar a configuração dinâmica de portas por software, permitindo a definição de portas de "Rede", "Rede Inline", "Ferramenta" e portas de "Ferramenta Inline";
- 3.2.5. Entende-se por portas de Rede, todas as portas que serão responsáveis por receber a cópia do tráfego através dos TAPs/SPANs;
- 3.2.6. Entende-se por portas de Ferramenta, todas as portas que serão responsáveis por encaminhar o tráfego, seja ele já filtrado e/ou modificado, para as ferramentas que serão conectadas a solução de NPB;
- 3.2.7. Entende-se por portas de Rede Inline, todas as portas que serão responsáveis por se conectar de forma Inline a rede de produção;
- 3.2.8. Entende-se por portas de Ferramenta Inline, todas as portas que serão responsáveis por encaminhar o tráfego de produção, selecionado através dos filtros ou não, para as ferramentas Inline que serão conectadas a solução de NPB.
- 3.2.9. A solução deverá suportar interfaces de 1 Gbps, 10Gbps, 25Gbps, 40Gbps e 100 Gbps através da adição ou substituição módulos/licenças, sem causar impacto no desempenho dos equipamentos ofertados;
- 3.2.10. O equipamento deverá possuir a capacidade de processamento de, no mínimo, 1.8Tbps (um ponto oito) Tbps de tráfego agregado para aplicação dos filtros (regras)

descritos nesta especificação;

- 3.2.11. O equipamento deve estar em conformidade com o padrão RoHS;
- 3.2.12. Deverá possuir módulos de ventilação hot swappable;
- 3.2.13. Possuir ventilação "front-to-back", ou seja, a saída de ar quente deve acontecer pela traseira do equipamento;
- 3.2.14. Deverá possuir fonte de alimentação interna que trabalhe em 100V-240V, 50/60 Hz, com detecção automática de tensão e frequência, hot-swappable;
- 3.2.15. Deverá possuir fonte de alimentação AC redundante interna, hot-swappable;
- 3.2.16. Deverá realizar automaticamente o deploy do Network Packet Broker com o mínimo de intervenção do usuário, mediante utilização de ZTP (Zero Touch Provisioning), assegurando que após reset de fábrica ou instalação inicial o dispositivo se auto configure por meio de arquivo previamente definido;
- 3.2.17. Deverá suportar simultaneamente em sua memória Flash (ou semelhante), duas imagens do sistema operacional entregue com o equipamento;
- 3.2.18. São apresentadas, a seguir, as especificações técnicas mínimas a serem ofertadas referentes ao objeto. Os termos "possuir", "permite/permitir", "implementar" e "é" implicam no fornecimento de todos os elementos necessários à adoção da tecnologia ou funcionalidade citada. O termo "ou" implica que a especificação técnica mínima dos serviços pode ser atendida por somente uma das opções. O termo "e" implica que a especificação técnica mínima dos serviços deve ser atendida englobando todas as opções;
- 3.2.19. A solução é definida como um Network Packet Broker, ou seja, realiza características de um broker a nível de pacotes de rede. Uma solução específica caracterizada como SSL Decryption ou com funcionalidade de SSL Inspection realiza apenas uma das múltiplas funções de um Network Packet Broker. Desta forma, não serão aceitas soluções como Firewalls UTM, Next-Generation Firewall (NGFW), Load Balancers com funcionalidade de SSL Offloading, e tais atestados não serão considerados como válidos;
- 3.2.20. Com o intuito de garantir a homologação do equipamento ofertado, no que tange o seu padrão de qualidade, de segurança, de compatibilidade eletromagnética, de não agressão ao meio ambiente e de funcionalidade técnica regulamentada, deverá ser anexada a sua certificação oficial ANATEL para o network packet broker;
- 3.2.21. Os componentes de Hardware da solução devem possuir garantia do fabricante de, no mínimo, 36 (trinta e seis meses a partir da emissão do aceite definitivo).

GERENCIAMENTO DO NETWORK PACKET BROKER

- 3.2.22. Deverá permitir configuração customizada baseadas nos perfis de acesso (RBAC - Role Base Access Control);
- 3.2.23. Deverá implementar os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps;
- 3.2.24. Deverá possuir suporte a MIB II;
- 3.2.25. Deverá implementar a MIB privativa que forneça informações relativas ao funcionamento do equipamento;
- 3.2.26. Deverá suportar SNMP trap sobre IPv6;

- 3.2.27. Deve suportar configuração total da solução através de console local RS-232 ou RJ-45, bem como deverá permitir configurar total da solução através de interface de linha de comando (CLI);
- 3.2.28. Deverá permitir a atualização remota do sistema operacional e arquivos de configuração utilizados no equipamento via interface de gerenciamento;
- 3.2.29. Deverá permitir a gravação de log externo (syslog);
- 3.2.30. Deverá permitir o armazenamento de sua configuração em memória não volátil, podendo, numa queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior à queda de alimentação;
- 3.2.31. Deverá possuir ferramentas para depuração e gerenciamento em primeiro nível, tais como estatísticas de utilização e log de eventos;
- 3.2.32. Deve suportar configuração total da solução através de console local RS-232 ou RJ-45;
- 3.2.33. Deve possuir gerenciamento através de interface Web (HTTPS) ou CLI;
- 3.2.34. Deverá implementar o protocolo NTP (Network Time Protocol);
- 3.2.35. Deverá implementar mecanismo de autenticação para acesso local ou remoto ao equipamento baseada em um Servidor de Autenticação/Autorização do tipo TACACS/TACACS+, RADIUS e LDAP;
- 3.2.36. Deve suportar IPv6 para TACACS+;
- 3.2.37. Deverá implementar o protocolo SSHv2 para acesso à interface de linha de comando;
- 3.2.38. Deverá proteger a interface de comando do equipamento através de senha;
- 3.2.39. Possuir gerenciador em um único ponto central para orquestrar todo os elementos físicos, virtuais, em nuvem e containers que compõem o projeto. A solução deve permitir o gerenciamento de todos os componentes da solução, incluindo appliances físicos e virtuais, nuvem e containers.

FILTROS (REGRAS):

- 3.2.40. A solução deverá implementar as seguintes configurações para agregação e encaminhamento de pacotes das portas de Rede para as portas de Ferramentas, tanto para os fluxos Out-of-Band (Cópia de Tráfego) quanto para Inline, respectivamente:
 - 3.2.40.1. Uma para uma;
 - 3.2.40.2. Uma para Várias - Com suporte a balanceamento;
 - 3.2.40.3. Várias para uma;
 - 3.2.40.4. Várias para Várias - Com suporte a balanceamento;
- 3.2.41. Deverá permitir criar filtros (regras) baseados em, no mínimo, os seguintes campos:
 - 3.2.41.1. Endereços MAC de origem e destino;
 - 3.2.41.2. Endereço IPv4 de origem/destino;
 - 3.2.41.3. Portas TCP e UDP de origem e destino;
 - 3.2.41.4. VLAN ID;
 - 3.2.41.5. Ethertype;
 - 3.2.41.6. IPFrag;

- 3.2.41.7. TTL;
- 3.2.41.8. TOS;
- 3.2.41.9. Protocol;
- 3.2.41.10. TCP Control Mask/Bits;
- 3.2.41.11. DSCP;
- 3.2.41.12. Versão do Protocolo IPv4 e IPv6;
- 3.2.41.13. Endereço IPv6 de origem/destino;
- 3.2.42. Deverá suportar a reescrita de endereços IPs ou MAC Address para proteger a confidencialidade dos endereços IP reais;
- 3.2.43. A solução deverá suportar, no mínimo, 35000 (trinta e cinco mil) filtros (regras);
- 3.2.44. Deverá permitir a inserção e remoção de novos filtros (regras) sem a necessidade de reiniciar o(s) equipamento(s), ou seja, a aplicação destes filtros (regras) deverá acontecer em tempo real;
- 3.2.45. Deve suportar overlapping de filtros (regras), ou seja, utilização conjunta de filtros de entrada (ingress) e filtros de saída (egress);
- 3.2.46. A solução deverá implementar funcionalidade Mesh/Cluster;
- 3.2.47. O Mesh/Cluster deverá permitir a configuração e gerenciamento de 2 (dois) ou mais agregadores como um único equipamento lógico. Não serão aceitas soluções em cascata para o atendimento desta funcionalidade;
- 3.2.48. A solução deverá suportar, no mínimo, 30 agregadores em modo Mesh/Cluster;
- 3.2.49. O Mesh/Cluster deverá permitir a configuração de todos os agregadores a partir de uma única interface WEB (HTTPS) e CLI;
- 3.2.50. A funcionalidade de Mesh/Cluster deverá suportar a criação de 1 (um) ou mais filtros (regras) que se utilizem de portas de Rede em um equipamento físico e direcionem este tráfego para portas de Ferramenta localizadas em outro equipamento físico, independentemente da quantidade de equipamentos entre estes equipamentos. Não serão aceitas soluções em cascata para o atendimento deste item;
- 3.2.51. A funcionalidade de Mesh/Cluster deve suportar arquitetura conhecida como Spine/Leaf, permitindo balanceamento do tráfego entre os Leafs e os Spines e adicionando redundância a solução em caso de falha de um dos equipamentos;
- 3.2.52. Deve suportar o conceito de FABRIC que permite a criação de filtros que se estendem por múltiplos agregadores ou mesh/clusters de agregadores;
- 3.2.53. Deve permitir a configuração de circuitos entre mesh/clusters de agregadores, permitindo que o tráfego recebido em um cluster seja entregue para uma ferramenta em outro cluster.

FUNCIONALIDADES INLINE

- 3.2.54. O equipamento deve implementar instalação sem necessidade de reconfiguração de roteadores e switches, quando utilizado no modo de operação Inline;
- 3.2.55. O equipamento deve implementar, de forma simultânea e em interfaces distintas, os modos:
- 3.2.56. TAP/SPAN (Cópia de Tráfego);

- 3.2.57. Inline (Tráfego de Produção);
- 3.2.58. A solução deverá ser capaz de configurar a sequência das ferramentas Inline (serial), quando possuir 2 (duas) ou mais ferramentas, pela qual os pacotes deverão ser encaminhados sequencialmente quando o agregador funcionar de forma Inline.
- 3.2.59. A solução deverá ser capaz de configurar um grupo de ferramentas Inline (paralelo), quando possuir 2 (duas) ou mais ferramentas, pela qual os pacotes deverão ser balanceados entre as ferramentas quando o agregador funcionar de forma Inline.
- 3.2.60. A solução deverá permitir a configuração conjunta das funcionalidades serial e paralelo, permitindo criar uma sequência serial de ferramentas que estão em paralelo;
- 3.2.61. A solução deverá permitir que ferramentas inline em modo standalone, serial e paralelo, possam ter a flexibilidade de receber somente o tráfego de interesse, sem impacto entre elas e sem a necessidade de solução de contorno físico. Por exemplo, a ferramenta 1 precisa receber todo o tráfego e a ferramenta 2 necessita receber apenas tráfego WEB, nesse tipo de cenário as ferramentas devem receber o tráfego desejado sem necessidade de arranjos físicos e sem impactar o tráfego da outra;
- 3.2.62. Implementar funcionalidade conhecida como Fail-Safe através do uso de bypass, que mesmo em caso de perda de energia, os links interceptados da rede continuem ativos, não gerando indisponibilidade de rede;
- 3.2.63. Não é permitido composição com bypass externo, este deve ser obrigatoriamente do mesmo fabricante do restante da solução não é permitido composição com bypass OEM ou de terceiros;
- 3.2.64. A solução deve suportar Heartbeat para monitoramento da saúde das ferramentas, quando utilizadas de forma Inline, permitindo detectar e remover somente a ferramenta que apresentar falha, sem causar impacto no fluxo de dados das outras ferramentas e no tráfego de rede;
- 3.2.65. A solução deve suportar Heartbeat Negativo, que permite utilizar um pacote específico para a geração do tráfego de checagem, no entanto, este pacote deve ser bloqueado pela ferramenta inline, não retornando novamente para a solução de NPB. Caso este pacote retorne a ferramenta inline será considerada com falha e deverá ser removida sem impacto na rede e nos fluxos de dados;
- 3.2.66. A solução, quando utilizada em modo Inline, deve permitir remover uma ou mais ferramentas da sequência do tráfego sem causar impacto no tráfego da rede. Esta funcionalidade tem como principal objetivo remover ferramentas para atualização e para fins de troubleshooting, sem causar interrupção de rede;
- 3.2.67. A solução deve permitir a alteração do modo de operação sem causar interrupção de rede da ferramenta inline para “simulação inline” sem causar interrupção de rede, de modo que a ferramenta entenda que está inline mas está recebendo apenas uma cópia dos dados que foram encaminhados para rede.

INTERFACES

- 3.2.68. A solução deverá suportar, no mínimo, 32 (trinta e duas) interfaces 1Gb;
- 3.2.69. A solução deverá suportar, no mínimo, 72 (setenta e duas) interfaces 10/25Gb;
- 3.2.70. A solução deverá implementar, no mínimo, 16 (dezesesseis) interfaces 1/10/25Gb SFP28. Devem ser fornecidas com, ao menos, 2 (dois) transceivers de 10Gb SFP+ LC MM e 6 (seis) transceivers de 1Gb 1000Base-TX;

- 3.2.71. Todas as licenças devem ser fornecidas com vigência e suporte por trinta e seis (36) meses;
- 3.2.72. Todas as portas físicas do equipamento fornecido deverão estar habilitadas e devidamente licenciadas para captura de pacotes, encontrando-se prontas para uso imediato em fábrica, independentemente de terem sido ou não explicitamente especificadas neste Termo de Referência, não sendo admitida qualquer forma de licenciamento parcial, expansão progressiva, ativação futura ou aquisição adicional de licenças.

FUNCIONALIDADES AVANÇADAS

- 3.2.73. Deverá implementar capacidade de processamento agregado de, no mínimo, 200 (duzentos) Gbps de throughput, específico para o processamento de Deduplicação, Corte de Pacotes, Mascaramento e Inserção de trailer;
- 3.2.74. Esta capacidade poderá ser alcançada através da adição de módulos ou licenças;
- 3.2.75. A solução não pode impor limites de tráfego processado por licença. Todos os recursos avançados de hardware devem entregar o total de throughput sem restrição artificial;
- 3.2.76. Deve implementar funcionalidade Tunnel, que permite encapsulamento e desencapsulamento de tráfego entre 2 (dois) equipamentos através de redes L3 (roteadas);
- 3.2.77. A funcionalidade de Tunnel deve implementar o encapsulamento e o desencapsulamento utilizando protocolo L2GRE ou similar, permitindo transportar o tráfego encapsulado através de diferentes redes L3;
- 3.2.78. Deve implementar o balanceamento de carga dos pacotes de encapsulamento IPv6 L2GRE;
- 3.2.79. A solução deverá implementar balanceamento entre diferentes túneis, permitindo utilizar duas ou mais ferramentas da mesma solução como destino para todo o tráfego encapsulado;
- 3.2.80. Deve implementar a funcionalidade Packet Trimming (Corte do Pacote), otimizando o tráfego que será encaminhado para as ferramentas reduzindo o tamanho do pacote;
- 3.2.81. A funcionalidade de Packet Trimming deve ser configurável para cortar o pacote das seguintes formas:
- 3.2.81.1. Corte, ou seja, definir se todos os pacotes de uma sessão, a partir de um número especificado, serão cortados;
- 3.2.81.2. Drop, ou seja, definir se todos os pacotes de uma sessão, a partir de um número especificado, serão eliminados;
- 3.2.82. Deve implementar a funcionalidade Packet Trimming (Corte do Pacote), otimizando o tráfego que será encaminhado para as ferramentas reduzindo o tamanho do pacote;
- 3.2.83. A funcionalidade de Packet Trimming deve ser configurável para cortar o pacote das seguintes formas:
- 3.2.83.1. Dinâmico, ou seja, a partir de um campo específico do cabeçalho ethernet definido pelo usuário;
- 3.2.83.2. Estático, ou seja, a partir de um offset específico definido pelo usuário;
- 3.2.84. Deve suportar terminação ERSPAN, permitindo terminar um tráfego espelhado de

equipamentos que suportam ERSPAN;

- 3.2.85. Deve suportar terminação ERSPAN para as versões II e III;
- 3.2.86. Deve implementar a funcionalidade Masking (Alteração de dados), que é capaz de modificar determinadas informações contidas no tráfego de rede antes de redirecioná-lo para as Ferramentas, para atendimento de normas PCI quando necessário;
- 3.2.87. A funcionalidade Masking deverá ser capaz de trocar uma determinada informação como o CPF do usuário por outros caracteres (XXX.XXX.XXX-XX, por exemplo), de modo que essa informação específica seja protegida antes de ser enviada para as soluções.
- 3.2.88. Deve suportar a funcionalidade Protocol Stripping (Remoção de Cabeçalho), permitindo identificar e remover TAGs de VLANs e cabeçalhos específicos dos pacotes de rede;
- 3.2.89. A funcionalidade de Protocol Stripping deve suportar a remoção de pelo menos os seguintes cabeçalhos:
 - 3.2.89.1. ERSPAN
 - 3.2.89.2. VLAN;
 - 3.2.89.3. MPLS;
 - 3.2.89.4. VNTag;
 - 3.2.89.5. VxLAN;
 - 3.2.89.6. Fabric Path;
 - 3.2.89.7. GRE;
 - 3.2.89.8. ISL;
 - 3.2.89.9. QinQ;
 - 3.2.89.10. GTP;
- 3.2.90. A funcionalidade de Protocol Stripping também deverá suportar a remoção de cabeçalhos que não estejam pré-definidos, permitindo assim a customização de um offset e quantidade de bytes deverão ser removidos, permitindo assim a remoção de cabeçalhos não padronizados;
- 3.2.91. Deve implementar a funcionalidade Packet De-Duplication (De-duplicação de Pacotes), enviando somente uma única cópia do pacote para as Ferramentas;
- 3.2.92. A funcionalidade de Packet De-Duplication deve suportar de-duplicação de pacotes IPv4, IPv6 e pacotes sem IP, devendo levar em consideração o Payload e os cabeçalhos ethernet;
- 3.2.93. A funcionalidade Packet De-Duplication deve detectar pacotes duplicados recebidos em diferentes portas ou módulos do(s) equipamento(s), inclusive se utilizado em modo Mesh/Cluster, detectando pacotes duplicados entre diferentes portas, módulos e equipamentos;
- 3.2.94. A funcionalidade Packet De-Duplication deve permitir habilitar ou desabilitar a inspeção de, no mínimo, os seguintes campos para avaliar se é um pacote duplicado ou não:

- 3.2.94.1. IPv4 ToS;
- 3.2.94.2. IPv6 TC;
- 3.2.94.3. Número da Sequência TCP;
- 3.2.94.4. VLAN ID;
- 3.2.95. A solução deverá implementar o recurso de inserção de trailer (etiquetagem de porta de origem) de modo a permitir a identificação inequívoca da origem da captura de cada pacote de tráfego;
- 3.2.96. Deverá implementar capacidade de processamento agregado de, no mínimo, 80 (Oitenta) Gbps de throughput, específico para o processamento de Filtragem de aplicação e Geração de Metadados Netflow v5, v9, ipfix e CEF(Syslog);
- 3.2.97. Esta capacidade poderá ser alcançada através da adição de módulos ou licenças;
- 3.2.98. A solução não pode impor limites de tráfego processado por licença. Todos os recursos avançados de hardware devem entregar o total de throughput sem restrição artificial;
- 3.2.99. Deve implementar a funcionalidade de geração de metadados de no mínimo NetFlow, IPFIX, JSON e CEF;
- 3.2.100. Deve implementar geração de NetFlow nas versões v5 e v9 e IPFIX;
- 3.2.101. A geração de NetFlow/IPFIX deve suportar os seguintes métodos de amostragem:
- 3.2.102. Unsampled (Sem amostragem);
 - 3.2.102.1. Deve gerar, no mínimo, os seguintes metadados Netflow v5, v9 e IPFIX, CEF e JSON para prover informações superiores à da camada de rede, quando utilizando no mínimo os protocolos:
 - 3.2.102.2. HTTP2; HTTP Response Code; HTTP Version; HTTP Host; HTTP User Agent;
 - 3.2.102.3. DNS Query Name; DNS Query Type; DNS Response Code; DNS Response TTL;
 - 3.2.102.4. DNS Response IPv6/IPv4; DNS Response Name;
 - 3.2.102.5. RDP Encryption Level; RDP Color_depth; RDP Connection_type;
 - 3.2.102.6. MYSQL Query; MYSQL Base;
 - 3.2.102.7. SSH User Agent; SSH Server Agent; SSH Version; SSH RTT;
 - 3.2.102.8. SMB Filename; SMB Filesize;
 - 3.2.102.9. MODBUS events; MODBUS fifo_count; MODBUS Erro_Code;
 - 3.2.102.10. KERBEROS Cname_Type; KERBEROS Err_Data; KERBEROS Err_Text;
- 3.2.103. Deve implementar a exportação de, no mínimo, cinco mil (5000) diferentes atributos da camada de aplicação para soluções analíticas como SIEM e plataformas de observabilidade;
- 3.2.104. Os metadados extraídos da camada de aplicação devem permitir a identificação de ações específicas de usuários tais como login e acessos em arquivos;
- 3.2.105. Deve implementar a funcionalidade DPA (Deep Packet Analysis), que permita criar filtros (regras) que identifiquem qualquer informação dentro do pacote, desde o

cabeçalho até o Payload;

- 3.2.106. A funcionalidade DPA deve permitir a criação de filtros (regras) utilizando linguagem de programação Perl ou RegEx;
- 3.2.107. A funcionalidade DPA deve permitir a criação de filtros (regras) utilizando uma string;
- 3.2.108. A funcionalidade DPA deve permitir a criação de filtros (regras) que façam "match" nos campos ethernet mesmo quando a informação estiver encapsulada por outros protocolos, como FCoE;
- 3.2.109. Deve implementar funcionalidade de Application Aware (App-Aware), que permite compreender uma sessão completa de um fluxo de dados e encaminhar/bloquear todos os pacotes subsequentes desta sessão para as Ferramentas;
- 3.2.110. A funcionalidade App-Aware deve implementar a utilização de buffer da sessão, permitindo armazenar, no mínimo, os 20 pacotes iniciais da sessão, para que nos casos em que o padrão da sessão for detectado após o handshake da sessão, todos os pacotes anteriores também sejam encaminhados para as Ferramentas;
- 3.2.111. Deve implementar a filtragem de tráfego com base na visibilidade da camada de aplicação, permitindo a identificação bidirecional do tráfego na camada 7 do modelo OSI através de funcionalidade de DPI (Deep Packet Inspection);
- 3.2.112. Deve implementar a identificação de, no mínimo, 3500 aplicações agrupadas por famílias ou grupos de aplicações tais como YouTube, Whatsapp e Gmail;
- 3.2.113. Deve implementar a definição de assinaturas para aplicações customizadas, incluindo protocolos e extensões proprietárias;
- 3.2.114. Após a identificação do tráfego com base na aplicação, a solução deve suportar a criação de filtros (regras) de encaminhamento e replicação de tráfego;

GERÊNCIA CENTRALIZADA

- 3.2.115. Deverá ser fornecido um software capaz de controlar, administrar, gerenciar e monitorar a solução de Visibilidade;
- 3.2.116. O software deverá estar licenciado para, no mínimo, 5 ativos físicos da solução de Visibilidade, e permitir upgrades através da aquisição de licença adicional;
- 3.2.117. Possuir gerenciador único em um único ponto central para orquestrar todo os elementos físicos, virtuais, em nuvem e containers que compõem o projeto. A solução deve permitir o gerenciamento de todos os componentes da solução, incluindo appliances físicos e virtuais, nuvem e containers;
- 3.2.118. A solução deve possuir uma interface gráfica e intuitiva com API abertas para simples customização de aplicações e integração com produtos de terceiros;
- 3.2.119. A solução deve implementar Automação com Ansible e uso de API REST;
- 3.2.120. O dispositivo pode ser fornecido em forma de servidor físico instalados, configurados e possuindo todos os softwares necessários para prover os requisitos técnicos especificados, inclusive o sistema operacional, sem qualquer ônus adicional;
- 3.2.121. O dispositivo também pode ser fornecido em forma de appliance virtual compatível com hypervisors VMware e Hyper-V;
- 3.2.122. No caso de servidores, a solução poderá adotar hardwares padrão de mercado, desde que atendam aos requisitos recomendados pela última versão do manual de instalação dos softwares utilizados, no momento da assinatura do contrato;

- 3.2.123. Para ambos os casos deverá possuir altura máxima de 1RU;
- 3.2.124. Todo hardware que compõe a solução deverá possuir alimentação elétrica de 110/240 V, 47 a 63 Hz, com chaveamento automático;
- 3.2.125. A solução deve ser capaz de visualizar e gerenciar os dados e métricas coletadas em múltiplos segmentos monitorados em uma única console (centralizada), permitindo desta forma integração, maior segurança, escalabilidade, robustez e disponibilidade da solução;
- 3.2.126. Possuir interface gráfica para a criação dos filtros (regras), onde é possível selecionar as portas de Rede e as portas de Ferramentas, independentemente do equipamento físico. Os filtros (regras) criados para estes tráfegos deverão ser aplicados através desta mesma interface Web (HTTPS), facilitando a operação e entendimento dos fluxos;
- 3.2.127. A solução deve possibilitar a configuração de diferentes perfis de administradores. Deve ser possível ainda criar usuários com perfil de administração e outros de apenas visualização;
- 3.2.128. Deve permitir gerar um token somente se você for um usuário autenticado e com base em seus privilégios de acesso a Gerência;
- 3.2.129. A solução deve permitir que os usuários façam “drill down” à partir de visões de alto nível, orientadas a serviços, até visões técnicas com dados detalhados, que auxiliem na análise da causa raiz do problema;
- 3.2.130. Deve permitir a criação de topologias da solução de Visibilidade para todos os equipamentos ativos e gerenciáveis;
- 3.2.131. Deve permitir a identificação do status das portas dos dispositivos up ou down, tecnologia e velocidade das portas;
- 3.2.132. A solução deve permitir o inventário detalhado de atributos dos ativos da solução, atendendo, no mínimo, números seriais, módulos instalados, status do equipamento e versão de software instalado;
- 3.2.133. A solução deve permitir o armazenamento das configurações dos dispositivos;
- 3.2.134. A ferramenta deve permitir o agendamento da função de armazenamento de configuração de determinados elementos da rede. O agendamento deve ter periodicidade mínima de um dia;
- 3.2.135. Deve permitir o upgrade do sistema operacional ou Boot Prom dos dispositivos, unitariamente e para um grupo de dispositivos, inclusive podendo agendar um dia e horário para que este upgrade aconteça automaticamente;
- 3.2.136. A ferramenta deve permitir a execução do reset dos dispositivos;
- 3.2.137. A ferramenta deve permitir restaurar a configuração armazenada. Deve ser possível ainda aplicar essa configuração em um equipamento em processo de substituição;
- 3.2.138. Deve permitir a instalação dos TAPs virtuais a partir da console de gerência;
- 3.2.139. Deve possuir integração via API com a VMWare, para permitir cópia do tráfego entre as VMs mesmo em caso de mobilidade das VMs;
- 3.2.140. A solução deverá ser capaz de criar e configurar os filtros (regras) virtuais, ou seja, os filtros (regras) que serão aplicados dentro da solução virtual para que seja espelhado para fora do servidor somente o tráfego desejado.

3.2.141. A solução deverá possuir dashboards com, no mínimo, as seguintes informações:

- 3.2.141.1. Total de portas que estão perdendo pacotes;
- 3.2.141.2. Total de portas acima do limite de utilização, tanto portas de Rede como portas de Ferramenta;
- 3.2.141.3. TOP portas com maior utilização;
- 3.2.141.4. Visualização simplificada de todos os filtros (regras) aplicados, indicando as portas de Redes e Ferramentas;

3.2.142. Requisitos de Logs:

- 3.2.142.1. A solução deve possuir ferramenta para acompanhamento e análise de eventos de logs;
- 3.2.142.2. Deve permitir a geração de log externo (syslog) para integração com soluções de SIEM;

3.2.143. A solução deverá gerar e armazenar trilhas de auditoria que permitam o rastreamento de ações efetuadas em todos os seus componentes. Os registros de logs devem conter a identificação do evento, data e hora, identificação do usuário, identificação do dispositivo e endereço IP do dispositivo ou permitir que estas informações sejam correlacionadas com o mecanismo de SIEM como por exemplo QRadar IBM e Splunk;

3.2.144. Deve apresentar dashboards de estatísticas de Inline SSL:

- 3.2.144.1. Novas conexões/handshakes por segundo;
- 3.2.144.2. Número de conexões concorrentes;
- 3.2.144.3. Totais sessões interceptadas;
- 3.2.144.4. Média de CPU;
- 3.2.144.5. Versão TLS Client/Server;
- 3.2.144.6. Média de decryption por engine;
- 3.2.144.7. Taxa de tráfego; e
- 3.2.144.8. Sessões descriptografadas.
- 3.2.144.9. Volume total (Bytes);
- 3.2.144.10. Throughput Client e Server (bps);
- 3.2.144.11. Distribuição dos Modos do SSL Outbound, Inbound e Não SSL;
- 3.2.144.12. Top 10 URLs e categorias acessadas pelo inline ssl;
- 3.2.144.13. Top 10 Cifras.

AGREGADOR DE PONTO DE CAPTURA – CARACTERÍSTICAS TÉCNICAS GERAIS

3.2.145. O equipamento agregador deve ser baseado em Appliance suportando montagem em rack (bastidor) de 19" (dezenove polegadas), com utilização de no mínimo 2-RU (dois unidades de bastidor) de altura, com fornecimento dos respectivos conjuntos de fixação;

3.2.146. A solução ofertada deverá possuir funcionalidades e hardware específicos para este propósito de agregação, regeneração, filtragem e modificação/transformação do tráfego, não sendo aceita soluções similares, como: Switches, Roteadores, Firewalls, Balanceadores, Servidores, soluções Híbridas etc.;

- 3.2.147. A solução deverá ser composta por único fabricante, incluindo os itens de Agregador, módulos e GBICs, com vista a não desperdício de recursos técnicos e facilidade de integração;
- 3.2.148. Deverá possibilitar a configuração dinâmica de portas por software, permitindo a definição de portas de “Rede”, “Rede Inline”, “híbrida”, “circuito”, “Ferramenta” e portas de “Ferramenta Inline”;
- 3.2.149. Entende-se por portas de Rede, todas as portas que serão responsáveis por receber a cópia do tráfego através dos TAPs/SPANs;
- 3.2.150. Entende-se por portas de Ferramenta, todas as portas que serão responsáveis por encaminhar o tráfego, seja ele já filtrado e/ou modificado, para as ferramentas que serão conectadas a solução de NPB;
- 3.2.151. Entende-se por portas de Rede Inline, todas as portas que serão responsáveis por se conectar de forma Inline a rede de produção;
- 3.2.152. Entende-se por portas de Ferramenta Inline, todas as portas que serão responsáveis por encaminhar o tráfego de produção, selecionado através dos filtros ou não, para as ferramentas Inline que serão conectadas a solução de NPB.

AGREGADOR DE PONTO DE CAPTURA – GERENCIAMENTO DO AGREGADOR:

- 3.2.153. A console de gerenciamento do agregador deve ser única e deve abranger todos os itens ativos e gerenciáveis da solução;
- 3.2.154. A solução deve possuir uma interface gráfica e intuitiva com API abertas para simples customização de aplicações e integração com produtos de terceiros;
- 3.2.155. Deverá permitir configuração customizada baseadas nos perfis de acesso (RBAC - Role Base Access Control);
- 3.2.156. Deverá implementar os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps;
- 3.2.157. Deverá possuir suporte a MIB II;
- 3.2.158. Deverá implementar a MIB privativa que forneça informações relativas ao funcionamento do equipamento;
- 3.2.159. Deverá suportar SNMP trap sobre IPv6;
- 3.2.160. Deverá permitir a atualização remota do sistema operacional e arquivos de configuração utilizados no equipamento via interface de gerenciamento;
- 3.2.161. Deverá permitir a gravação de log externo (syslog);
- 3.2.162. Deverá permitir o armazenamento de sua configuração em memória não volátil, podendo, numa queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior à queda de alimentação;
- 3.2.163. Deverá possuir ferramentas para depuração e gerenciamento em primeiro nível, tais como estatísticas de utilização e log de eventos;
- 3.2.164. Deve possuir gerenciamento através de interface Web (HTTPS) e CLI;
- 3.2.165. Deverá implementar o protocolo NTP (Network Time Protocol);
- 3.2.166. Deverá implementar mecanismo de autenticação para acesso local ou remoto ao equipamento baseada em um Servidor de Autenticação/Autorização do tipo TACACS/TACACS+, RADIUS e LDAP;

- 3.2.167. Deve suportar IPv6 para TACACS+;
- 3.2.168. Deverá implementar o protocolo SSHv2 para acesso à interface de linha de comando;
- 3.2.169. Deverá proteger a interface de comando do equipamento através de senha;
- 3.2.170. Deverão ser fornecidos, no mínimo, Agregadores de Tráfego com as seguintes quantidades de interfaces:
- 3.2.170.1. Suportar no mínimo sessenta e quatro (64) portas de 40/100Gbps compatíveis com os padrões QSFP+/QSFP28;
 - 3.2.170.2. Suportar no mínimo cento e vinte e oito (128) portas de 10/125Gbps compatíveis com os padrões SFP+/SFP28;
 - 3.2.170.3. Deverão ser fornecidos 4 (quatro) transceivers QSFP28 100G SR4 MPO12 MM multimodo, 18 (dezoito) transceivers QSFP+ 40G SR4 MPO12 MM multimodo, 20 (vinte) transceivers QSFP+ 40G SWDM4 LC MM multimodo, 20 (dois) transceivers SFP+ 10G LC multimodo e 6 (seis) transceivers UTP RJ45 1Gb;
- 3.2.171. O equipamento deverá possuir a capacidade de processamento de, no mínimo, 6.3Tbps (Seis ponto três) Tbps de tráfego agregado para aplicação dos filtros (regras) descritos nesta especificação;
- 3.2.172. O equipamento deve estar em conformidade com o padrão RoHS;
- 3.2.173. Deverá possuir módulos de ventilação hot swappable;
- 3.2.174. Possuir ventilação "front-to-back", ou seja, a saída de ar quente deve acontecer pela traseira do equipamento;
- 3.2.175. Deverá possuir fonte de alimentação interna que trabalhe em 100V-240V, 50/60 Hz, com detecção automática de tensão e frequência, hot-swappable;
- 3.2.176. Deverá possuir fonte de alimentação AC redundante interna, hot-swappable;
- 3.2.177. Deverá realizar automaticamente o deploy do Network Packet Broker com o mínimo de intervenção do usuário, mediante utilização de ZTP (Zero Touch Provisioning), assegurando que após reset de fábrica ou instalação inicial o dispositivo se auto configure por meio de arquivo previamente definido;
- 3.2.178. Deverá suportar simultaneamente em sua memória Flash (ou semelhante), duas imagens do sistema operacional entregue com o equipamento;
- 3.2.179. São apresentadas, a seguir, as especificações técnicas mínimas a serem ofertadas referentes ao objeto. Os termos "possuir", "permite/permitir", "implementar" e "é" implicam no fornecimento de todos os elementos necessários à adoção da tecnologia ou funcionalidade citada. O termo "ou" implica que a especificação técnica mínima dos serviços pode ser atendida por somente uma das opções. O termo "e" implica que a especificação técnica mínima dos serviços deve ser atendida englobando todas as opções;
- 3.2.180. A solução é definida como um Network Packet Broker, ou seja, realiza características de um broker a nível de pacotes de rede. Uma solução específica caracterizada como SSL Decryption ou com funcionalidade de SSL Inspection realiza apenas uma das múltiplas funções de um Network Packet Broker. Desta forma, não serão aceitas soluções como Firewalls UTM, Next-Generation Firewall (NGFW), Load Balancers com funcionalidade de SSL Offloading, e tais atestados não serão considerados como válidos;

- 3.2.181. Os Agregadores de Tráfego devem ser fornecidos com as licenças necessárias para ativação de todas as suas portas disponíveis simultâneas;
- 3.2.182. Os Agregadores de Tráfego devem ser interligados com o Concentrador de Tráfego que implementará as funcionalidades avançadas através de conexões físicas dedicadas;
- 3.2.183. A interligação entre os Agregadores de Tráfego e o Concentrador de Tráfego deverá ser feita através de conexões de 100Gbps;

MÓDULO DE CAPTURA DE TRÁFEGO EM AMBIENTE VIRTUAL

- 3.2.184. O módulo deve ser capaz de implementar a coleta de tráfego dentro do mundo virtual (tráfego entre VMs) através de virtual TAPs;
- 3.2.185. Deverá se integrar, através de APIs específicas, com a VMware, Nutanix ou OpenStack, não sendo aceita soluções que utilizem do modo promíscuo ou que faça qualquer alteração no kernel do Hypervisor, para todas as plataformas solicitadas;
- 3.2.186. Para a coleta de tráfego entre VMs deverá ser compatível com, no mínimo, as seguintes plataformas:
- 3.2.186.1. VMware 7 ou superior;
 - 3.2.186.2. NSX-T 3.1.0 ou superior;
 - 3.2.186.3. OpenStack;
- 3.2.187. Deverá possuir recurso de monitoração de vMotion e DRS (VMware Distributed Resource Scheduler);
- 3.2.188. Deverá implementar o monitoramento de múltiplos VMware vDS (VMware virtual distributed switches) simultaneamente;
- 3.2.189. A solução deverá capturar o tráfego em modo inline, sem agentes, nos ambientes de nuvem pública Azure e AWS, garantindo também as funcionalidades de deduplicação de tráfego, filtragem seletiva e corte de pacotes;
- 3.2.190. Deverá se integrar, através de APIs específicas, com a Azure, AWS e Google Cloud.
- 3.2.191. Para a coleta de tráfego deverá ser compatível com, no mínimo, as seguintes plataformas:
- 3.2.191.1. AWS EKS
 - 3.2.191.2. Azure AKS;
 - 3.2.191.3. GCP GKE;
 - 3.2.191.4. VMware Tanzu;
 - 3.2.191.5. Openshift;
- 3.2.192. Deverá implementar a identificação automática das VMs que devem ser monitoradas através das definições de regras de seleção do tráfego que deve ser monitorado, evitando que cada VM tenha que ser selecionada individualmente para monitoramento;
- 3.2.193. Deverá suportar a mobilidade das máquinas virtuais, de forma que quando ocorrer uma migração de uma VM, todas as políticas relacionadas a esta VM continuem sendo aplicadas sem a necessidade de reconfiguração manual;
- 3.2.194. Deve implementar a coleta de tráfego entre VMs de, no mínimo, 1000 hypervisors e

integração com, no mínimo, 10 vCenters e 3200 Máquinas virtuais;

- 3.2.195. Deve ser implementado um Virtual Broker em cada hypervisor. Cada Virtual Broker deve possuir a capacidade de executar a funcionalidade de deduplicação de tráfego (de-duplication), bem como realizar o balanceamento de carga entre, no mínimo, dois Virtual Brokers por hypervisor;
- 3.2.196. Deverá processar, no mínimo, 50 TB de dados por dia;
- 3.2.197. Deve implementar a funcionalidade de desencapsulamento de cabeçalhos L2GRE e VXLAN dos pacotes de rede;
- 3.2.198. Deve implementar a funcionalidade de encapsulamento dos pacotes de rede com o protocolo L2GRE ou VXLAN, permitindo o envio de tráfego tunelado para as ferramentas de monitoramento, nativamente no ambiente virtual;
- 3.2.199. Deve suportar a funcionalidade Packet De-Duplication (Desduplicação de Pacotes), enviando somente uma única cópia do pacote para as Ferramentas de monitoramento, nativamente no ambiente virtual;
- 3.2.200. Deve suportar a geração de flow sem amostragem, trazendo visibilidade de 100% do tráfego;
- 3.2.201. Deve ser capaz de enriquecer as informações de NetFlow com dados contextuais da camada de aplicação;
- 3.2.202. Deve permitir a extração de metadados do tráfego para mais de 3000 aplicações diferentes;
- 3.2.203. Deve extrair até 5000 atributos das diferentes aplicações;
- 3.2.204. Deverá suportar o recebimento de telemetria nos formatos NetFlow v5, v9 e IPFIX, provenientes de fontes externas;
- 3.2.205. Deverá, ainda, exportar esses registros em formato JSON ou encaminhá-los via Kafka;
- 3.2.206. Deve suportar o recebimento de NetFlow/IPFIX e envio no formato JSON;
- 3.2.207. Deve permitir o envio de metadados dados para até quatro coletores diferentes;
- 3.2.208. Deve possibilitar a atualização (upgrade) de versão dos agentes de captura virtual, de forma automática e centralizada, por meio do console de gerenciamento centralizada, sem a necessidade de intervenção manual em cada agente individual;
- 3.2.209. Deve suportar a deciptação passiva (out-of-band) do tráfego TLS;
- 3.2.210. Deve suportar o envio de dados em diferentes formatos, tais como no mínimo, IPFIX, CEF e JSON;
- 3.2.211. A solução deve suportar a captura de tráfego em ambientes virtuais, containers e nuvem. Deve suportar a captura de pacotes antes da criptografia e após a deciptação, no mínimo para os seguintes sistemas operacionais e ambientes de containerização:
 - 3.2.211.1. Sistemas Linux baseados em Debian;
 - 3.2.211.2. Sistemas Linux baseados em Redhat;
 - 3.2.211.3. Ambientes de containerização:
 - AKS;
 - EKS;
 - Openshift;

- Kubernetes.

- 3.2.212. Deve suportar a abertura das seguintes variações de criptografias do TLS, 1.2 com PFS (Perfect Forward Secrecy), 1.3 e mTLS;
- 3.2.213. A funcionalidade deve ser independente de upgrades do S.O;
- 3.2.214. Deve suportar IPv4 e IPv6;
- 3.2.215. Deve suportar OpenSSL version 1.0.2, 1.1.0, 1.1.1 e 3.x;
- 3.2.216. Deve gerar, no mínimo, os seguintes metadados para prover informações superiores à da camada de rede da AWS, Azure, VMware vCenter e Kubernetes, quando utilizando no mínimo os protocolos:
- 3.2.216.1. aws_instance_id;aws_subnet_id;aws_security_group_name;aws_iam_instance_profile_arn;aws_tags;
- 3.2.216.2. azure_subscription_id;azure_resource_group;azure_vnet_id;azure_location;azure_network_if_attach_id;
- 3.2.216.3. vmware_vm_name;vmware_vm_network;vmware_vm_os_distro_name;vmware_datacenter_name; vmware_cluster_name;
- 3.2.216.4. k8s_cluster_name; k8s_node_name; k8s_node_status; k8s_service_name; k8s_container_name;

MÓDULO DE CAPTURA DE TRÁFEGO TIPO 1 – CARACTERÍSTICAS TÉCNICAS ESPECÍFICAS

- 3.2.217. Deve ser tipo chassis para TAP de Fibra (Hardware);
- 3.2.218. Deverá ser do mesmo fabricante dos demais itens.
- 3.2.219. Deverão ser fornecidos 3(três) unidades de chassis, com suporte a, no mínimo, 6 (seis) TAPs de fibra com conectores LC ou MPO, específicas para interligação dos enlaces de rede.
- 3.2.220. O chassis deverá possuir os seguintes requisitos técnicos:
- 3.2.221. Deve ser composto por um único equipamento, montável em rack 19" devendo este vir acompanhado dos devidos acessórios para tal. O equipamento deverá ser do tipo chassis/modular.
- 3.2.222. Deve possuir altura máxima de 1 RU (1,75");
- 3.2.223. Operar em temperaturas de 0°C a 60°C e umidade relativa de 10% a 85%;
- 3.2.224. Deve ser totalmente passivo, ou seja, não é necessário nenhum tipo de alimentação elétrica, software e configuração para o seu funcionamento.

MODULO DE CAPTURA DE TRÁFEGO TIPO 2 – CARACTERÍSTICAS TÉCNICAS ESPECÍFICAS

- 3.2.225. Deve ser tipo TAP para links de Fibra Multimodo 1/10/25/40/100Gbps;
- 3.2.226. Deverá ser compatível com o Chassis para TAP de Fibra;
- 3.2.227. Deverão ser fornecidos, no mínimo, 7 (sete) módulos de captura de tráfego tipo 2;
- 3.2.228. Cada unidade TAP tipo 2 deverá possuir as seguintes características de interfaces, fibras, conectores e Split Ratio:
- 3.2.228.1. Possuir 2 (duas) interfaces de rede, responsável por conectar os dispositivos de rede;

- 3.2.228.2. Possuir 2 (duas) interfaces de monitoramento, responsável por enviar todo o tráfego TX, coletado nas interfaces de rede, em uma interface de monitoramento e todo o tráfego RX, coletado nas interfaces de rede, na outra interface de monitoramento;
- 3.2.229. Deverá ser fornecido com capacidade de suportar, no mínimo, 06 Links com a seguinte especificação: Multimodo 850nm, 50 microns, 1/10G com conector LC e split ratio de 50/50.

INSTALAÇÃO E CONFIGURAÇÃO DO MÓDULO DE OBSERVABILIDADE E PRIVACIDADE E MÓDULOS

- 3.2.230. Os serviços de instalação física, configuração e documentação, deverão ser executados por equipe técnica da CONTRATADA;
- 3.2.231. O(s) profissional(is) técnico(s) da CONTRATADA responsável(is) pelos serviços descritos neste ITEM deve(m) possuir os certificados dos fabricantes das soluções respectivas;
- 3.2.232. A implantação deverá contemplar as seguintes fases:
- 3.2.232.1. **Planejamento:** nesta etapa a Contratada deverá realizar o planejamento do projeto, onde serão definidos os prazos por atividade, as pessoas, a estratégia de implantação do serviço, o plano de testes, a localização dos equipamentos na arquitetura da rede do órgão, bem como quaisquer outros itens que sejam necessários para a implantação do projeto. Devem-se considerar as janelas de manutenção do órgão, plano de rollback e o escopo definido. Os responsáveis técnicos do órgão acompanharão e aprovarão o planejamento com o macro cronograma do projeto e principais marcos.
- 3.2.232.2. **Documentação do projeto:** Deverá ser entregue a documentação do projeto, conforme descrita a seguir, em formato e quantidade a serem acordados entre as partes e nos momentos especificados.
- 3.2.232.3. **Plano de Requisitos de Infraestrutura:** A CONTRATADA, antes de iniciar a execução das instalações deve levantar as necessidades de infraestrutura necessárias para instalação da configuração (espaço em rack, energização, refrigeração, tipo de conectorização, entre outros).
- 3.2.232.4. **Plano de Implementação:** A CONTRATADA, antes de iniciar a execução das configurações, deverá elaborar uma documentação técnica fundamentando todas as configurações que serão realizadas.
- 3.2.232.5. **Plano de Migração:** A CONTRATADA, antes de iniciar a execução das configurações, deverá analisar o ambiente do órgão para avaliar como será realizada a integração e a migração do ambiente atual de Produção.
- 3.2.233. Após a aprovação do planejamento deverá ser iniciado o processo de implantação, levando-se em consideração a disponibilidade das equipes envolvidas e cumprimento dos prazos pactuado, contemplando:
- 3.2.233.1. Instalação física dos equipamentos
- 3.2.233.2. Configuração
- 3.2.233.3. Instalação em ambiente
- 3.2.233.4. Etapa de testes e de funcionamento experimental

- 3.2.233.5. Migração
- 3.2.233.6. Validação do funcionamento em ambiente de produção
- 3.2.233.7. Documentação Final

3.3. ITENS 5 - TREINAMENTO

- 3.3.1. Este item trata da capacitação técnica da equipe da IPLANRIO, no uso das soluções contratadas;
- 3.3.2. Caberá a CONTRATADA fornecer, no mínimo, 4 (quatro) vouchers para repasse de conhecimento da Solução equivalentes a pelo menos 6 horas de curso (tempo de treinamento do Voucher) que poderão ser realizadas no formato presencial ou online na plataforma instalada;
- 3.3.3. Os Vouchers para a capacitação deverão possuir validade mínima de 1(um) ano contados a partir da emissão do empenho e assinatura do contrato;
- 3.3.4. Os treinamentos devem ser oficiais do fabricante, abordando o conhecimento dos componentes de software e hardware da solução contratada;

4. ITENS 6 - DO SUPORTE TÉCNICO

- 4.1.1. 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;
- 4.1.2. Disponibilizar técnico especializado na solução ofertada no regime de 24 horas por 7 dia, durante o período de vigência do contrato, para garantir o perfeito funcionamento da solução;
- 4.1.3. Os serviços contratados poderão ser executados após o expediente, em finais de semana ou feriados, a critério da CONTRATANTE;
- 4.1.4. O suporte técnico da CONTRATANTE deverá ser prestado para cada componente da solução adquirida e será acionada em caso de qualquer indisponibilidade da solução.
- 4.1.5. Os serviços de manutenção preventiva e corretiva deverão ser executados no ambiente da CONTRATANTE;
- 4.1.6. As manutenções serão solicitadas através de chamado ou por notificação automática de detecção de alarme, inoperância, falhas que possam ocasionar a indisponibilidade do serviço;
- 4.1.7. Deverá implantar novas versões, aplicar patches de atualização, documentar e prestar suporte técnico especializado durante a vigência do contrato;
- 4.1.8. Toda atividade executada pela CONTRATADA deverá ser entregue documentação ao responsável técnico da CONTRATANTE, em até 72 horas, após a demanda para aceite;
- 4.1.9. Responder, formalmente, dentro de 03 (três) dias úteis, a todas as correspondências emitidas pela CONTRATANTE, prestando todos os esclarecimentos solicitados;
- 4.1.10. 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;

- 4.1.11. 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. 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);
- 4.1.12. 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;
- 4.1.13. Todos os chamados com referência aos componentes, deverão seguir as seguintes premissas:
- 4.1.13.1. 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;
- 4.1.13.2. 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;
- 4.1.13.3. 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.
- 4.1.14. Fica estabelecido o seguinte Acordo de Nível de Serviço (SLA) para a prestação de suporte técnico especializado.

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

- 4.1.15. 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;
- 4.1.16. 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;

4.1.17. 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;

4.1.18. A CONTRATADA deverá participar ativamente das possíveis atualizações/migrações de novas versões da solução oferecida, ou mesmo do reposicionamento destas, sempre que demandada pela CONTRATANTE, seguindo plano de ações que possua, pelo menos, as fases descritas abaixo:

- I. Levantamento;
- II. Planejamento;
- III. Homologação;
- IV. Execução;
- V. Operação assistida;
- VI. Conclusão;

4.1.19. 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.

5. DO FORNECIMENTO

- 5.1. Os equipamentos, softwares e licenças deverão ser entregues no IPLANRIO, no endereço da R. Afonso Cavalcanti 455 – Anexo – Sala 307 – Cidade Nova – Rio de Janeiro – RJ - CEP 20211-110, em até 60 (sessenta) dias úteis contados da data da assinatura do contrato, em parcela única, conforme cronograma de execução física e financeira.
- 5.2. Todos os acessórios necessários à instalação dos produtos, incluindo kit tipo trilho para adaptação, cabos de alimentação, suportes, gavetas e braços, se necessário;
- 5.3. Os itens deverão ser entregues novos, sem uso, lacrados, sem avarias, acompanhados de suas notas fiscais e documentos legais necessários.

6. DA FUNDAMENTAÇÃO LEGAL DA CONTRATAÇÃO

A presente contratação tem fundamento na Lei Federal nº 13.303/2016, no Decreto Municipal nº 44.698/2018 e no Regulamento Interno de Licitações e Contratos da IPLANRIO – RILC IPLANRIO, disponível no Portal da Prefeitura do Rio de Janeiro: <https://IPLANRIO.prefeitura.rio/contratos-e-licitacoes/>. Subsidiariamente, no que for cabível, aplica-se as disposições atinentes ao pregão eletrônico previstas na Lei Federal nº 14.133/2021.

7. DA QUALIFICAÇÃO TÉCNICA

- 7.1. 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.
- 7.2. Considera-se compatível com o objeto da licitação o fornecimento de no mínimo 50% do constante na tabela 1 deste Termo de Referência e especificações de quantidades descritas neste Termo de Referência
- 7.3. Será admitida a soma dos atestados ou certidões apresentados pelas licitantes, desde que os mesmos sejam tecnicamente pertinentes e compatíveis em características, quantidades e prazos com o objeto da licitação.

8. DAS OBRIGAÇÕES DA CONTRATANTE

- 8.1. Realizar os pagamentos na forma e condições previstas;
- 8.2. Realizar a fiscalização do objeto deste Termo de Referência.

9. DAS OBRIGAÇÕES DA CONTRATADA

- 9.1. Realizar os serviços de acordo com todas as exigências contidas no Termo de Referência e na proposta;
- 9.2. Tomar as medidas preventivas necessárias para evitar danos a terceiros, em consequência da execução dos serviços;
- 9.3. Responsabilizar-se integralmente pelo ressarcimento de quaisquer danos e prejuízos, de qualquer natureza, que causar à CONTRATANTE ou a terceiros, decorrentes da execução do objeto desta contratação, respondendo por si, seus empregados, prepostos e sucessores, independentemente das medidas preventivas adotadas e da comprovação de sua culpa ou dolo na execução do contrato;
- 9.4. Atender às determinações e exigências formuladas pela CONTRATANTE;
- 9.5. Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, o objeto do contrato em que se verificarem vícios, efeitos ou incorreções resultantes da execução ou de materiais empregados, no prazo determinado pela Fiscalização;
- 9.6. Responsabilizar-se, na forma do Contrato, por todos os ônus, encargos e obrigações comerciais, sociais, tributárias, trabalhistas e previdenciárias, ou quaisquer outras previstas na legislação em vigor, bem como por todos os gastos e encargos com material e mão de obra necessária à completa execução dos serviços:
 - a) em caso de ajuizamento de ações trabalhistas contra a CONTRATADA, decorrentes da execução do presente Contrato, com a inclusão do Município do Rio de Janeiro ou da CONTRATANTE como responsável subsidiário ou solidário, a CONTRATANTE poderá reter, das parcelas vincendas, o montante dos valores cobrados, que serão complementados a qualquer tempo com nova retenção em caso de insuficiência;
 - b) no caso da existência de débitos tributários ou previdenciários, decorrentes da execução do presente Contrato, que possam ensejar responsabilidade subsidiária ou solidária da

CONTRATANTE, as parcelas vincendas poderão ser retidas até o montante dos valores cobrados, que serão complementados a qualquer tempo com nova retenção em caso de insuficiência;

- c) as retenções previstas nas alíneas “a” e “b” poderão ser realizadas tão logo tenha ciência o Município do Rio de Janeiro ou a CONTRATANTE da existência de ação trabalhista ou de débitos tributários e previdenciários e serão destinadas ao pagamento das respectivas obrigações caso o Município do Rio de Janeiro ou entidade da Administração Pública indireta sejam compelidos a tanto, administrativa ou judicialmente, não cabendo, em nenhuma hipótese, ressarcimento à CONTRATADA;
- d) eventuais retenções previstas nas alíneas “a” e “b” somente serão liberadas pela CONTRATANTE se houver justa causa devidamente fundamentada.

- 9.7. Manter as condições de habilitação e qualificação exigidas para a contratação durante todo prazo de execução contratual;
- 9.8. Responsabilizar-se, na forma do Contrato, pela qualidade dos serviços executados e dos materiais empregados, em conformidade com as especificações do Termo de Referência, com as normas da Associação Brasileira de Normas Técnicas – ABNT, e demais normas técnicas pertinentes, a ser atestada pelos responsáveis pela fiscalização da execução do contrato, assim como pelo refazimento do serviço e a substituição dos materiais recusados, sem ônus para o(a) CONTRATANTE e sem prejuízo da aplicação das sanções cabíveis;
- 9.9. Responsabilizar-se inteira e exclusivamente pelo uso regular de marcas, patentes, registros, processos e licenças relativas à execução desta contratação, eximindo a CONTRATANTE das consequências de qualquer utilização indevida;
- 9.10. Indicar, nas notas fiscais emitidas, quando o objeto envolver prestação de serviços, o efetivo período do mês que está sendo faturado.
- 9.11. Entregar os bens de acordo com todas as exigências contidas no Termo de Referência;

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

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.

11. DOS PRAZOS

- 11.1. O prazo de vigência da contratação será de 24 (vinte e quatro) meses, contados a partir da assinatura do contrato, podendo ser prorrogado nos termos da legislação em vigor.
- 11.2. O prazo de entrega do (s) material (is)/equipamento (s) será de até 60 (sessenta) dias úteis, a contar da data de assinatura do contrato, podendo ser prorrogado a critério da CONTRATANTE.
- 11.3. O prazo de instalação e configuração da solução será de até 30 (trinta) dias úteis, a contar da data da entrega do (s) material (is)/equipamento (s), podendo ser prorrogado

a critério da CONTRATANTE.

12. DA GARANTIA CONTRATUAL

- 12.1. 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.
- 12.2. 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.
- 12.3. 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.
- 12.4. 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.
- 12.5. 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.
- 12.6. 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.
- 12.7. 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.
- 12.8. 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.

13. DA FISCALIZAÇÃO E ACEITE DO OBJETO

- 13.1. 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.

- 13.2. 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.
- 13.3. 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.
- 13.4. 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.
- 13.5. 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.
- 13.6. 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.
- 13.7. A aceitação definitiva 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.
- 13.8. O objeto do presente Termo de Referência será recebido em tantas parcelas quantas forem às relativas ao pagamento.
- 13.9. 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 anotará 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.
- 13.10. 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.

- 13.11. 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.

14. DAS CONDIÇÕES DE PAGAMENTO

- 14.1. O pagamento dos itens 1 a 4 da tabela 1, serão efetuados de forma dividida em 70% no exercício de 2026 e 30% no exercício de 2027, integralmente de acordo com os percentuais citados anteriormente 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 IPLANRIO 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.
- 14.2. 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.
- 14.3. Em relação ao item 6 da tabela 1, 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 contidas no RLC IPLANRIO 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.
- 14.4. O pagamento do item 5 da tabela 1 será efetuado à CONTRATADA em 01 (uma única) parcela à vista, após ateste dos treinamentos e 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 IPLANRIO 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.
- a) O ateste dos treinamentos será emitido em até 05 (cinco) dias úteis após a entrega dos serviços.
- 14.5. 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.
- 14.6. 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.
- 14.7. 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.

- 14.8. 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.
- 14.9. 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.
- 14.10. O pagamento será efetuado à CONTRATADA através de crédito em conta bancária do fornecedor cadastrado junto à Coordenação do Tesouro Municipal.

15. DAS SANÇÕES ADMINISTRATIVAS

- 15.1. Pelo descumprimento total ou parcial da Ata de Registro de Preços ou do Contrato, o Órgão Gerenciador e os (as) CONTRATANTES, respectivamente, poderão, sem prejuízo responsabilidade civil e criminal que couber, aplicar as seguintes sanções, previstas nos artigos 7º da Lei Federal nº 10.520/02 no art. 589 do RGCAF e Regulamento de Licitações e Contratos da Contratante, garantida a defesa prévia ao contratado:

I - advertência;

II - Multa de mora de até 1% (um por cento) por dia útil sobre o valor do Contrato ou do saldo não atendido do Contrato;

III - 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;

IV - suspensão temporária do direito de licitar e impedimento de contratar com a Administração Municipal;

- 15.2. A multa aplicada será depositada em conta bancária indicada pela IplanRio, descontada dos pagamentos eventualmente devidos, descontada da garantia ou cobrada judicialmente.
- 15.3. As sanções previstas nos incisos I e IV do subitem 15.1 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;
- 15.4. Do ato que aplicar a pena prevista no inciso IV do subitem 15.1, a autoridade competente no âmbito da CONTRATANTE dará conhecimento aos demais órgãos e entidades municipais interessados, na página oficial desta empresa pública na internet.
- 15.5. A sanção prevista no inciso IV do subitem 15.1 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 IplanRio em virtude de atos ilícitos praticados.

- 15.6. As multas previstas nos incisos II e III do subitem 15.1 não possuem caráter compensatório, e, assim, o pagamento delas não eximirá a CONTRATADA de responsabilidade pelas perdas e danos decorrentes das infrações cometidas.
- 15.7. As multas aplicadas poderão ser compensadas com valores devidos à CONTRATADA mediante requerimento expresso nesse sentido.
- 15.8. 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.

16. DA MATRIZ DE RISCOS

- 16.1. 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.
- 16.2. É vedada a celebração de aditivos decorrentes de eventos supervenientes alocados na Matriz de Riscos como sendo de responsabilidade da CONTRATADA.
- 16.3. Sempre que atendidas as condições do contrato e mantidas as disposições da Matriz de Risco, considera-se mantido o equilíbrio econômico-financeiro.
- 16.4. A proposta comercial deverá ser elaborada levando em consideração a natureza e a extensão dos riscos relacionados na Matriz de Risco.

16. DA RETIRADA E DESTINAÇÃO DE BENS DE INFORMÁTICA

Os equipamentos substituídos ou considerados inservíveis deverão ser retirados no prazo de 30 (trinta) dias, contado da notificação pela CONTRATANTE, com comprovação da destinação ambientalmente adequada no prazo de 45 (quarenta e cinco) dias, nos termos do Decreto Rio n.º 48.161/2020.

A comprovação da destinação ambientalmente adequada deverá ser feita por meio de certificado de reciclagem ou de destruição, emitido por entidade credenciada, acompanhado de nota fiscal correspondente. O não cumprimento desta obrigação acarretará as sanções administrativas previstas neste Termo de Referência.

17. DA PROPOSTA DE PREÇOS

- 17.1. 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.
- 17.2. 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.

18. DO TIPO DE LICITAÇÃO

- 18.1. O tipo de licitação será o menor preço global, tendo em vista a natureza integrada e indivisível da solução, conforme justificativa técnica constante do item 'Justificativa para o parcelamento ou não da contratação' do Estudo Técnico Preliminar (ETP), que demonstra a necessidade de fornecimento por ecossistema único, com gerenciamento centralizado e garantia unificada.

19. DA PROTEÇÃO DE DADOS PESSOAIS

- 19.1. 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, 23 de julho de 2026.

Documento assinado digitalmente
 LEONARDO CEZAR CAVALIERI DOS SANTOS
Data: 25/10/2026 15:57:34-0300
Verifique em <https://validar.iti.gov.br>

Leonardo Cavalieri
Matrícula: 40/622.627-9
Gerente de Segurança Cibernética
IPLANRIO/DOP

Aprovação

Jorge Francisco Antunes da Silva
Matrícula: 40/2622163-4
Diretor de Operações
IPLANRIO

ANEXO I – Matriz de Risco

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	Organizacio nal	Aquisição	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	Organizacio nal	Aquisição	7	9	63	Mitigar	A contratada deverá manter fluxo de caixa para cobrir o período descoberto	Contratada
R004	Ameaça	Devido a alteração da política econômico-financeira, pode haver aumento nos tributos após a contratação	Organizacio nal	Aquisição	4	5	20	Aceitar Ativamente	A contratada deverá buscar alternativas para cumprimento do contrato	Contratada
R005	Ameaça	Monitoramento do ambiente, devido à ausência de mão de obra qualificada e operação 24horas por 7 dias	Organizacio nal	Aquisição	9	9	81	Mitigar	Ampliar quadro técnico e capacitar para grupo de trabalho com foco exclusivo na monitoração com regime 24hx7d	Contratante
R006	Ameaça	Devido ao atraso de pagamento do contrato, a equipe da contratada poderá levar ao atraso no atendimento do serviço	Organizacio nal	Aquisição	7	8	56	Mitigar	Deverá manter fluxo de caixa para cobrir o período descoberto	Contratada