PROJETO BÁSICO DA NOVA REDE MACEIÓ

LINK DE TRÁFEGO IP PARA INTERNET COM SUPORTE A BGP, SOLUÇÃO DE SEGURANÇA INTEGRADA E REDUNDÂNCIA DE LINK

PREFEITURA DA CIDADE DE MACEIÓ

Sumário

1. APRESENTAÇÃO DO PROJETO NOVA REDE MACEIÓ

1.1. O projeto Intitulado “Nova Rede MACEIÓ” trata da estruturação da rede de Dados e telecomunicações da Prefeitura Municipal de Maceió, com a integração e melhoria dos serviços de VOIP, TELEFONIA FIXA, TELEFONIA MÓVEL, REDE DE DADOS e seus serviços auxiliares. A necessidade de implantação de uma rede convergente e multiplataforma é um desafio para a construção de estruturas que forneçam uma melhor prestação de serviço para a comunidade, além de disponibilizar um ambiente de trabalho mais eficiente para os servidores.

1.2. A informatização cada vez maior e a necessidade de trocas de dados e informações mais eficientes são tratadas como prioritário, para que a prestação de serviço público eleve seu padrão de qualidade e os seus usuários possam perceber suas melhorias, com o aumento do fornecimento de serviços on-line, redução de custos diversos, melhoria no acesso à informação além do aprimoramento e agilidade no processo de tomada de decisão.

2. OBJETIVOS DO PROJETO

2.1. Este projeto pretende oferecer a Prefeitura da Cidade de Maceió a prestação de serviços de comunicação multisserviços com racionalização de investimentos e ampliação de serviço, beneficiando e melhorando o exercício da gestão pública.

2.2. Subsidiar a construção de uma solução de comunicação chamada de SISTEMA INTEGRADO DE TELECOMUNICAÇÃO DA PREFEITURA DA CIDADE DE MACEIÓ.

2.3. Subsidiar a construção de uma solução de comunicação multisserviços.

3. FINALIDADES DO PROJETO

3.1. Proporcionar a Prefeitura de Maceió uma solução integrada, garantindo um salto qualitativo e quantitativo na expansão da oferta de serviços públicos à sociedade de Maceió, assegurando alta qualidade tecnológica, relacionamento uniformizado para todos os clientes e usuários, racionalização de recursos e ampliação de serviços, economia de escala com preços aderentes aos atualmente praticados pelo mercado.

3.2. Utilizar serviços de teleinformática e tecnologias adequadas para a promoção de inovações tecnológicas, expansão dos serviços oferecidos por meios digitais, facilitando a interligação de órgãos, que por sua vez, ampliará a oferta e melhoria da qualidade dos serviços prestados à sociedade.

3.3. Atender às unidades administrativas, localizadas nas zonas urbanas da capital, inclusive aquelas menos assistidas por infraestrutura básica.

3.4. Permitir uma gestão integrada, facilitando e otimizando tomada de decisões por parte da Prefeitura de Maceió.

3.5. Garantir a comunicação e integração de voz e dados entre todos os órgãos da Prefeitura através da NOVA REDE MACEIÓ.

3.6. Garantir a comunicação entre todos os órgãos municipais através da NOVA REDE MACEIÓ, que permitirá a operação de Sistemas Transacionais, Sistemas Informacionais, Sistemas Corporativos Públicos, acessos às Bases de Dados Públicas Institucionais, entrada/saída de dados, acesso à informação e serviços na web, videoconferência e teleconferência.

4. JUSTIFICATIVA DO PROJETO

4.1. O projeto NOVA REDE MACEIÓ justifica-se pela necessidade de instrumentalizar a Prefeitura da Cidade de Maceió com uma Rede de voz e dados Integrada, a serviço da modernização da gestão pública e para o fomento do desenvolvimento econômico e social em diversas áreas do conhecimento, com os seguintes aspectos:

4.2. Ampliar a prestação dos serviços integrados de telemática adequando-os às necessidades das unidades administrativas da cidade de Maceió, possibilitando assim, a expansão dos serviços de prefeitura voltados ao atendimento do cidadão.

4.3. Estabelecer um Modelo de Gestão de Telemática que ofereça um controle efetivo de previsão mensal de despesas, por parte da Prefeitura, e acompanhamento das despesas na área de comunicação de dados.

4.4. Agilizar a prestação dos serviços de telemática, unificando e padronizando a aquisição de tecnologias para comunicação convergente de forma a atender as especificações técnicas e de prazos exigidas pelos projetos da prefeitura, facilitando a Gestão Pública, como:

4.5. Atualização tecnológica;

4.6. Manutenção de equipamentos de rede de dados e telefonia fixa e móvel;

4.7. Administração e gerência dos recursos e serviços tecnológicos com abrangência em Maceió;

4.8. Melhorar a qualidade dos serviços.

4.9. Oferecer tecnologias convergentes e integradas para que os sistemas de informações setoriais e corporativos operacionalizados em diferentes plataformas passem a compartilhar uma mesma estrutura para os serviços de comunicação convergentes.

4.10. Oferecer tecnologias convergentes multisserviços para serem usadas em acessos a Sistemas de Informações Públicas, acesso à Internet, e disponibilizar um canal de comunicação entre as unidades administrativas da prefeitura e entre a sociedade, com a garantia de soluções específicas de segurança implementadas.

4.11. Oferecer e contemplar de forma padronizada às unidades administrativas da Prefeitura Municipal da cidade de Maceió, distribuídas em todo seu território, de acordo com as características específicas de cada uma.

4.12. Uniformizar os custos de operacionalização da rede, através da coordenação integrada dos recursos e serviços envolvidos.

4.13. Eliminar custos em aquisição de equipamentos para recursos de conectividade e configurações necessárias na prestação dos serviços de tecnologia de comunicação convergentes, tirando dos usuários o problema de manutenção e atualização tecnológica, que tem sido um fator dificultador para a Gestão Pública.

4.14. Manter e ampliar todos os benefícios já implantados com a atual REDE DE DADOS da Prefeitura da Cidade de Maceió.

TERMO DE REFERÊNCIA

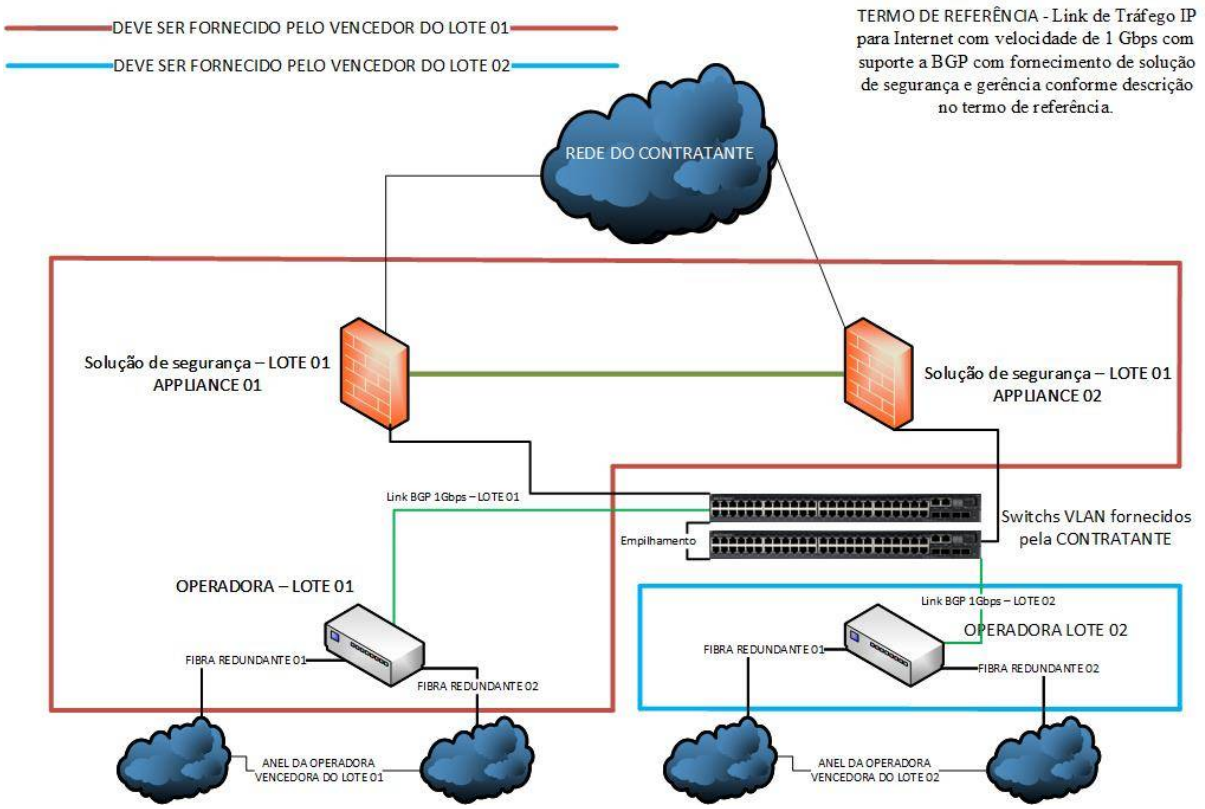
LINK DE TRÁFEGO IP PARA INTERNET COM SUPORTE A BGP COM SOLUÇÃO DE SEGURANÇA INTEGRADA E REDUNDÂNCIA DE LINK

1. OBJETO DA CONTRATAÇÃO

1.1. Trata-se da abertura de processo licitatório de Registro de preço, para contratação de empresa especializada em SERVIÇO de LINK DE TRÁFEGO IP PARA INTERNET COM SUPORTE A BGP, SOLUÇÃO DE SEGURANÇA INTEGRADA E REDUNDÂNCIA DE LINK. Os serviços e seus respectivos itens a serem fornecidos estão descritos na tabela a seguir:

LOTE	ITEM	SERVIÇOS	FATURAMENTO
01	01	Link de tráfego IP para internet com velocidade de 1 Gbps com suporte a BGP.	Mensal
	02	Solução de segurança e gerência.	Mensal
	03	Lote 1 - Blocos de IP (Bloco IPv4 /24 e Bloco IPv6 /48).	Mensal
02	03	Link de tráfego IP para internet com velocidade de 1 Gbps com suporte a BGP.	Mensal
	04	Lote 2 - Blocos de IP (Bloco IPv4 /24 e Bloco IPv6 /48).	Mensal

Diagrama da solução



2. JUSTIFICATIVA

2.1. Diante do atual cenário tecnológico que se encontra a Prefeitura Municipal de Maceió com a imprescindibilidade de acesso aos serviços fornecidos pelas suas Secretarias através de diversos sistemas desenvolvidos para ambiente WEB (World Wide Web - Rede Mundial de Computadores) - emissão de guias de pagamento de tributos (IPTU, ISS, Taxa de Localização, etc), sistema de gestão acadêmica, gestão de matrícula on-line dos estudantes (aproximadamente 50.000 alunos), emissão de contracheques, emissão de demonstrativo financeiro referente ao Imposto de Renda Retido na Fonte - IRRF, Sistemas administrativos (Protocolo Unificado, Folha de Pagamento, Almoxarifado, Patrimônio, etc), Sistemas de gestão da saúde, E-SUS, entre outros. É notável o crescimento de tráfego e consequentemente se faz necessário o aumento de sua infraestrutura. Além disso, cada vez mais é necessária a garantia de disponibilidade destes sistemas, devido às suas criticidades e por suas características de atendimento aos usuários, deve ter o mínimo de inatividade.

2.2. Para prestação dos serviços supracitados, atualmente a Prefeitura Municipal de Maceió possui em sua estrutura tecnológica 1 (um) link dedicado de 1 (um) Gbps, que atende a demanda da Secretaria Municipal de Gestão, Secretaria Municipal de Economia, Secretaria Municipal de Educação (e suas escolas), Secretaria municipal de Saúde (e seus postos), além de todas as sedes dos órgãos e unidades que estão sendo atendidas na rede privada MPLS. O tráfego agregado atualmente contratado desses links é de 5.7Gbps, aquém do que é necessário para a rede corporativa desta municipalidade.

2.3. Considerando ainda que a Prefeitura de Maceió possui instalado em sua plataforma corporativa, vários servidores computacionais críticos ao seu negócio, o crescente número de ameaças e ataques identificados, expondo ou debilitando a rede da Prefeitura de Maceió, considerando o nível de especialização necessária e a grande quantidade de atualizações técnicas para a manutenção deste tipo de serviço, a necessidade de manter este serviço ativo ininterruptamente, inclusive com monitoramento constante e pessoa qualificado para atuação, a necessidade de suporte para múltiplos serviços de apoio técnicos e incidentes ilimitados, fundamentado nas considerações descritas anteriormente, faz-se necessário contratação de solução para atuar de forma proativa e redundante, no monitoramento e gestão de eventos de segurança para detectar precocemente incidentes e mitigar possíveis vulnerabilidades e/ou ataques que a Prefeitura esteja sofrendo naquele momento, incluindo solução de equipamentos (hardwares) e seus programas (softwares), objetivando uma melhor integração entre os equipamentos e os serviços já existentes.

2.4. Esta Diretoria de Tecnologia da informação optou por contratar serviço de tráfego IP com suporte a BGP por ser o protocolo de roteamento mais robusto e por permitir a conexão de múltiplos sistemas autônomos (AS). O protocolo BGP basicamente ensina caminhos (rotas) e constrói mapas de forma dinâmica. Usando o protocolo BGP, o AS envia essas informações para seus vizinhos e recebe deles a informação correspondente. No mapa da tabela BGP, cada roteador da internet tem informação dos melhores caminhos para cada um dos destinos da rede e como prefeitura de Maceió está em processo de solicitação de seu próprio AS pela entidade responsável REGISTRO.BR, será possível conectar o nosso AS ao PTT (IX) que com uma única ligação física entre os mesmos pode interligar-se a centenas de outros servidores de forma rápida e segura. Nessa troca de tráfego, os Ases permitem o acesso do outro, ou outros às suas próprias redes, mutuamente de forma colaborativa reduzindo assim o trânsito de internet.

2.5. Nessa senda, torna-se necessária a eminente contratação de empresa especializada em fornecimento do serviço de link de tráfego IP com suporte a BGP na velocidade de 1 Gbps com solução de segurança integrada para que a Prefeitura Municipal de Maceió disponibilize um serviço de acesso à Internet, de maneira que venha produzir efeitos necessários com toda excelência na prestação de seus serviços de acesso dedicado e direto à Internet.

2.6. Visando garantir a alta disponibilidade, é também necessário contratar empresa especializada em fornecimento de link de tráfego IP com suporte a BGP e, devido a política de redundância, a empresa contratada deste item não poderá ser a mesma vencedora do item serviço de link de tráfego IP com suporte a BGP na velocidade de 1 Gbps com solução de segurança integrada (LOTE 1).

2.7. Devido ao processo de solicitação de ASN junto ao registro BR estar em andamento sob o número de protocolo (18406-20191104-24), foi necessária a inclusão dos itens 03 e 05 para o fornecimento de blocos de IP caso a solicitação seja negada ou haja um atraso na liberação do registro.

3. DO PAGAMENTO

3.1.1. Antes da emissão da fatura a CONTRATADA deverá enviar relatório em formato digital (.xlsx) de execução do serviço à CONTRATANTE e será observado a qualidade dos serviços prestados, conforme Acordo de Nível de Serviço. Este deverá conter:

3.1.1.1. Descrição do serviço como consta no item do contrato;

3.1.1.2. Indisponibilidades registradas do serviço;

3.1.1.3. Todos os chamados abertos no período contendo todas as informações do SLA;

3.1.1.4. Todos os descontos por descumprimento de SLA, já devem constar no relatório; Cabe a CONTRATANTE validar todas as informações do mesmo;

3.1.2. Os procedimentos que deverão ser realizados para o pagamento mensal dos serviços serão:

3.1.2.1. A CONTRATADA, através de seu preposto, deverá entregar ao fiscal do contrato, até o 5.º (quinto) dia útil subsequente ao mês anterior, o relatório mencionado no item 3.1.1;

3.1.2.2. O fiscal do contrato analisará a qualidade dos serviços prestados, conforme conteúdo do Acordo de Nível de Serviços, emitindo no prazo máximo de 5 (cinco) dias úteis, documento à CONTRATADA informando se houve ajuste no valor do pagamento;

3.1.2.3. A CONTRATADA terá o prazo de 5 (cinco) dias úteis para possível impugnação relativa ao percentual de ajuste de pagamento aferido ou para apresentar a respectiva nota fiscal e documentação inerente;

3.1.2.4. Havendo impugnação por parte da CONTRATADA, e constatada a existência de erro material, o fiscal poderá rever o fator de ajuste de pagamento ou, caso contrário, submeter à apreciação superior em até 2 (dois) dias úteis;

3.1.2.5. Decidida a impugnação, a CONTRATADA emitirá a nota fiscal conforme a decisão final.

3.1.3. O pagamento será efetuado mensalmente até o dia do vencimento da fatura, através de ordem bancária para pagamento de faturas com código de barras, sendo efetuada a retenção na fonte dos tributos e contribuições elencadas nas disposições determinadas pelos órgãos fiscais e fazendários, em conformidade com as legislações e instruções normativas vigentes, uma vez satisfeitas as condições estabelecidas neste documento, salvo por atraso no repasse de recursos financeiros ou a ocorrência de erro no documento de cobrança, situação em que será observado o previsto no **item 3.1.4** abaixo.

3.1.4. A CONTRATADA deverá disponibilizar a fatura de cobrança dos serviços, mensalmente, para a CONTRATANTE no mínimo 15 (quinze) dias úteis antes da data de seu vencimento. Caso haja atraso na sua apresentação, o pagamento será prorrogado pelo mesmo período do atraso.

3.1.5. O pagamento da nota fiscal só se efetivará depois de confirmada a situação fiscal da CONTRATADA, através da comprovação de regularidade com a Seguridade Social, FGTS e a Fazenda Federal, os quais poderão ser dispensados caso se encontre atualizado o cadastramento do contratado junto ao SICAF. A CONTRATADA deverá enviar junto com a nota fiscal, todas as certidões e solicitação de pagamento.

3.1.6. O pagamento está condicionado, ainda, ao atesto na referida nota fiscal, pelo fiscal do contrato, que representa a aceitação e regularidade dos serviços.

3.1.7. Após análise da cobrança com o "DE ACORDO" do fiscal do contrato, a CONTRATADA deverá enviar a solicitação de pagamento ao endereço de e-mail informado pela CONTRATADA.

3.1.8. O ciclo de faturamento preferencialmente deverá ser entre os dias 1.º (primeiro) e 30 (trinta) de cada mês ou data acordada entre as partes.

3.1.9. Havendo erro na fatura, ou circunstância que impeça a liquidação da despesa, aquela será devolvida à CONTRATADA e o pagamento ficará pendente até que seja sanado o problema ocorrido, o que preferencialmente deverá ocorrer em até 30 dias, sem a cobrança de juros ou mora. Nessa hipótese, o prazo para pagamento se iniciará após a regularização da situação e reapresentação do documento fiscal, não acarretando qualquer ônus para a CONTRATANTE.

3.1.10. Considerar-se-á como sendo a data do pagamento, a data da emissão da ordem bancária.

3.1.11. Em caso de atraso de pagamento motivado exclusivamente pela CONTRATANTE, o valor devido deverá ser acrescido de atualização financeira, e sua apuração se fará desde a data de seu vencimento até a data do efetivo pagamento, em que os juros de mora serão calculados à taxa de 0,5% (meio por cento) ao mês, ou 6% (seis por cento) ao ano, mediante a aplicação das seguintes fórmulas:

I = (TX / 100) / 365 EM = I x N x VP, onde:

I = Índice de atualização financeira;

TX = Percentual da taxa de juros de mora anual;

EM = Encargos moratórios;

N = Nº de dias entre a data prevista para pagamento e a do efetivo pagamento;

VP = Valor da parcela em atraso.

3.1.12. A CONTRATADA não terá direito ao recebimento da compensação financeira de que trata o item anterior, caso concorra de alguma forma para o atraso do pagamento, como, por exemplo, as ocorrências indicadas no **item 3.1.4** acima.

3.1.13. O pagamento referente ao primeiro mês de serviços prestados será realizado no valor proporcional. Na seguinte fórmula:

VALOR MENSAL / 30 DIAS x DIAS DE SERVIÇO PRESTADO = VALOR PARA PAGAMENTO.

4. MODALIDADE DA LICITAÇÃO E CRITÉRIOS DE JULGAMENTO

4.1. A aquisição dar-se-á pela modalidade licitatória denominada pregão, em sua FORMA ELETRÔNICA, tendo como critério de julgamento e classificação das propostas, o menor preço POR LOTE, tendo como referência o valor estimado, observado as especificações técnicas definidas neste Termo de Referência.

4.2. O PREGÃO ELETRÔNICO ocorrerá sob o modo de disputa ABERTO e FECHADO, onde as licitantes apresentarão lances públicos e sucessivos, com lance final e fechado.

4.2.1. Tendo em vista o poder discricionário da Administração Pública, bem como o disposto no art. 14 do decreto 10.024/2019 fora definido este modo de disputa vislumbrando atender ao principio da vantajosidade, uma vez que este modo proporciona a escolha da proposta mais vantajosa à Administração Pública.

4.3. Pelo interesse da administração pública, os valores de referência não serão divulgados.

4.4. Todas as folhas da proposta deverão estar numeradas, inclusive os manuais ou documentos anexados;

4.5. A proposta de preços deverá contemplar, expressamente, o preço individual dos itens que compõem o objeto, nos quais já estarão incluídos todos os tributos, inclusive contribuições fiscais, encargos sociais e trabalhistas, ferramentas, acessórios, instalações, obras físicas, utensílios, transporte, bem como quaisquer outros custos que poderão ocorrer até o total cumprimento do contrato;

4.6. A proposta deverá contemplar: prazos de entrega com data de validade e declaração de que nos preços ofertados estão incluídos todos os custos diretos e indiretos associados ao objeto;

4.7. O critério de avaliação das propostas orçamentárias apresentadas pelas empresas concorrentes deverá ser o de menor preço por grupo de itens;

4.8. **Por se tratar de links redundantes, o vencedor do LOTE 01 não poderá ser vencedor do LOTE 02 e vice-versa. O vencedor do lote 02 deverá comprovar que não possui como única fornecedora de tráfego IP a vencedora do LOTE 01 e vice-versa. Tal análise deverá ser feita por equipe técnica da DTI, que participará como equipe de apoio ao pregoeiro.**

5. DA VISITA TÉCNICA

5.1. Fica facultado as empresas participantes a visita técnica as localidades, para análise.

5.2. As interessadas poderão entrar em contato com a DTI para agendar sua visita, previamente, com 7 (sete) dias úteis de antecedência, no horário das 08h00min às 13h00min, de segunda à sexta-feira, através do telefone (82) 98714-2222 ou e-mail telecomunicacoes@dti.maceio.al.gov.br. As visitas poderão ser realizadas até o dia útil anterior a realização da licitação, no horário das 08h00 às 14h00.

5.3. As visitas deverão ser realizadas por representante devidamente credenciado pela empresa. A empresa deverá emitir carta de credenciamento contendo os dados do representante, autorizando o mesmo a representá-la, devidamente assinada pelo responsável pela empresa, razão pela qual o agendamento prévio garantirá uma completa vistoria dos locais, com a prestação dos esclarecimentos necessários.

5.4. Caso não realize a visita técnica, a empresa deverá declarar que tomou conhecimento dos locais onde serão realizados os serviços, responsabilizando-se pelas informações prestadas, não se aceitando alegações futuras quanto ao desconhecimento de fatos, quantidades, especificações, levantamentos, e/ou manutenção, ou quaisquer outros fatores inerentes que venham a compor a proposta de preços a ser apresentada;

5.5. Os Atestados de Visita Técnica (**ANEXO B**) ou a Declaração das empresas deverão ser apresentados obrigatoriamente na licitação.

5.6. Será de responsabilidade da CONTRATADA os eventuais prejuízos decorrentes da sua opção pela não realização da vistoria.

6. DA GESTÃO E FISCALIZAÇÃO

6.1. Para o acompanhamento do processo de contratação, implantação, operacionalização e gestão do Projeto será nomeado um Grupo Gestor com a seguinte composição:

6.1.1. Diretoria de Tecnologia de Informação (DTI/SEMGE):

6.1.1.1. 01 (um) Gestor e;

6.1.1.2. 01 (um) fiscal.

6.2. A gestão e fiscalização administrativa do contrato será exercida por servidor nomeado em Portaria da Prefeitura de Maceió, denominado gestor do contrato, o qual será responsável por todo o acompanhamento administrativo do contrato, recebimento e verificação de contas, entre outras atribuições. Caberá à Secretaria Municipal de Gestão - SEMGE analisar as especificações técnicas dos serviços prestados e verificar sua conformidade com as especificações contratuais. (Gestão administrativa de competência da Diretoria de Tecnologia da Informação da Secretaria Municipal de Gestão) e as seguintes atribuições:

6.2.1. Expedir ordens de fornecimento;

6.2.2. Proceder ao acompanhamento da entrega dos materiais e prestação do serviço;

6.2.3. Fiscalizar a entrega dos materiais quanto à qualidade desejada;

6.2.4. Comunicar à Contratada o descumprimento do contrato e indicar os procedimentos necessários ao seu correto cumprimento;

6.2.5. Solicitar à Administração a aplicação de penalidades por descumprimento de cláusula contratual;

6.2.6. Fornecer atestados de capacidade técnica quando solicitado, desde que atendidas às obrigações contratuais;

6.2.7. Atestar as notas fiscais relativas à execução dos serviços para efeito de pagamentos;

6.2.8. Recusar o objeto/serviço que for entregue fora das especificações contidas no Contrato ou que forem executados em quantidades divergentes daquelas constantes na ordem de serviços;

6.2.9. Solicitar à Contratada e a seu preposto todas as providências necessárias ao bom e fiel cumprimento das obrigações.

7. DA DOTAÇÃO ORÇAMENTÁRIA

7.1. As despesas decorrentes da contratação do objeto deste edital correrão à conta dos recursos específicos consignados no orçamento da CONTRATANTE.

7.2. Quando da contratação, para fazer face à despesa, será emitida Declaração do Ordenador da Despesa de que a mesma tem adequação orçamentária e financeira com a Lei de Responsabilidade

Fiscal, com o Plano Plurianual e com a Lei de Diretrizes Orçamentárias, acompanhada da Nota de Empenho expedida pelo setor contábil do Órgão interessado.

~~8.~~ DESCRIÇÃO DOS ITENS

8.1. LOTE 1 – ITEM 1 – E LOTE 2 – ITEM 4 LINK DE TRÁFEGO IP 1 GBPS COM CONECTIVIDADE A INTERNET

8.1.1. Modalidade dedicado com velocidade simétrica (upload e download) de 1Gbps com suporte ao protocolo BGP, incluindo disponibilização de todos os recursos de conectividade, tais como: modems, conversores, roteadores, cabos e outros concernentes ao funcionamento do serviço contratado;

8.1.2. Os links e equipamentos deverão ser instalados no datacenter da prefeitura localizado no prédio da Secretaria Municipal de Economia, na Rua Dr. Pedro Monteiro, 47, Centro, Maceió – AL no 3º Andar.

8.1.3. A tecnologia utilizada para tráfego de dados deverá ser implementada utilizando-se fibra óptica, ao longo de todo o circuito, com infraestrutura redundante tipo anel óptico;

8.1.4. O anel óptico redundante deve ser implementado de maneira tal que garanta total continuidade do serviço na indisponibilidade de uma das fibras ópticas (Ex.: Queda de poste, vandalismo, etc.);

8.1.5. Em caso de falha na fibra principal, o anel óptico redundante deverá assumir de imediato, sem perdas;

8.1.6. A CONTRATADA deve prover uma solução de segurança corporativa Anti-DDoS de volumetria de detecção e mitigação contra ataques de negação de serviço distribuída. O link deverá ser entregue a CONTRATANTE *líquida* e sem esse tipo de tráfego.

8.1.7. NÍVEIS DE SERVIÇO

8.1.7.1. Considerando que o período de indisponibilidade no ambiente de Tecnologia da Informação tem como preceito fundamental o tempo pelo qual os serviços que presumidamente estejam à disposição dos usuários e que não puderam ser acessados ou até mesmo não promoveram um adequado resultado, faz-se necessário implementar um link de conectividade com a Internet com a maior disponibilidade possível.

8.1.7.2. O item Serviço de comunicação de dados entre a Prefeitura de Maceió e a Internet deverá possuir latência de no máximo, 80 MS (oitenta milissegundos). A latência será considerada como o tempo em que um pacote IP leva para ir de um ponto a outro da rede e retornar à origem. A latência será aferida pela CONTRATANTE da seguinte forma:

8.1.7.2.1. Coletar amostras de latência a cada 05 (cinco) minutos para o roteador da operadora;

8.1.7.2.2. Ao final de cada mês deverá verificar o percentual de pacotes acima do limite de latência, dentro desse período de apuração;

8.1.7.3. Para o item Serviço de Link de tráfego IP com conectividade a Internet entre o ambiente da CONTRATANTE e a Internet, as medições devem ser feitas entre o roteador responsável pelo serviço no ambiente da Prefeitura de Maceió e o primeiro roteador na Internet;

8.1.7.4. Os intervalos de tempo que o enlace apresentar aferições de latência superiores ao valor especificado serão considerados como períodos de indisponibilidade.

8.1.7.5. O Link de conectividade com a Internet deverá possuir perda de pacotes de no máximo 1% (um por cento), índice que será aferido pela CONTRATANTE da seguinte forma:

8.1.7.5.1. A cada 5 (cinco) minutos deve ser medida a perda de pacotes;

8.1.7.5.2. Ao final de cada mês deverá ser verificado o percentual de pacotes perdidos dentro desse período de apuração;

8.1.7.5.3. As medições devem ser feitas entre o equipamento responsável pelo serviço no ambiente da Prefeitura de Maceió e o primeiro roteador na Internet;

8.1.7.5.4. Os intervalos de tempo que os enlaces apresentarem aferições do percentual de perda de pacotes superiores ao valor especificado, serão considerados como períodos de indisponibilidade;

8.1.7.5.5. Para o cálculo deste parâmetro serão considerados erros de interface, pacotes corrompidos pelo enlace, bem como descartes injustificados por parte do roteador;

8.1.7.5.6. A solução deverá possuir disponibilidade de, no mínimo, 99,5% (noventa e nove vírgula cinco porcento);

8.1.7.5.7. A disponibilidade do serviço corresponde ao percentual de tempo, durante o período de 1 (um) mês, em que o mesmo esteve em condições normais de funcionamento. Serão considerados como períodos de indisponibilidade o tempo em que o serviço estiver total ou parcialmente indisponível.

8.1.7.6. Não serão consideradas indisponibilidades as seguintes situações:

8.1.7.6.1. Paradas programadas pela CONTRATADA e aprovadas pela Prefeitura de Maceió. Neste caso a autorização deve ser solicitada pela Prefeitura de Maceió com, pelo menos, 5 (cinco) dias úteis de antecedência;

8.1.7.6.2. Paradas em função da falta de alimentação dos equipamentos instalados no datacenter da Prefeitura de Maceió;

8.1.7.6.3. Paradas internas ocasionadas pela Prefeitura de Maceió, sem responsabilidade da CONTRATADA;

8.1.7.7. A CONTRATADA deverá disponibilizar à Prefeitura de Maceió, portal na Internet, para acompanhamento dos níveis de serviços prestados, para fins de aferição com os dados apurados pela CONTRANTE;

8.1.7.8. Entende-se por portal, ferramenta de gerência acessível pela Internet, por intermédio de um navegador Web, com acesso restrito através de usuário/senha eletrônica e utilizando-se de protocolo HTTPS;

8.1.7.9. O portal de acompanhamento dos serviços deverá possuir acesso aos históricos dos registros das ocorrências e registros de solicitações e reclamações enviadas pela Prefeitura de Maceió;

8.1.7.10. A análise técnica na qualidade de transmissão quanto a Taxa de Erros e Perda de Pacotes deverá ser realizada pela gerência da rede da CONTRATADA, com a auditoria da Diretoria de Tecnologia da Informação - DTI/SEMGE, sempre quando houver a necessária solicitação da CONTRATANTE, sem custos adicionais;

8.1.7.11. A gerência da rede da CONTRATADA deverá apurar, através de emissão de relatórios mensais, os tempos de falha do circuito dedicado, considerando as ocorrências desde a zero hora do primeiro dia do mês até as vinte e quatro horas do último dia do mês anterior ao da apuração.

8.1.7.12. Considera-se início para efeito de contagem do prazo, o registro da chamada junto a Central de Atendimento (Telefônico, sistema WEB, E-mail), disponibilizada pela CONTRATADA, até a comunicação da resolução definitiva com a análise técnica e aprovação realizadas pela Diretoria de Tecnologia da Informação - DTI da SEMGE, imprescindíveis para a autorização de fechamento do chamado.

8.1.7.13. A CONTRATADA deverá fornecer pelo menos 4 (quatro) usuário/senha para acesso ao portal de acompanhamento dos serviços de Internet e Segurança;

8.1.7.14. O portal de acompanhamento dos serviços deverá possibilitar que sejam visualizados e impressos os relatórios das informações de desempenho do link de conectividade;

8.1.7.15. A CONTRATANTE irá também acompanhar o desempenho do link através do seu sistema de monitoramento próprio e utilizará as métricas definidas neste termo para efeitos de glosa;

8.1.7.16. Deverá ser fornecido, mensalmente, relatório contendo os registros das ocorrências no referido período;

8.1.7.17. A CONTRATADA deverá divulgar, no portal de acompanhamento dos serviços, relatórios detalhando os valores das medições dos parâmetros de qualidade do link de conectividade, conforme detalhamento deste Termo de Referência. Devem ser feitas medições a cada 5 (cinco) minutos. Para cada medição o relatório deve apresentar pelo menos os seguintes valores:

8.1.7.17.1. Dia e hora da medição;

8.1.7.17.2. Total de pacotes trafegados;

8.1.7.17.3. Total de pacotes com erros;

8.1.7.17.4. Latência;

8.1.7.18. A disponibilidade global do serviço de link de tráfego IP (Internet Protocol), deverá ser calculada, para um período de 1 (um) mês, através da equação descrita na tabela abaixo:

Tabela: Equação que mede a disponibilidade global do serviço IP (período mensal)

D(%)= [(To - Ti)/To]*100, onde
D = Disponibilidade; To = Período de Operação (1 mês) em minutos. Para o cálculo do índice de disponibilidade, o "tempo total mensal" será calculado a partir do total de dias da prestação do serviço vezes 1440 (mil quatrocentos e quarenta) minutos; Ti (*Downtime*) = Somatório dos tempos de indisponibilidade do serviço observado durante o período de operação (1 mês), em minutos (excetuando-se as paradas internas sob responsabilidade da Prefeitura de Maceió)

8.1.7.19. Os serviços contratados serão considerados indisponíveis a partir do momento em que eventuais problemas forem detectados até o seu retorno às condições plenas de funcionamento;

8.1.7.20. A apuração e/ou contabilização das grandezas acima definidas, para efeito de aferição de resultados, dar-se-á mensalmente;

8.1.7.21. O período de indisponibilidade (Ti) será glosado proporcionalmente na fatura mensal em relação ao tempo total mensal de operação (To), conforme o seguinte cálculo:

G = [(100-D)/100] * VMF

Onde:

VMF: Valor mensal da fatura;

G: Valor Total da Glosa.

D: Índice de Disponibilidade Mensal;

8.1.8. DA FORMA DE ENTREGA E EXECUÇÃO

8.1.8.1. A Contratada deverá entregar o cronograma de implantação em até 2 dias úteis após a ordem de fornecimento. Neste cronograma deve conter no mínimo:

8.1.8.1.1. Data da Visita técnica preliminar e coleta de informações;

8.1.8.1.2. Data da migração do serviço;

8.1.8.2. A Contratada terá o prazo de 20 dias úteis para a instalação do serviço após a ordem de fornecimento emitida pelo gestor do contrato.

8.1.8.3. As datas mencionadas acima devem ser acordadas com a DTI/SEMGE e não devem ultrapassar o limite estabelecido no **item 8.1.8.2** para a entrega dos serviços.

8.1.8.4. Todos os serviços contratados serão instalados na sede da Secretaria Municipal de Economia, Rua Dr. Pedro Monteiro, 47, Centro Maceió – Alagoas;

8.1.8.5. O momento da migração dos serviços será acordado entre a Contratada e a DTI/SEMGE, de forma a minimizar as indisponibilidades dos sistemas/internet. O serviço de migração poderá ser realizado fora do horário comercial.

8.1.8.6. Será considerada para o efetivo início de prestação de serviço, o dia em que a Contratada comprovar, através de Relatório Técnico Conclusivo na forma digital, tráfego no link contratado. O relatório deve ser enviado para o e-mail: gestao.contratos@dti.maceio.al.gov.br. Neste relatório deve conter:

8.1.8.7. Data dos testes;

8.1.8.8. Testes de velocidade;

8.1.8.9. Assinatura do técnico responsável da Contratada;

8.1.8.10. Os testes serão acompanhados por técnicos da CONTRATANTE;

8.1.8.11. O relatório será analisado em até 2 dias úteis. Caso o relatório seja reprovado, o mesmo, deverá ser refeito. A nova data do relatório será considerada como o efetivo início de prestação do serviço;

8.1.8.12. A CONTRATADA terá um prazo de 10 (dias) para sanar qualquer irregularidade do início dos serviços apresentado no Relatório Técnico Conclusivo e apontado pela DTI/SEMGE;

8.1.9. DA INSTALAÇÃO, CONFIGURAÇÃO E INTEGRAÇÃO

8.1.9.1. O fornecimento e a passagem de cabos (fiação interna para ligação entre o quadro de “distribuição geral” (DG) e a sala em que os equipamentos serão acomodados nas localidades) será de responsabilidade da CONTRATADA limitando-se a 300 metros de cabos;

8.1.9.2. A CONTRATADA deverá fornecer os links obrigatoriamente terrestres, implementados por meio de fibra óptica;

8.1.9.3. A CONTRATADA deve ajustar seu plano de trabalho em conjunto com a equipe técnica do CONTRATANTE, de maneira a adequar horários e procedimentos de configuração e testes;

8.1.9.4. A CONTRATADA deve recompor obras civis e pintura eventualmente afetadas quando da passagem dos cabos, mantendo o padrão local;

8.1.9.5. A instalação dos links será acompanhada pelas equipes de gestão e fiscalização do contrato e pela DTI/SEMGE;

8.1.9.6. As visitas técnicas nos locais de instalação devem ser previamente agendadas com o CONTRATANTE;

8.2. LOTE 1 – ITEM 2 SOLUÇÃO DE SEGURANÇA

8.2.1. Alocação de equipamentos e gerenciamento (baseado em appliance), com função de Next-Generation Firewall (NGFW), Statefull, suportando a configuração em alta disponibilidade com tolerância a falhas (HA), podendo ser admitida a configuração ativo-passivo e ativo-ativo; Os equipamentos devem atender as funções e funcionalidades, no mínimo:

8.2.1.1. Controle de Aplicações

8.2.1.2. Proteção IPS

8.2.1.3. Proteção Antivírus, Antispyware e Antispam

8.2.1.4. Análise de Malwares Modernos

8.2.1.5. Filtro de URL

8.2.1.6. Controle de Transferência de Arquivos

8.2.1.7. Controle de Tráfego

8.2.1.8. De-criptografia SSL

8.2.1.9. Módulo VPN

8.2.1.10. Roteamento e NAT

8.2.1.11. Suporte a BGP

8.2.2. DA INSTALAÇÃO, CONFIGURAÇÃO E INTEGRAÇÃO

8.2.3. Executar todos dos serviços de planejamento, instalação, configuração, integração e testes de funcionalidade, conforme descrito neste Termo de Referência;

8.2.4. Instalação física da solução de segurança no ponto de conexão com a Internet e as redes conectadas;

8.2.5. Realizar, com os técnicos da contratante, testes de funcionalidade para constatar que os equipamentos foram instalados, configurados e integrados de acordo com os requisitos técnicos e parâmetros de configuração solicitados;

8.2.6. Elaborar uma documentação técnica, contendo todas as configurações efetuadas e as descrições das características e recursos utilizados;

8.2.7. Colocar à disposição da contratante, analistas técnicos especializados para a execução das soluções a serem implantadas em sua rede corporativa durante o tempo de funcionamento da solução, estes técnicos deverão ser devidamente certificados pelo fabricante da solução, e a certificação não pode estar vencida durante todo o período do contrato.

8.2.8. Configuração da solução de segurança com as políticas de acesso e estrutura de segurança:

8.2.8.1. Integração com o diretório de usuários corporativos (AD)/LDAP;

8.2.8.2. Configuração do controle de aplicações;

8.2.8.3. Configuração das VLAN;

8.2.8.4. Configuração do Filtro de conteúdo WEB;

8.2.8.5. Configuração do anti-malware de gateway;

8.2.8.6. Solução Anti Spam;

8.2.8.7. Configuração do IPS;

8.2.8.8. Configuração dos parâmetros de QoS que serão fornecidos pela equipe técnica da contratante;

8.2.8.9. Configuração dos clientes de VPN;

8.2.8.10. Testes e monitoração;

8.2.9. **CARACTERÍSTICAS DA DEMANDA, E CONFIGURAÇÕES MÍNIMAS DOS EQUIPAMENTOS:**

8.2.9.1. O serviço deve incluir as substituições de equipamentos, sem ônus, caso se perceba limitação ou degradação da rede com base nos limites físicos (banda, portas, cabos), conforme demanda especificado neste Termo;

8.2.9.2. A solução appliance não irá permitir soluções instaladas e executadas em um sistema operacional regular, como Microsoft Windows, FreeBSD, SUN solaris, GNU/Linux, etc.

8.2.9.3. Garantir que não haja restrição por número de usuários que utilizem a solução disponibilizada;

8.2.9.4. O serviço deve incluir as substituições de equipamentos defeituosos fornecidos na composição da solução;

8.2.9.5. Os equipamentos devem ser instalados conforme diagrama no item 1 deste termo de referência;

8.2.9.6. A contratante ficará responsável pela disponibilização de espaço em rack (limitando-se a 12U) para os equipamentos de segurança da informação, ficando a cargo da contratada o fornecimento de patch cords e outros insumos pertinentes a conectorização, energização e organização dos equipamentos à rede da contratante;

8.2.9.7. Para efeito de cotação, a infraestrutura elétrica, deverá ser considerada a partir do circuito mais próximo limitando-se a 40 (quarenta) metros;

8.2.9.8. Para efeito de cotação, a infraestrutura lógica deverá ser considerada a partir do patch panel mais próximo, limitando-se a 90 (noventa) metros.

8.2.9.9. Incluir todas as licenças de software e de hardware necessárias ao perfeito e completo funcionamento das soluções ofertadas;

8.2.9.10. Adicionalmente, o serviço deve prever que, ao término do contrato, todos os equipamentos e softwares deverão permanecer à disposição da contratante, sem custos, por período de até seis meses, a critério da Contratante, para fins de migração da solução para um novo contrato, devendo, durante este período, atender e respeitar todas as cláusulas e regras deste Termo de Referência, bem como de seus anexos, contratos e adendos;

8.2.9.11. As características de performance mínima exigida para os equipamentos estão descritas na tabela abaixo:

Especificação Mínima	**Lote 1 - Item 1***
	Valor
Throughput de Firewall (Gbps)	27
Conexões simultâneas (milhões)	8
Novas conexões por segundo (mil)	450
Throughput de IPSec (Gbps)	20
Proteção combinada contra ameaças** (Gbps)	7
Quantidade mínima de interfaces RJ45 (1 Gbps)	8
Quantidade mínima de interfaces SFP (1 Gbps)	8
Quantidade mínima de interfaces SFP+ (10 Gbps)	2
Políticas de Firewall (mil)	10

* Devem ser ofertados 01 (um) par de equipamentos configurados em HA.

** Com funcionalidades habilitadas simultaneamente devidamente atuantes: controle de aplicação, IDS/IPS e controle de malware (antivírus, etc.) medidas com parâmetros de throughput considerando tráfego misto. Não serão aceitas medidas baseadas em condições ideais.

8.2.10. CARACTERISTICAS GERAIS DOS EQUIPAMENTOS

8.2.10.1. Suporte a, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance;

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

8.2.10.3. Os dispositivos de proteção de rede devem possuir suporte a 4094 VLAN Tags 802.1q;

8.2.10.4. Os dispositivos de proteção de rede devem possuir suporte a agregação de links 802.3ad e LACP;

8.2.10.5. Os dispositivos de proteção de rede devem possuir suporte a Policy based routing ou policy based forwarding;

8.2.10.6. Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);

8.2.10.7. Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay;

8.2.10.8. Os dispositivos de proteção de rede devem possuir suporte a DHCP Server;

8.2.10.9. Os dispositivos de proteção de rede devem possuir suporte a Jumbo Frames;

8.2.10.10. Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;

8.2.10.11. Deve suportar NAT dinâmico (Many-to-1) e (Many-to-Many);

8.2.10.12. Deve suportar NAT estático (1-to-1) e (Many-to-Many);

8.2.10.13. Deve suportar NAT estático bidirecional 1-to-1;

8.2.10.14. Deve suportar Tradução de porta (PAT);

8.2.10.15. Deve suportar NAT de Origem e Destino;

8.2.10.16. Deve poder combinar NAT de origem e NAT de destino na mesma politica

8.2.10.17. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;

8.2.10.18. Deve suportar NAT64 e NAT46;

8.2.10.19. Deve implementar o protocolo ICMP;

8.2.10.20. Deve implementar balanceamento de link por hash do IP de origem;

8.2.10.21. Deve implementar balanceamento de link por hash do IP de origem e destino;

8.2.10.22. Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, três links;

8.2.10.23. Deve implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais;

8.2.10.24. Proteção anti-spoofing;

8.2.10.25. Implementar otimização do tráfego entre dois equipamentos;

8.2.10.26. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);

8.2.10.27. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);

8.2.10.28. Suportar OSPF graceful restart;

8.2.10.29. Os dispositivos de proteção devem ter a capacidade de operar de forma simultânea em uma única instância de firewall, mediante o uso de suas interfaces físicas nos seguintes modos: Modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (L2) e camada 3 (L3);

8.2.10.30. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;

8.2.10.31. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em modo transparente;

8.2.10.32. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo;

8.2.10.33. A configuração em alta disponibilidade deve sincronizar: Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS, sessões e objetos de rede;

8.2.10.34. A configuração em alta disponibilidade deve sincronizar: Tabelas FIB;

8.2.10.35. Deve permitir a criação de administradores independentes, para cada um dos sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados por equipes distintas;

8.2.10.36. Controle, inspeção e descriptografia de SSL para tráfego de entrada (Inbound) e Saída (Outbound), sendo que deve suportar o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolamento das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos);

8.2.10.37. Deverá suportar controles por zona de segurança;

8.2.10.38. Controles de políticas por porta e protocolo;

8.2.10.39. Controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;

8.2.10.40. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;

8.2.10.41. Firewall deve ser capaz de aplicar a inspeção UTM (Application Control e Webfiltering no mínimo) diretamente às políticas de segurança versus via perfis;

8.2.10.42. Além dos endereços e serviços de destino, objetos de serviços de Internet devem poder ser adicionados directamente às políticas de firewall;

8.2.10.43. Deve suportar o armazenamento de logs em tempo real tanto para o ambiente de nuvem quanto o ambiente local (on-premise);

8.2.10.44. Deve suportar o padrão de indústria 'syslog' protocol para armanazemento usando o formato Common Event Format (CEF);

8.2.10.45. Deve haver uma maneira de assegurar que o almazenamento dos logs em tempo real não superam a velocidade de upload;

8.2.10.46. Deve suportar o protocolo padrão da indústria VXLAN;

8.2.10.47. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;

8.2.10.48. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;

8.2.10.49. Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;

8.2.10.50. Atualizar a base de assinaturas de aplicações automaticamente;

8.2.10.51. Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos;

8.2.10.52. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;

8.2.10.53. Deve ser possível adicionar controle de aplicações em múltiplas regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;

8.2.10.54. Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;

8.2.10.55. Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;

8.2.10.56. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante;

8.2.10.57. A criação de assinaturas personalizadas deve permitir o uso de expressões regulares, contexto (sessões ou transações), usando posição no payload dos pacotes TCP e UDP e usando decoders de pelo menos os seguintes protocolos: HTTP, FTP, NBSS, DCE RPC, SMTP, Telnet, SSH, MS-SQL, IMAP, DNS, LDAP, RTSP e SSL;

8.2.10.58. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;

8.2.10.59. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Nível de risco da aplicação;

8.2.10.60. Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação;

8.2.10.61. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;

8.2.10.62. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);

8.2.10.63. As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante;

8.2.10.64. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;

8.2.10.65. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear, bloquear IP do atacante por um intervalo de tempo e enviar tcp-reset;

8.2.10.66. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;

8.2.10.67. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;

8.2.10.68. Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura;

8.2.10.69. Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes politicas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;

8.2.10.70. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;

8.2.10.71. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação;

8.2.10.72. Deve permitir que na captura de pacotes por assinaturas de IPS seja definido o número de pacotes a serem capturados ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos;

8.2.10.73. Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;

8.2.10.74. Os eventos devem identificar o país de onde partiu a ameaça;

8.2.10.75. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferentes de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança;

8.2.10.76. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local;

8.2.10.77. Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;

8.2.10.78. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local;

8.2.10.79. Deve possuir a função de exclusão de URLs do bloqueio, por categoria;

8.2.10.80. Permitir a customização de página de bloqueio;

8.2.10.81. Permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão Continuar para permitir o usuário continuar acessando o site);

8.2.10.82. Além do Explicit Web Proxy, suportar proxy Web transparente;

8.2.10.83. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local;

8.2.10.84. Permitir a customização de página de bloqueio;

8.2.10.85. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem;

8.2.10.86. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de destino;

8.2.10.87. Suportar a criação de políticas de QoS e Traffic Shaping por usuário e grupo;

8.2.10.88. Suportar a criação de políticas de QoS e Traffic Shaping por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;

8.2.10.89. Suportar a criação de políticas de QoS e Traffic Shaping por porta;

8.2.10.90. O QoS deve possibilitar a definição de tráfego com banda garantida;

8.2.10.91. O QoS deve possibilitar a definição de tráfego com banda máxima;

8.2.10.92. O QoS deve possibilitar a definição de fila de prioridade;

8.2.10.93. Suportar priorização em tempo real de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype;

8.2.10.94. Suportar marcação de pacotes Diffserv, inclusive por aplicação;

8.2.10.95. Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping;

8.2.10.96. Deve suportar QOS (traffic-shapping), em interface agregadas ou redundantes;

8.2.10.97. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP, etc);

8.2.10.98. Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

8.2.10.99. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre esses tipos de arquivos;

8.2.10.100. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular;

8.2.10.101. Suportar a criação de políticas por geo-localização, permitindo o trafego de determinado Pais/Países sejam bloqueados;

8.2.10.102. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;

8.2.10.103. Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas;

8.2.10.104. Suportar VPN Site-to-Site e Cliente-To-Site;

8.2.10.105. Suportar IPSec VPN;

8.2.10.106. Suportar SSL VPN;

8.2.10.107. Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de throubleshooting;

8.2.10.108. A VPN SSL deve suportar o usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;

8.2.10.109. A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;

8.2.10.110. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;

8.2.10.111. Atribuição de DNS nos clientes remotos de VPN;

8.2.10.112. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;

8.2.10.113. Suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local;

8.2.10.114. Suportar leitura e verificação de CRL (certificate revocation list);

8.2.10.115. Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;

8.2.10.116. O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 7 (32 e 64 bit), Windows 8 (32 e 64 bit), Windows 10 (32 e 64 bit) e Mac OS X (v10.10 ou superior);

8.2.11. GESTÃO DOS EQUIPAMENTOS E SERVIÇO DE SEGURANÇA DA INFORMAÇÃO

8.2.11.1. Os serviços deverão ser prestados remotamente, a partir de Centros de Operação de Segurança (SOC) próprios, com atendimento em Português do Brasil, de acordo com as especificações mínimas deste Termo;

8.2.11.2. A viabilização da operação remota será feita através de comunicação segura entre um agente de monitoramento instalado na rede da contratante e o SOC;

8.2.11.3. Disponibilizar Central de Atendimento 0800 ou equivalente a ligação local, web e e-mail, para abertura de chamados referentes a:

8.2.11.4. Solicitação de mudanças no sistema de monitoramento para que este reflita mudanças na infraestrutura da Contratante;

8.2.11.5. Solicitação de programação de períodos de manutenção;

8.2.11.6. Solicitação de relatórios de histórico de eventos e métricas de performance de recursos como links de comunicação e memória;

8.2.11.7. Solicitação de relatório de tendências para prevenção de indisponibilidade futura;

8.2.11.8. Aberturas de chamados de suporte técnico à solução de segurança fornecida;

8.2.11.9. Disponibilizar um número de serviço, em língua portuguesa, para abertura de chamados técnicos. Este serviço deverá obrigatoriamente estar disponível 24x7;

8.2.11.10. Atuar, de forma proativa, no monitoramento e gestão de eventos de segurança 24x7, para detectar precocemente incidentes e mitigar possíveis vulnerabilidades e/ou ataques que a contratante esteja sofrendo naquele momento;

8.2.11.11. Incluir todas as licenças de software e de hardware necessárias ao perfeito e completo funcionamento das soluções ofertadas;

8.2.11.12. O SOC requer a atuação de, minimamente, macro equipes e suas subdivisões, localmente ou remotamente, conforme relação abaixo:

8.2.11.12.1. Gestão de Segurança (SOC)

8.2.11.12.2. Gestão de Eventos e Incidentes de Segurança;

8.2.11.12.3. Gestão de Acessos;

8.2.11.12.4. Gestão de Segurança de Rede;

8.2.11.12.5. Suporte Operacional

8.2.11.12.6. Gestão da Plataforma de Gerenciamento;

8.2.11.12.7. Gestão de Níveis de Serviço (Qualidade);

8.2.11.12.8. Comitê de Gestão de Mudanças;

8.2.11.13. A Gestão de Segurança (SOC) deve ser capaz de realizar a detecção e reagir a incidentes de segurança. Dentre as principais atribuições deste serviço destacam-se:

8.2.11.14. Monitorar e solucionar eventos e incidentes de segurança lógica da Rede da CONTRATANTE;

8.2.11.15. Conceder acesso às ferramentas de monitoramento administradas pela CONTRATADA, conforme diretrizes da CONTRATANTE;

8.2.11.16. Apoiar a gestão das políticas e dos processos de segurança da Rede da CONTRATANTE;

8.2.11.17. Realizar procedimentos de backup das soluções de segurança da Rede da CONTRATANTE;

8.2.11.18. Gerir e atualizar versões das ferramentas administradas pela CONTRATADA e das soluções de segurança da Rede da CONTRATANTE;

8.2.11.19. Caberá ao serviço de Gestão de Segurança a análise de todo e qualquer incidente de segurança de rede e acesso, entre outros, tendo como incumbência também a pronta reação a este incidente, realizando as devidas proteções na rede, mudanças de configuração, bloqueios, alterações de perfil, identificação dos indivíduos contraventores, entre outras ações;

8.2.11.20. A equipe de Gestão de Segurança será também responsável pelo apoio à definição de todas as políticas de segurança da rede e de acesso à mesma, tendo como atribuição também a configuração dos parâmetros necessários para sua implementação;

8.2.11.21. A equipe de Gestão de Segurança será responsável pelo apoio à gestão de acessos aos sistemas de suporte a operação, com a atribuição de manter e controlar também todos os logs de acessos e mudanças de configuração da rede;

8.2.11.22. A equipe de Gestão de Segurança deverá operar em regime 24 horas por 7 dias, ou seja, estar presencialmente e/ou remotamente e de forma ininterrupta disponível para realizar o diagnóstico, correlações, enriquecimento de informações, tratamento e correção das falhas e emissão de relatórios. Caberá à CONTRATADA apresentar proposta de dimensionamento que cubra a escala 24x7 e atenda a volumetria, processos e necessidades da CONTRATANTE, cabendo a CONTRATANTE a avaliação da proposta;

8.2.11.23. A equipe de Gestão de Segurança deverá realizar a manutenção do backup de configurações e logs de todos os equipamentos utilizados para atender a este lote, com frequência mínima de acordo com a política de gestão de segurança;

8.2.11.24. Na área de Gestão de Segurança deverão atuar as equipes que efetivamente monitoram os eventos de segurança, alarmes, bilhetes, condições da rede e gerências em geral e tratam estes eventos a fim de sanar falhas, anormalidades, degradações ou problemas que afetem gerências, monitoramento e principalmente a rede da PREFEITURA DE MACEIÓ;

8.2.11.25. De forma geral, a equipe de Gestão de Segurança deverá:

8.2.11.25.1. Operar e manter as soluções de segurança da informação seguindo os processos estabelecidos e mantendo os padrões de desempenho, disponibilidade e segurança estabelecidos;

8.2.11.25.2. Monitorar os ativos de segurança da informação da CONTRATADA dos sites que compõem a Rede da PREFEITURA DE MACEIÓ;

8.2.11.25.3. Solucionar incidentes de segurança ocorridos na rede, provendo suporte técnico;

8.2.11.25.4. Atuar preventivamente para evitar que incidentes de segurança ocorram;

8.2.11.25.5. Informar à CONTRATANTE sobre serviços afetados devido a falhas críticas na rede ocasionadas por eventos de segurança;

8.2.11.25.6. Analisar e realizar mudanças solicitadas para solucionar incidentes de segurança ou introduzir melhorias na rede;

8.2.11.25.7. Realizar o acionamento de equipes de campo, quando for o caso, para atuação em incidentes, manutenções, ativações, modificações, remoções, verificações preventivas de serviços, equipamentos, facilidades e clientes;

8.2.11.25.8. Realizar o relacionamento operacional com a operadora vencedora do lote 02 para garantir a adequada prestação dos serviços;

8.2.11.26. Seguir práticas ITIL para Gestão de Incidentes:

8.2.11.27. Registrar os incidentes.

8.2.11.28. Categorizar e priorizar os incidentes:

8.2.11.28.1. Investigar e diagnosticar a causa dos incidentes

8.2.11.28.2. Restabelecer os serviços o mais rápido possível (workarounds)

8.2.11.28.3. Realizar as escalações necessárias (funcional e hierárquica)

8.2.11.28.4. Abrir solicitações de mudanças para resolução dos incidentes

8.2.11.28.5. Gerir SLA`s de resolução de incidentes

8.2.11.28.6. Seguir práticas ITIL para Gestão de Mudanças:

8.2.11.28.7. Classificar e priorizar as mudanças

8.2.11.28.8. Analisar os impactos e riscos das mudanças solicitadas

8.2.11.28.9. Suportar o Comitê de Mudanças da CONTRATANTE

8.2.11.28.10. Apoiar os planos de implementação de mudanças

8.2.11.28.11. Acompanhar a coordenação e a execução dos planos de mudanças

8.2.11.28.12. Registrar e documentar as mudanças

8.2.11.29. Seguir práticas ITIL para Gestão de Problemas:

8.2.11.29.1. Analisar reincidências e registrar tickets de problemas

8.2.11.29.2. Apoiar na investigação da causa raiz de problemas registrados

8.2.11.29.3. Apoiar a gestão da base de problemas e soluções conhecidos

8.2.11.29.4. Solicitar mudanças para resolução de problemas

8.2.11.30. Por bilhetes entendem-se os tickets gerados na solução de gestão de força de trabalho, de gestão de falhas e bilhetes registrados pela Ferramenta de Gerenciamento de Incidentes ou mesmo qualquer outra demanda encaminhada para a CONTRATADA, mesmo que de forma manual, por telefone, e-mail ou sms. Caberá à equipe de Gestão de Segurança receber os bilhetes e fazer todas as análises e tratativas preliminares;

8.2.11.31. A equipe de Gestão de Segurança deverá monitorar as soluções de segurança, tratar alarmes e falhas de segurança, ter capacidades plenas para execução de scripts, guias de diagnóstico, procedimentos, instruções salvas em repositórios, entre outros, escalonando a uma equipe de conhecimento avançado somente quando exauridas todas as possibilidades previstas no seu escopo;

8.2.11.32. A equipe de Gestão de Segurança deverá possuir capacidade de análise e diagnóstico para identificar decorrência de alarmes e identificação do evento causa raiz;

8.2.11.33. A equipe de Gestão de Segurança deverá realizar treinamentos e atualização constante de forma a manter-se atualizada quanto a mudanças de topologia e facilidades da rede, novos procedimentos e fluxos de trabalho, entre outros;

8.2.11.34. A equipe de Gestão de Segurança deverá ainda, além de elaborar relatórios técnicos para as falhas complexas de segurança, preparar documentação de apoio, elaborando

procedimentos, fluxogramas, diagramas de blocos, scripts de configuração, IT (instruções de trabalho) e treinamentos para constantemente preparar e capacitar outros membros da equipe;

8.2.11.35. A equipe de Gestão de Segurança deverá prestar suporte técnico em tempo real, sempre que assim for necessário, para as equipes de campo, em atividades que envolvam atuação local e suporte especializado ou do fabricante;

8.2.11.36. A equipe de Gestão de Segurança será também responsável pela realização periódica de testes em facilidades e recursos das soluções de segurança, a fim de identificar possíveis falhas nestas soluções;

8.2.11.37. A CONTRATADA deverá dispor de serviço de Suporte Operacional, composta por Gestão de Níveis de Serviço (qualidade), Problemas e Plataformas de Monitoramento. Dentre as principais atribuições desta área destacam-se:

8.2.11.37.1. Criar e manter cadastro da plataforma de monitoramento da CONTRATADA;

8.2.11.37.2. Elaborar relatórios de níveis de serviço para apoiar em reuniões envolvendo CONTRATANTE, CONTRATADA e também outros fornecedores;

8.2.11.37.3. Apoiar a Gestão do Comitê de Mudanças.

8.2.11.38. A equipe de Gestão de Níveis de Serviço deverá providenciar insumo e relatórios, sempre que solicitado, para cobrança de SLA, descontos ou glosas nos contratos pagos com outros fornecedores, sempre que falhas nos serviços contratados destas empresas ocorrerem;

8.2.11.39. A CONTRATADA deverá disponibilizar um membro para compor o Comitê de Gestão de Mudanças, que terá por objetivo a análise criteriosa de toda e qualquer mudança no ambiente computacional, definir horários e dias de atuação, aprovar ou negar pedidos, direcionar e orientar fornecedores e a CONTRATANTE de forma a fomentar sempre a evolução e manutenção da rede com impacto zero a serviços e clientes ou, quando a atividade não puder ser feita sem impacto, que este seja o menor possível e seja feito de forma controlada, visível, com conhecimento geral e de forma acompanhada do início ao fim;

8.2.11.40. A participação do profissional exigido no item anterior se reunirá 1 (uma) vez por mês, com duração de 1 (uma) hora sempre em horários compreendidos entre 08:00 e 14:00 horas em dias úteis com a possibilidade de participação remota por vídeo chamada;

8.2.11.41. Para gerir as equipes descritas acima, que comporão o SOC, a CONTRATADA deverá disponibilizar um coordenador, que deverá atuar dentro do SOC ou remotamente em horário comercial e estar disponível para acionamentos em situações necessárias fora do horário comercial;

8.2.11.42. A CONTRATADA deverá executar as atividades remotas de manutenção preventiva e corretiva de acordo com as recomendações dos fornecedores e/ou fabricantes das soluções de segurança presentes na Rede da CONTRATANTE;

8.2.11.43. A CONTRATADA não poderá alegar problemas com outras empresas CONTRATADAS, coligadas e ou operadoras como motivo do não cumprimento das metas dos indicadores operacionais, definidas pela CONTRATANTE, sem as devidas comprovações.

8.2.11.44. A CONTRATADA se compromete a adotar em seus processos operacionais sistemas informatizados de monitoramento das soluções de segurança e gerenciamento do SOC.

8.2.11.45. A CONTRATADA deverá informar imediatamente a CONTRATANTE quando constatar um defeito irrecuperável em qualquer componente das soluções de segurança implantandos na CONTRATANTE.

8.2.11.46. Toda intervenção de caráter preventivo ou corretivo que implique em paralisação de serviço (testes, alteração de configuração, upgrade de software e outros) deve ser efetuada em "janela de manutenção", conforme procedimentos do SOC / CONTRATANTE. Exceções deverão ser previamente aprovadas pela CONTRATANTE;

8.2.11.47. A CONTRATADA deverá transferir o conhecimento das soluções de monitoramento de segurança da informação e gestão do SOC, bem como o treinamento em processos e procedimentos implantados pela CONTRATADA para uma equipe de técnicos da CONTRATANTE;

8.2.11.48. A CONTRATADA deverá disponibilizar pessoal capacitado para mapear e modelar os processos que serão executados no Gerenciamento dos Serviços de TIC fornecidos;

8.2.11.49. A CONTRATADA deverá manter regime de trabalho de forma a não permitir degradação e descontinuidade no atendimento dos serviços, considerando os horários de maior concentração de eventos e incidentes. Deverá apresentar proposta que atenda os requisitos de turno apresentados abaixo e o cumprimento dos indicadores especificados no Termo de Referência:

ATUAÇÃO				
GRUPOS DE ATIVIDADES	**8x5**	**12x5**	**24x7**	**Sobreaviso**
Gestão de Segurança (SOC)				
Gestão de Eventos e Incidentes de Segurança			X	
Gestão de Acessos	X			
Gestão de Segurança de Rede	X			
Suporte Operacional				
Gestão da Plataforma de Gerenciamento	X			
Gestão de Níveis de Serviço (Qualidade)	X			
Comitê de Gestão de Mudanças	X			
Gestor/Coordenador do SOC	**X**			**X**

8.2.12. **A GERÊNCIA DA SOLUÇÃO DE SEGURANÇA DEVE SER PRESTADA PELA CONTRATADA E A FERRAMENTA UTILIZADA DEVE POSSUIR AS SEGUINTES CARACTERÍSTICAS**:

8.2.12.1. Administração da Solução: definição e implantação de políticas de acesso, regras de acesso (NAT, DNAT, Roteamento), filtros de conteúdo, IPS, BGP, GeoIP, AppControl, Botnet, VPN e Gateway Antivírus;

8.2.12.2. Continuar tratando o tráfego corretamente, sem causar interrupção das comunicações, mesmo no caso de queda da comunicação dos equipamentos gerenciados com o serviço de gerência;

8.2.12.3. Gerenciamento de Operação: backup de configuração (regras), aplicação de "patches" e novas atualizações de software, gerenciamento de modificações e análise de logs;

8.2.12.4. Monitoração da Solução: análise de comportamento de usuários, análise de tráfego atípico, alertas e detecção de ataques ou tentativa de invasão, incluindo "Port Scan", "Denial of Services" (DOS), e ataques de autenticação;

8.2.12.5. Ações corretivas: relacionadas a eventos de emergências as quais podem ser uma falha nos equipamentos, uma possível intrusão que possa comprometer a política de segurança da empresa, ou ainda uma não resposta dos equipamentos;

8.2.12.6. Manutenção da Solução: compreende a atualização de software e a manutenção de hardware maximizando o perfeito funcionamento dos dispositivos;

8.2.12.7. Mitigação de incidentes: ações voltadas à solução dos alertas identificados na monitoração (incluindo ataques e intrusões);

8.2.12.8. Emitir, no mínimo, alertas de:

8.2.12.8.1. Ataques de força bruta com e sem sucesso;

8.2.12.8.2. Infecção de equipamentos por vírus;

8.2.12.8.3. Comprometimento / invasão de ativos da rede;

8.2.12.8.4. Realização de ações suspeitas por parte de usuários privilegiados;

8.2.12.8.5. Alertas de operação de serviços, como interrupções e falhas;

8.2.12.8.6. Ataques de negação de serviço (DoS e DdoS);

8.2.12.8.7. Falhas de autenticação;

8.2.12.8.8. Autenticações concorrentes de múltiplas regiões ou cidades com as mesmas credenciais (roubo de identidade);

8.2.12.8.9. Ataques comuns em aplicações WEB, como XSS e SQL injection;

8.2.12.8.10. Atividades de botnets;

8.2.12.9. Identificar, em tempo real e de maneira automatizada, a origem dos eventos de segurança, identificando cidade, estados e países e não somente os endereços IP de origem;

8.2.12.10. Implantação de novas regras de segurança conforme solicitação da contratante;

8.2.12.11. Implantação de novas arquiteturas de segurança conforme solicitação da contratante;

8.2.13. **RELATÓRIOS E VISIBILIDADE**

8.2.13.1. A contratada deve prestar esclarecimentos por escrito a contratante, através de relatórios, sobre eventuais falhas ou interrupções de serviços;

8.2.13.2. Emitir recomendações técnicas para a melhoria da rede e da infraestrutura de segurança da Contratante.

8.2.13.3. Emitir relatórios de incidentes

8.2.13.4. Disponibilizar portal para acesso seguro WEB (através do protocolo HTTPS) disponível na plataforma de acompanhamento;

8.2.13.5. A Contratante deverá possuir credenciais de acesso ao portal Web do ambiente de monitoramento, para acompanhamento em tempo real de indicadores, alarmes e métricas de monitoramento;

8.2.13.6. Dispor de informações gráficas contendo o status, alarmes e métricas dos sistemas monitorados e a ferramenta de relatórios;

8.2.13.7. Possuir visões (Dashboards) pré-configuradas;

8.2.13.8. Permitir a criação de visões (Dashboards) conforme o perfil do usuário;

8.2.13.9. Ser acessível via navegadores de mercado, tais como Microsoft Internet Explorer, Google Chrome e Mozila Firefox, independente do sistema operacional do cliente;

8.2.13.10. O sistema de relatórios deve conter relatórios prontos para uso com temas sobre utilização, capacidade ou disponibilidade;

8.2.13.11. O sistema de relatórios deve possuir capacidade de receber logs de segurança de todos os equipamentos ofertados nesse termo;

8.2.13.12. O sistema de relatórios deve possuir capacidade de fornecer logs on-line por no mínimo 30 (trinta) dias;

8.2.13.13. É de responsabilidade da contratada o backup e armazenamento dos logs pelo período de 01 (um) ano. Está previsto uma geração máxima de 6TB (seis terabytes) de logs bruto por mês.

8.2.13.14. Os relatórios devem conter gráficos, tabelas ou objetos gráficos contendo dados de desempenho;

8.2.13.15. Deve permitir a geração de relatórios para adequação a requerimentos de auditoria para a norma ISO 27001:2005;

8.2.13.16. Deverão ser previstos os seguintes tipos de relatórios:

8.2.13.16.1. Relatório de utilização e filtragem WEB;

8.2.13.16.2. Relatório de ataques e incidentes de segurança;

8.2.13.16.3. Relatório de configurações;

8.2.13.16.4. Relatório com informações de classificação de eventos de segurança;

8.2.13.16.5. Relatório para consultas de eventos, logs e alarmes em tempo real;

8.2.13.16.6. Possibilidade de sumarização dos dados por hora, dia, semana ou mês;

8.2.13.17. Os relatórios devem permitir:

8.2.13.17.1. Acesso discriminado e controlado;

8.2.13.17.2. Emitir nos formatos Excel, CSV e PDF;

8.2.13.17.3. Ser enviados via e-mail;

8.2.13.17.4. Agendamento de relatórios;

8.2.13.17.5. Envio de relatórios pelo sistema de agendamento a usuários internos cadastrados no sistema;

8.2.13.18. Relatórios gerenciais semanais e mensais ou sob demanda de acordo com o período solicitado, incluindo:

8.2.13.18.1. Tempo total de disponibilidade/indisponibilidade de cada ativo e serviço;

8.2.13.18.2. Histórico de alertas para ativos e serviços;

8.2.13.18.3. Histórico de métricas de utilização de recursos, incluindo, canais de comunicações de dados internos e externos (Internet), CPU e Memória;

8.2.13.18.4. Relatório de disponibilidade e performance dos ativos e métricas monitoradas

8.2.13.18.5. Classificação dos eventos de segurança (ataques, reconhecimento, malware, atividades suspeitas, etc.);

8.2.13.18.6. Eventos de segurança por direção (externo, interno e local);

8.2.13.18.7. TOP aplicações mais impactadas;

8.2.13.18.8. TOP origens dos eventos de segurança;

8.2.13.18.9. TOP endereços de destino das ameaças;

8.2.13.18.10. TOP países e cidades de origem das ameaças;

8.2.13.18.11. TOP atacantes, vulnerabilidades, ameaças, alarmes, violações de auditoria;

8.2.13.18.12. Além dos metadados processados pela solução, deve oferecer opção de entrega dos logs originais coletados;

8.3. MANUTENÇÃO DE SERVIÇO, PRAZO DE ATENDIMENTO E PENALIDADES.

8.3.1. A manutenção preventiva ou atualização dos recursos técnicos utilizados na prestação do serviço, quando necessárias interrupções programadas, deverá ser realizada através de comunicação escrita e prévia de no mínimo 7 (dias) dias úteis, a qual deverá ser agendada com a equipe técnica da CONTRATANTE e que será efetuada no período compreendido entre 00:01 e 06:00 horas, horário de Brasília, de domingo e/ou segunda-feira.

8.3.2. A CONTRATADA disponibilizará um número telefônico para abertura de chamados no regime 24x7x365 e também deverá disponibilizar sistema WEB e e-mail.

8.3.3. A CONTRATADA deverá nomear preposto que será o responsável por realizar atendimento em caso de dificuldades na abertura de chamados. Este deverá disponibilizar contato telefônico em horário comercial de segunda a sexta-feira das 08:00h as 17:00h.

8.3.4. O suporte técnico ocorrerá sem qualquer ônus para a Prefeitura de Maceió.

8.3.5. Em caso de intervenção física ou troca de equipamento a atuação da contratada deverá ser on-site.

8.3.6. Os prazos para a solução dos incidentes são contados em dias corridos, ou seja, 24x7 (vinte e quatro horas, sete dias por semana).

8.3.7. LOTE 1 – ITEM 01 - LINK DE TRÁFEGO IP COM CONECTIVIDADE A INTERNET E SUPORTE A BGP

8.3.7.1. O prazo de atendimento para resolução de possíveis indisponibilidades no uso dos serviços, deverá abranger três níveis de solução definitiva, quais sejam:

8.3.7.1.1. **Severidade Alta**: Esse nível de severidade é aplicado quando há a indisponibilidade total no uso dos serviços;

Solução Definitiva: ALTA
<u>Indisponibilidade Total do Serviço</u>:
Prazo Solução Definitiva: 2 (duas) horas

8.3.7.1.2. Entende-se indisponibilidade total, a prestação de serviços inaproveitáveis, conforme os seguintes parâmetros:

8.3.7.1.2.1. Perda do circuito contratado;

8.3.7.1.2.2. Latência do circuito contratado ultrapassar 90 MS (noventa milissegundos);

8.3.7.1.3. **Severidade Média**: Esse nível de severidade é aplicado quando há falha, simultânea ou não, no uso dos serviços, estando ainda disponíveis, porém apresentando problemas;

Solução Definitiva: MÉDIA
<u>Serviços disponíveis, mas apresentando conectividade intermitente</u>:
Prazo Solução Definitiva: 4 (quatro) horas

8.3.7.1.4. Entende-se indisponibilidade, a prestação de serviço fora dos Níveis de Serviço, conformes os seguintes parâmetros:

8.3.7.1.4.1. Perda do circuito contratado entre 0,5% (zero vírgula cinco por cento) e 10% (dez por cento) de minutos de um dia;

8.3.7.1.4.2. Latência do circuito contratado de 80 MS (oitenta milissegundos) até 90 MS (noventa milissegundos)

8.3.7.1.5. **Severidade Baixa**: Esse nível de severidade é aplicado para problemas que não afetem o desempenho e disponibilidade dos serviços, bem como para atualizações de software e solicitações de alteração nas configurações dos roteadores e IPS.

Solução Definitiva: BAIXA
<u>Serviços disponíveis e atualização</u>:
Prazo Solução Definitiva: 4 (quatro) dias úteis

8.3.7.1.6. Prestação de Esclarecimentos Técnicos: é aplicado quando a CONTRATADA solicitar formalmente esclarecimentos técnicos relativos às ocorrências, ao uso e ao aprimoramento dos serviços.

Prazo de Resposta
<u>Esclarecimentos técnicos</u>:
Prazo Solução Definitiva: 4 (quatro) dias úteis

8.3.7.2. Será considerado como prazo de solução definitiva, o tempo decorrido entre a abertura do chamado técnico - efetuado por equipe técnica da Prefeitura de Maceió e a efetiva recolocação dos serviços em seu pleno estado de funcionamento;

8.3.7.3. A contagem do prazo de solução definitiva de cada chamado iniciar-se-á a partir da abertura do chamado, em um dos canais de atendimento disponibilizados pela CONTRATADA, até o momento da comunicação da resolução definitiva do problema e o aceite pela equipe técnica da Prefeitura de Maceió;

8.3.7.4. A glosa será contada a partir do tempo decorrido e identificado no item “Prazo Solução Definitiva” de acordo com a severidade prevista.

8.3.7.5. Depois de concluído o chamado, a CONTRATADA comunicará o fato à equipe técnica da Prefeitura de Maceió e solicitará autorização para o fechamento do mesmo. Caso a Prefeitura de Maceió não confirme que o problema foi de fato resolvido, o chamado deverá ser reaberto até que seja efetivamente solucionado. Neste caso, a Prefeitura de Maceió fornecerá as pendências relativas ao chamado aberto;

8.3.7.6. A relação de chamados deverá estar disponível nos relatórios encaminhados mensalmente ao fiscal do contrato, atendendo aos seguintes tópicos:

8.3.7.6.1. Chamados Abertos no Período: listagem de todas as ocorrências registradas e ainda não solucionadas, durante o mês, com a indicação das ações já tomadas pela CONTRATADA;

8.3.7.6.2. Chamados Concluídos no Período: listagem de todas as ocorrências registradas e solucionadas, durante o mês, com a indicação das ações tomadas pela CONTRATADA.

8.3.7.7. O descumprimento dos prazos de atendimento implicará a aplicação de glosas conforme Tabela abaixo:

Tabela de aplicação de Glosas

Resultado esperados e níveis de qualidade exigidos	Unidade de cálculo	Fórmula de cálculo da glosa	Limite da glosa
1 – Alta	1 h	NHAT * 0,50% * VMF	10% da VMF
2 – Média	1 h	NHAT * 0,25% * VMF	10% da VMF
3 – Baixo	1 h	NHAT * 0,05% * VMF	10% da VMF
4 – Esclarecimentos sobre incidentes	1 d	NDAT * 0,6% * VMF	10% da VMF

Onde:
VMF: Valor mensal da fatura;
NHAT: número de horas decorridas após o término de atendimento.
NDAT: número de dias decorridos após o término de atendimento.

8.3.8. **LOTE 01 – ITEM 02 - SOLUÇÃO DE SEGURANÇA**

8.3.8.1. O Sistema WEB para este item deverá registrar todos os chamados com data e hora da abertura e fechamento, número, informações de contato do requerente e severidade. De forma que seja possível que a CONTRATANTE possa mensurar os prazos definidos no **item 8.3.8**.

8.3.8.2. A contratada deve respeitar os seguintes Níveis Mínimos de Serviço, de acordo com o nível de severidade:

8.3.8.3. No caso da necessidade de substituição de equipamentos da solução de segurança o SLA é de 24 horas;

8.3.8.4. SLO (Service Level Objectives - Objetivos de Nível de Serviço) para serviços gerenciados;

8.3.8.5. Os SLO's serão estabelecidos de acordo com a severidade do incidente ocorrido, conforme descrito no quadro abaixo:

Incidentes de Serviço	Definição
Crítico	Evento que gera indisponibilidade dos serviços de um ativo classificado como crítico
Alto	Evento que degrada os serviços de um ativo classificado como crítico ou que gera indisponibilidade dos serviços de um ativo não crítico
Médio	Evento que degrada os serviços de um ativo classificado como não crítico
Baixo	Evento que não afeta os serviços

8.3.8.6. Abaixo os tempos de atendimento:

Definição	Crítico	Alto	Médio	Baixo
Tempo de atendimento a partir da comunicação do cliente até a atribuição do chamado a um analista do SOC (Security Operation Center)	15 min.	30 min.	1h	2h
Tempo de resposta a partir da comunicação do cliente até que o SOC (Security Operation Center) faça o primeiro diagnóstico	1h	1,5h	3h	6h
Tempo de resolução a partir da comunicação do cliente até que o SOC (Security Operation Center) comunique a resolução do mesmo	4h	6h	12h	24h
Tempo de notificação desde a detecção da falha até que seja comunicado ao cliente	15 min	30 min	1h	1h

8.3.8.1. O nível dos serviços prestados será medido mensalmente com base nas seguintes métricas:

MÉTRICA	SLA	APLICA-SE A
Tempo de Atendimento	95%	Consultas, requisições e incidentes
Tempo de Resposta	95%	Consultas, requisições e incidentes
Tempo de Notificação	95%	Consultas, requisições e incidentes
Tempo de Resolução	95%	Consultas e requisições

8.3.8.2. A Multa, na forma prevista neste instrumento convocatório, no contrato e quando do não cumprimento de suas obrigações, serão aplicadas conforme as disposições a seguir:

ITEM	INCIDÊNCIA	MULTA
O Não cumprimento de atendimento dos Níveis Mínimos de Serviço	90 a 95% de ocorrência mensal	2 % do valor mensal do serviço
	85 a 89,99% de ocorrência mensal	10 % do valor mensal do serviço
	80 a 84,99% de ocorrência mensal	30 % do valor mensal do serviço
	Abaixo de 79,99% de ocorrência mensal	5 % do valor total do contrato
	Reincidência abaixo de 79,99% de ocorrência mensal	10% do valor total do contrato

8.3.8.3. Cálculo do SLA por registro de ocorrência:

SLA em % = (SLA em Minutos / Tempo para resolução em Minutos) x 100

8.3.8.4. A CONTRATADA ficará sujeita às sanções administrativas previstas na Lei n.º 8.666/93 e suas alterações, no Decreto n.º 5.450/2005 e suas alterações e na Lei n.º 10.520/2002, a ser aplicada pela autoridade competente da Prefeitura de Maceió, conforme a gravidade do caso,

assegurado o direito a ampla defesa, sem prejuízo do ressarcimento dos danos ou prejuízos porventura causados à Administração e das cabíveis cominações legais.

8.3.8.5. Além das penalidades descritas acima, O CONTRATANTE poderá aplicar à CONTRATADA as seguintes penalidades, garantida ampla e prévia defesa em processo administrativo:

8.3.8.6. Multa moratória de 0,5% sobre o valor total dos serviços contratados, por hora ou fração da inoperância ou indisponibilidade, no caso de atraso injustificado ao prazo estipulado para resolução dos problemas de inoperância dos serviços contratados, conforme Plano Geral de Metas de Qualidade para o SMP (PGMQ – SMP), limitada ao percentual máximo de 10% do valor anual dos serviços;

8.3.8.7. Multa de 10% sobre o valor total do serviço, em caso de descumprimento total ou parcial das obrigações dispostas neste Termo de Referência;

8.3.8.8. Impedimento de licitar e contratar com a União, Estados, Distrito Federal e Municípios, e descredenciamento no SICAF por até 5 (cinco) anos.

8.3.8.9. As inoperâncias ou indisponibilidades dos serviços, no todo ou em parte, que não sejam de responsabilidade da PREFEITURA DE MACEIÓ, deverão gerar descontos na fatura correspondente aos serviços não prestados proporcionais ao tempo da sua não prestação, acrescido, quando for o caso, das penalidades estipuladas;

8.3.8.10. Se o motivo ocorrer por comprovado impedimento ou reconhecida força maior, devidamente justificado e aceito pela Administração da SEMGE, a CONTRATADA ficará isenta das penalidades mencionadas.

8.3.8.11. A sanção estabelecida no **item 8.3.8.8** poderá ser aplicada à CONTRATADA juntamente àquela prevista no **item 8.3.8.7**, descontando-a dos pagamentos a serem efetuados.

8.3.8.12. Os atos administrativos de rescisão contratual e de aplicação das sanções serão publicados resumidamente no Diário Oficial do Município de Maceió.

8.3.8.13. Da aplicação das penalidades previstas caberá recurso no prazo de 05 (cinco) dias úteis a partir da data da intimação.

8.4. QUALIFICAÇÃO TÉCNICA

8.4.1. Além dos documentos exigidos no edital, referentes à regularidade com Seguridade Social, FGTS, Fazenda Federal e ao cumprimento no disposto no art. 27, inciso V, da Lei no 8.666/1993, deverá o CONTRATANTE apresentar no momento da homologação da licitação:

LOTE1 ITEM 1	LOTE 1 – ITEM 2	LOTE 2 – ITEM 4
Pelo menos 1 (um) atestado de capacidade técnica, fornecido por pessoa jurídica de direito público ou privado, comprovando que prestou, serviços de comunicação de dados para acesso a Internet, incluindo instalação e manutenção.	Pelo menos 1 (um) atestado de capacidade técnica, fornecido por pessoa jurídica de direito público ou privado, comprovando que prestou, serviços de segurança de infraestrutura lógica com gerência.	Pelo menos 1 (um) atestado de capacidade técnica, fornecido por pessoa jurídica de direito público ou privado, comprovando que prestou, serviços de comunicação de dados para acesso a Internet, incluindo instalação e manutenção.

Apresentar documento emitido pela ANATEL que comprove ser a PROPONENTE autorizada a prestar os serviços SCM (Serviço de Comunicação Multimídia).	Apresentar projeto técnico da solução proposta, onde constem as informações dos equipamentos utilizados, com marca e modelo ofertado.	Apresentar documento emitido pela ANATEL que comprove ser a PROPONENTE autorizada a prestar os serviços SCM (Serviço de Comunicação Multimídia).
Declarar que possui canais dedicados e redundantes com no mínimo 03 (três) AS (Autonomous System – Sistemas Autônomos) Nacionais em velocidade não inferior a 1 Gbps;	Declarar sua infraestrutura de centro de gerência de redes, especificando endereço e condições para garantia de funcionamento 24x7, com no mínimo um Grupo Motor Gerador e um No-Break ou um site backup.	Declarar que possui canais dedicados e redundantes com no mínimo 03 (três) AS (Autonomous System – Sistemas Autônomos) Nacionais em velocidade não inferior a 1 Gbps.
Os equipamentos e a camada de ligação de dados (enlaces) disponibilizados pela CONTRATADA deverão possuir certificação em conformidade com as normas e diretrizes estabelecidas através dos órgãos competentes ou entidades autônomas - ABNT (Associação Brasileira de Normas Técnicas) e ANATEL (Agência Nacional de Telecomunicações), e entidades de padrões reconhecidas internacionalmente – ITU-T (*International Telecommunication Union*), ISO (*International Standardization Organization*), IEEE (*Institute of Electrical and Electronics Engineers*), EIA/TIA (*Electronics Industry Alliance and Telecomumnication Industry Association*).	01(um) profissional certificado/treinado na solução de gerenciamento / monitoramento proposta para a prestação dos serviços de gerenciamento / monitoramento, pelo fabricante do equipamento. Caso não possua em seu quadro de funcionários, deverá apresentar compromisso de contratação no qual o profissional indicado acima pela licitante, para fins de comprovação de capacitação técnica, declare que participará a serviço da licitante, dos serviços objeto deste processo licitatório.	Os equipamentos e a camada de ligação de dados (enlaces) disponibilizados pela CONTRATADA deverão possuir certificação em conformidade com as normas e diretrizes estabelecidas através dos órgãos competentes ou entidades autônomas - ABNT (Associação Brasileira de Normas Técnicas) e ANATEL (Agência Nacional de Telecomunicações), e entidades de padrões reconhecidas internacionalmente – ITU-T (*International Telecommunication Union*), ISO (*International Standardization Organization*), IEEE (*Institute of Electrical and Electronics Engineers*), EIA/TIA (*Electronics Industry Alliance and Telecomumnication Industry Association*).

	Comprovação de que o LICITANTE, está qualificado a executar os serviços de Instalação e configuração das soluções propostas, através de: Contrato de representação comercial com o fabricante, páginas WEB de domínio público ou outro documento que comprove a aptidão da licitante com as soluções do fabricante.	

8.4.2. Todas as Declarações apresentadas deverão explicitamente fazer referência a este processo licitatório;

8.4.3. Estarão sujeitos à diligência por parte da comissão de licitação, que poderá averiguar através de visita técnica, a autenticidade das informações. Se durante esse processo, for constatada fraude em qualquer um dos documentos, a licitante envolvida estará automaticamente desclassificada do processo licitatório em questão, além de estar sujeita às penalidades da lei.

8.4.4. Os atestados deverão obrigatoriamente conter os dados do órgão declarante e da pessoa que assina, possibilitando sua identificação e contato.

8.4.5. A(s) Declaração(ões) e o(s) atestado(s) de capacidade técnica que não esteja(m) na língua portuguesa, deverá(ão) vir acompanhado(s) de tradução feita por tradutor juramentado.

9. DESCRIÇÃO DO LOTE 1 – ITEM 3 - BLOCOS DE IP (BLOCO IPV4 /24 E BLOCO IPV6 /48)

9.1. Fornecer um bloco de IPv4 público com máscara /24.

9.2. Fornecer um bloco de IPV6 público com máscara /48.

10. DESCRIÇÃO DO LOTE 2 – ITEM 5 - BLOCOS DE IP (BLOCO IPV4 /24 E BLOCO IPV6 /48)

10.1. Fornecer um bloco de IPv4 público com máscara /24.

10.2. Fornecer um bloco de IPV6 público com máscara /48.

11. OBRIGAÇÕES DAS PARTES

11.1. DA CONTRATADA

11.1.1. Será de responsabilidade da CONTRATADA a prestação dos serviços constante deste TR, com obediência a todas as condições estabelecidas em lei, no Edital e no Contrato, bem como as oferecidas em sua proposta;

11.1.2. A CONTRATADA responsabiliza-se pelas despesas necessárias à execução dos serviços. Todo o pessoal utilizado na execução dos serviços deverá ser vinculado à CONTRATADA, responsável, única e exclusivamente, pelo pagamento de sua remuneração, assim como por todos e quaisquer encargos trabalhistas, previdenciários e recolhimento dos tributos e taxas incidentes, fiscais e comerciais resultantes da execução dos mesmos;

11.1.3. Responder, integralmente, por perdas e danos que vier a causar ao CONTRATANTE ou a terceiros em razão de ação ou omissão, dolosa ou culposa, sua ou de prepostos, independentemente de outras cominações contratuais ou legais a que estiver sujeita;

11.1.4. Arcar com despesas decorrentes de qualquer infração, seja qual for, desde que praticada por seus técnicos durante a execução dos serviços;

11.1.5. Prestar as informações e os esclarecimentos que venham a ser solicitados pelo CONTRATANTE em até dois dias úteis, por intermédio do consultor designado para acompanhamento do contrato, a contar de sua solicitação, sobre eventuais atos ou fatos noticiados que se refiram a CONTRATADA, independente de solicitação;

11.1.6. Levar, imediatamente, ao conhecimento do Gestor do Contrato, qualquer fato extraordinário ou anormal que ocorrer na execução do objeto contratado, para adoção das medidas cabíveis;

11.1.7. Assumir inteira responsabilidade técnica e operacional do objeto contratado, não podendo, sob qualquer hipótese, transferir a outras empresas a responsabilidade por problemas de funcionamento do serviço;

11.1.8. Caso o problema de funcionamento do serviço detectado tenha a sua origem fora do escopo do objeto contratado, a CONTRATADA repassará as informações técnicas com a devida análise fundamentada que comprovem o fato para o CONTRATANTE, sem qualquer ônus para a mesma;

11.1.9. Garantir sigilo e inviolabilidade das conversações realizadas por meio do serviço desta contratação, respeitando as hipóteses e condições constitucionais e legais de quebra de sigilo de telecomunicações;

11.1.10. Prestar os serviços dentro dos parâmetros e rotinas estabelecidos, em observância às recomendações aceitas pela boa técnica, normas e legislação;

11.1.11. Implantar, de forma adequada, a supervisão permanente dos serviços, de forma a obter uma operação correta e eficaz, prestando os serviços de forma meticulosa e constante, mantendo sempre em perfeita ordem a execução dos mesmos;

11.1.12. Manter, durante toda a execução do contrato, compatibilidade com as obrigações a serem assumidas, todas as condições de habilitação e qualificação exigidas na licitação;

11.1.13. Não transferir a outrem, no todo ou em parte, o objeto do presente contrato, sem prévia e expressa anuência do CONTRATANTE;

11.1.14. É vedado à CONTRATADA, sob pena de rescisão contratual, caucionar ou utilizar o contrato para qualquer operação financeira, sem a prévia e expressa anuência do CONTRATANTE;

11.1.15. Assumir a responsabilidade por todas as providências e obrigações estabelecidas na legislação específica de acidentes do trabalho, quando, em ocorrência da espécie, forem vítimas os seus empregados no desempenho dos serviços ou em conexão com eles, ainda que ocorridos nas dependências do CONTRATANTE;

11.1.16. Assumir todos os encargos de possível demanda trabalhista, civil ou penal, relacionadas à execução dos serviços, originariamente ou vinculada por prevenção, conexão ou contingência;

11.1.17. Responder pelos danos causados diretamente ao CONTRATANTE, ou a terceiros, decorrentes de sua culpa ou dolo, quando da execução dos serviços, não excluindo ou reduzindo essa responsabilidade quanto à fiscalização ou ao acompanhamento pelo CONTRATANTE.

11.2. **DA CONTRATANTE**

11.2.1. Convocar a adjudicatária, dentro do prazo de eficácia de sua proposta, para assinatura da Ata;

11.2.2. Convocar a adjudicatária, dentro do prazo de validade da ata, para assinatura do contrato;

11.2.3. Publicar os extratos da Ata de Registro de Preços e contrato, na forma da Lei.

11.2.4. Emitir Nota de Empenho/Contrato e/ou Ordem de Fornecimento, a medida da Contratação.

11.2.5. Exigir o cumprimento de todas as obrigações assumidas pela empresa vencedora, de acordo como os termos deste documento e do contrato.

11.2.6. Reservar local apropriado para o recebimento do objeto deste documento.

11.2.7. Ter pessoal disponível para o recebimento do objeto no horário previsto neste documento.

11.2.8. Receber o objeto de acordo com as especificações descritas neste documento.

11.2.9. Atestar as Notas Fiscais/Faturas que estejam corretamente preenchidas e em conformidade com os quantitativos solicitados e os serviços restados, e efetuar os pagamentos à beneficiária.

11.2.10. Comunicar à Contratada, por escrito, sobre imperfeições, falhas ou irregularidades verificadas no objeto fornecido, para que seja substituído, reparado ou corrigido, sem prejuízo das penalidades cabíveis.

11.2.11. Acompanhar e fiscalizar a execução do Contrato, por intermédio de representante especialmente designado.

11.2.12. Aplicar as penalidades regulamentares contratuais.

11.2.13. Permitir o livre acesso dos empregados da CONTRATADA às instalações onde serão executados os serviços a partir de agendamento prévio, desde que estejam devidamente credenciados, portando crachá de identificação e exclusivamente para execução dos serviços;

11.2.14. Prestar as informações e os esclarecimentos que venham a ser solicitados pelos empregados da CONTRATADA;

11.2.15. Proceder ao acompanhamento técnico da prestação dos serviços e fiscalizar o cumprimento das obrigações assumidas pela CONTRATADA, inclusive quanto à continuidade da prestação dos serviços que, ressalvados os casos de força maior, justificados e aceitos pelo CONTRATANTE, não deve ser interrompida;

11.2.16. Assegurar-se da boa prestação dos serviços, verificando sempre o seu bom desempenho;

11.2.17. Assegurar-se de que os preços contratados estão compatíveis com aqueles praticados no mercado pelas demais prestadoras dos serviços objeto deste ajuste, de forma a garantir que continuem a ser os mais vantajosos para o CONTRATANTE;

11.2.18. Controlar as ligações realizadas e documentar as ocorrências havidas;

11.2.19. Dar ciência à CONTRATADA imediatamente sobre qualquer anormalidade que verificar na execução dos serviços;

11.2.20. Relacionar as dependências das instalações físicas, bem, ainda, os bens de sua propriedade colocados à disposição da CONTRATADA durante a execução dos serviços, com a indicação do estado de conservação, se for o caso;

11.2.21. Atestar a execução do objeto do contrato por meio do Fiscal do Contrato;

11.2.22. Efetuar pagamento à CONTRATADA de acordo com as condições de preço e prazo estabelecidas no contrato, os serviços e as aquisições efetivamente realizadas.

12. CONDIÇÕES GERAIS

12.1. Deverão estar inclusos no preço proposto todos os equipamentos necessários para a implementação da rede objeto do edital, incluindo equipamentos, roteadores, obras de adequação, etc;

12.2. Deverão estar inclusos no preço proposto, os custos de manutenção de todos os circuitos e equipamentos;

12.3. A CONTRATADA poderá optar pela subcontratação do serviço do Lote 1 item 2. A CONTRATADA permanecerá como única e exclusiva responsável pelo serviço perante o CONTRATANTE.

12.4. Visando aumentar a competitividade, serão aceitas participações de empresas em consórcio, de acordo com o art.33, seus incisos e parágrafos, e demais alterações da lei 8.666/93.

13. DA VIGÊNCIA

13.1. O prazo da contratação será de 30 (trinta) meses, podendo ser renovado, por sucessivos períodos, caso haja interesse das partes, até o limite de 60 (sessenta) meses, nos termos do art. 57, II, da Lei 8.666/93.

14. TIPO DE CONTRATAÇÃO

14.1. A contratação se dará por meio de CONTRATO com a SECRETARIA MUNICIPAL DE GESTÃO, CNPJ: 18.113.955/0001-10.

15. DO EQUILÍBRIO ECONÔMICO-FINANCEIRO CONTRATUAL

15.1. Fica proibido o reajuste do valor do contrato no interregno de 12 (doze) meses, exceto nas hipóteses decorrentes do Art. 65, alínea “d” do inciso II da Lei Federal 8.666/93, devidamente comprovado.

15.2. Em caso de reajuste, após o período mencionado no subitem acima, será utilizado como base o IPCA (Índice Preços ao Consumidor Amplo).

15.3. Toda revisão deverá incidir a partir da data em que for protocolado o pedido.

15.4. A Administração poderá suprimir ou acrescer o objeto do Contrato em até 25% (vinte e cinco por cento) do seu valor inicial atualizado, a seu critério exclusivo, de acordo com o disposto no art. 65, § 1º, da Lei Federal nº 8.666/1993.

16. DA GARANTIA CONTRATUAL

16.1. A Contratada prestará, no ato da assinatura do contrato, garantia de execução correspondente a 1% (um por cento) do valor do Contrato, em uma das modalidades previstas no §1º do art. 56 da Lei Federal n.º 8.666, de 1993, a ser escolhida pela Contratada.

_____
Reinaldo Braga da Silva Junior
Secretário de Gestão / SEMGE

_____
Felipe Gomes de Oliveira
Coordenador Geral de Controle e Acompanhamento de Serviços / SEMGE

_____
Jacson Luis Alves da Silva
Coordenador Geral de Contratação de Serviços e Aquisição de Produtos / SEMGE

_____
João Geraldo de Oliveira Lima
Diretor de TI/SEMGE

ANEXO A

PROPOSTA DE PREÇO

LOTE 01

LOTE	ITEM	SERVIÇOS	VELOCIDADE	QUANT.	PAGAMENTO	VALOR UNITÁRIO	VALOR MENSAL	VALOR TOTAL (12 MESES)
01	01	Link de tráfego IP para internet com velocidade de 1 Gbps com suporte a BGP.	1 Gbps *Full*	1	MENSAL			
	02	Solução de segurança e gerência.		1	MENSAL			
	03	Lote 1 - Blocos de IP (Bloco IPv4 /24 e Bloco IPv6 /48).		1	MENSAL			
02	03	Link de tráfego IP para internet com velocidade de 1 Gbps com suporte a BGP.	1 Gbps *Full*	1	MENSAL			
	04	Lote 2 - Blocos de IP (Bloco IPv4 /24 e Bloco IPv6 /48).		1	MENSAL			

ANEXO B

TERMO DE VISITA TÉCNICA

(Usar Papel Timbrado da Empresa)

TERMO DE VISTÓRIA TÉCNICA

Declaramos, sob pena da lei, que a empresa _____, CNPJ nº. _____, com endereço na Avenida / Rua _____, realizou, nesta data, Vistoria Técnica em todas as instalações tecnológicas e de infraestrutura da Prefeitura de Maceió e de seus endereços listados no(s) LOTE(s): _____, não tendo nada a questionar a posteriori sobre as especificações técnicas e condições pertinentes ao OBJETO deste Termo de Referência.

Maceió (AL), ____ de _____ de 2020.

Responsável Técnico: _____
Documento de Identidade: _____
Assinatura: _____

Visto:

_____
Responsável pela DTI SEMGE