TERMO DE REFERÊNCIA

1 OBJETO

1.1. O presente Termo de Referência estabelece as especificações, condições e requisitos para a **"Contratação de empresa para prestação de serviços de fornecimento e instalação de LINK DE INTERNET DEDICADO de 500Mbps com segurança incluída, via fibra óptica, incluindo instalação, manutenção e serviços técnicos",** para atender a Prefeitura municipal de Itaboraí, secretarias municipais e suas dependências.

1.2. O critério de seleção das propostas será o menor preço por item.

2. DAS ESPECIFICAÇÕES

2.1. DESCRIÇÃO DOS SERVIÇOS

Item	Descrição	UNIDADE	Quantidade
1	Link de acesso à Internet com largura de banda garantida de 500 Mbps, simétricos, com tráfego sem limite de quantidade e nem restrição de dados trafegados, porta lógica ou serviço, com segurança incluída.	Serviço	01
2	Link backup de acesso à Internet com largura de banda garantida de 500 Mbps, simétricos, com tráfego sem limite de quantidade e nem restrição de dados trafegados, porta lógica ou serviço, com segurança incluída.	Serviço	01

a Considerando a necessidade de alta disponibilidade de acesso, justifica-se a contratação de dois links de internet com rotas e caminhos distintos para garantir a continuidade e a segurança dos serviços de rede em caso de falha ou interrupção no link principal.

b O item 1, referente ao link principal, será utilizado para a operação regular e contínua das atividades da instituição. Já o item 2, que trata do link de backup, deverá possuir infraestrutura independente, com rotas e caminhos de rede diferentes, preferencialmente em CPDs (Centros de Processamento de Dados) distintos, de forma a assegurar a redundância e a alta disponibilidade da conexão à internet.

c A utilização de rotas e caminhos distintos evita que ambas as conexões sejam afetadas

simultaneamente por falhas em um único ponto da rede, proporcionando maior resiliência, segurança e mitigando riscos de perda de conectividade em situações de falhas técnicas, desastres naturais ou ataques cibernéticos.

d O link de backup (item 2) não será destinado exclusivamente a emergências ou falhas do link principal, mas deverá ser utilizado de forma contínua para garantir a otimização da distribuição de tráfego de dados, equilíbrio de carga e alta disponibilidade da rede. Assim, o link de backup deverá ser configurado para operar de maneira simultânea ao link principal, com capacidade para suportar o tráfego diário de dados da instituição, sem depender exclusivamente de uma falha ou indisponibilidade do link primário. A utilização contínua do link de backup é essencial para garantir que a infraestrutura de rede se mantenha estável e eficiente, mesmo durante picos de demanda, sem impactar a qualidade do serviço.

2.1.1 PROVA DE CONCEITO

a . Caso a licitante provisoriamente vencedora do **item 1** seja a mesma provisoriamente vencedora do **item 2**, a licitante deverá, como condição para a execução do contrato, ser submetida a uma **Prova de Conceito (PoC)** em até 3 dias úteis, após a solicitação feita pelo agente de contratação, para comprovar que os links contratados atendem aos requisitos de independência e redundância exigidos.

b . A PoC tem como objetivo demonstrar que os **links** atendem aos requisitos de independência e redundância. A demonstração da PoC precisa ser feita para garantir que os links de internet possuam infraestruturas físicas e lógicas distintas, o que exige que a licitante provisoriamente vencedora possua em fase de planejamento dessa infraestrutura na fase de validação da proposta . A licitante deverá disponibilizar toda a infraestrutura necessária à realização da prova de conceito, incluindo equipamentos e insumos, sem custo adicional para a Administração, sendo esta etapa de caráter eliminatório para avaliação da viabilidade da solução proposta.**"**A PoC consistirá na demonstração, em ambiente controlado e com a presença de representantes da licitante, de que os dois links possuem **infraestruturas físicas e lógicas distintas**, com **rotas e caminhos independentes**, de forma que a falha em um dos links não comprometa a operação do outro. A licitante deverá apresentar evidências de que:

. **Rotas Físicas e Lógicas Distintas**: Os links de internet (principal e backup) são conectados por **infra estruturas distintas**, com **caminhos geograficamente separados** e que não compartilham os mesmos pontos de interconexão ou equipamentos críticos, como switches, roteadores ou pontos de distribuição de dados.

Centros de Processamento de Dados (CPDs) Independentes: Os links devem ser entregues a partir de **CPDs separados**, garantindo que falhas em um local específico (como quedas de energia ou falhas de equipamentos) não impactem ambos os links simultaneamente.

Rotas de Tráfego Redundantes e Independentes: As rotas de tráfego de dados de ambos os links não podem utilizar os mesmos caminhos ou fornecedores de rede. A licitante deverá demonstrar que, mesmo que um dos links apresente falhas, o outro continuará operando sem interrupção.

Caso a licitante provisoriamente vencedora não comprove, na Prova de Conceito (PoC), que os links atendem aos requisitos de independência e redundância, ela deverá ser inabilitada para o item 2 conforme análise da SEMFAT.

2.1.2 CONDIÇÕES DE EXECUÇÃO

a . A CONTRATADA deverá disponibilizar toda a infraestrutura de telecomunicações (equipamentos e insumos) necessária ao pleno funcionamento dos serviços contratados, sem custo adicional ao CONTRATANTE;

b . A CONTRATADA deverá se encarregar de prover o meio físico de interligação entre a sua rede e a

rede do CONTRATANTE, atendendo aos parâmetros definidos nesta especificação, ficando este serviço sob sua inteira responsabilidade;

c . A administração e manutenção desses equipamentos serão de inteira responsabilidade da CONTRATADA, devendo obedecer aos níveis de qualidade exigidos na presente contratação;

d . A solução adotada pela CONTRATADA deverá atender a todas as normas técnicas exigidas pelos órgãos públicos competentes e responsáveis pela regulamentação, controle e fiscalização do meio físico, da conexão lógica, do tipo de transmissão, da velocidade de tráfego, da faixa de frequência e largura de banda utilizada;

e . A CONTRATADA deverá ter rede instalada e com um POP – Ponto Operacional Provedor no Município, para que viabilize os prazos de execução dos serviços;

f . A CONTRATADA deverá possuir pelo menos dois (02) fornecedores distintos do Link de dados, fornecidos por rotas diferentes, na topologia de anel, garantindo assim o fornecimento ininterrupto da solução de dados para a PMI;

g . A CONTRATADA deverá dispor e fornecer a CONTRATANTE ferramentas automatizadas de Gerência Proativa – com implantação de um NOC (Network OperationCenter) para gerir e monitorar a rede de dados e o Link de Internet da Prefeitura de Itaboraí em escala de 24/7/365 (24h por dia, sete dias na semana e 365 dias no ano), em que a gerência e as regras do firewall deverão ser compartilhadas com os especialistas de TI da Prefeitura de Itaboraí;

h . A CONTRATADA deverá apresentar a CONTRATANTE os softwares de Monitoramento e emissão de relatórios técnicos e gerenciais utilizados no processo; a CONTRATANTE dará preferência ao uso de ferramentas de domínio público devido a necessidade de implementação de uma Política de Uso de Software Livre), em que a gerência e as regras do firewall deverão ser compartilhadas com os especialistas de TI da Prefeitura de Itaboraí;

i . O backbone da CONTRATADA deverá prever rotas alternativas em sua estrutura, ao menos do ponto de vista lógico, de modo que eventuais falhas em equipamentos ou linhas de dados não afetem a disponibilidade do sistema;

j . Em caso de queda do backbone principal, deverá rotear o fluxo para conexões backup, em um prazo máximo de 01 (uma) hora, de forma transparente para CONTRATANTE;

k . O Provedor deverá dispor de recursos de gerência e supervisão para o circuito;

l . O Provedor deverá fornecer um range sequencial de uma sub-rede com no mínimo 10 (dez) endereços IP válidos para a Rede Mundial, a fim de permitir a conexão efetiva dos sistemas à Internet, e vice-versa, atendendo a todos os requisitos de segurança e de aplicações definidos para essa conexão;

m . Pela natureza corporativa da atividade do CONTRATANTE, o serviço, objeto da presente contratação, deverá propiciar segurança física dos dados. Entende-se por segurança física a proteção contra o acesso não autorizado ao link e dispositivos do Provedor responsáveis pelo transporte e encaminhamento dos dados;

n . A CONTRATADA deverá prover, no âmbito do serviço de segurança do link de internet, uma solução para identificação, tratamento e mitigação transparente de ataques do tipo negação de serviço (DoS – DenialofService) e do tipo negação de serviço distribuído (DDoS – distributedDenialofService).

o . A CONTRATADA deve possuir infraestrutura de mitigação com capacidade para conter ataques de grande volume, sendo eles de origem nacional ou internacional. Deve também possuir pelo menos dois (2) centros de limpeza, cada um com capacidade de mitigação de 40 Gbps de tráfego “sujo” destino à contratante.

p . O ataque deverá ser mitigado na estrutura da CONTRATADA, separando o tráfego legítimo do malicioso, de modo que os serviços de Internet providos pelo CONTRATANTE continuem disponíveis aos seus usuários.

q . A solução deverá ser capaz de mitigar e entregar, conforme largura de banda CONTRATADA, até 60 Gbps de tráfego limpo diretamente no Data Center da CONTRATANTE.

r . Deve suportar uma quantidade mínima de trinta (30) prefixos IP "/24" protegidos.

s . A CONTRATADA deverá prover o serviço de mitigação sem limitação de tempo de duração do ataque e com quantidade ilimitada de eventos de ataque ao longo da vigência contratual. Ademais, não deve existir restrição quanto ao tempo mínimo de intervalo entre mitigações.

t . A solução deverá ser capaz de prover proteção, no mínimo, contra os seguintes ataques que explorem a capacidade dos canais de comunicação (ataques volumétricos): UDP Flood, ICMPFlood, DNS Amplification, NTP Amplification e SSDP Amplification.

u . A solução deverá ser capaz de prover proteção, no mínimo, contra os seguintes ataques que explorem a capacidade de processamento de requisições da infraestrutura de redes: SYN Flood, TCP Flag Abuses, Smurf, Teardrop, PingofDeath e Fragmentação excessiva.

v . A CONTRATADA deve disponibilizar uma Central de Atendimento, com equipe especializada (SOC – SecurityOperationCenter) em monitoramento, detecção e mitigação de ataques, com opção de atendimento através de telefone 0800, correio eletrônico, em idioma português brasileiro, durante as 24 (vinte e quatro) horas do dia, nos 7 (sete) dias da semana, no período de vigência contratual.

w . A CONTRATADA deverá realizar a mitigação dos principais tipos de ataques conhecidos em até 15 minutos (após o tráfego ter sido anunciado e reconhecido pela contratada).

x . As soluções de detecção e mitigação devem possuir serviço de atualização de assinaturas de ataques.

y . Em casos de ataques não detectados pela solução, quando identificados pela CONTRATANTE, deverão ser mitigados pela CONTRATADA após a abertura de chamado através da Central de Atendimento, em até 15 minutos, sem nenhum ônus ao CONTRATANTE.

z . O serviço contratado deverá permitir incorporar modificações e/ou ampliações futuras de características no circuito, nos limites descritos no Termo de Referência, sem qualquer alteração no meio físico;

aa . Em caso de alteração de endereço na prestação dos serviços, a CONTRATADA deverá adotar todas as providências necessárias à implementação da mudança, de forma que o prazo máximo para interrupção seja de 04 (quatro) horas;

bb . As falhas e paralisações que não sejam imputáveis a CONTRATADA serão expurgadas, assim como os tempos de paralisação em que a CONTRATADA não puder atuar por motivo atribuível a CONTRATANTE.

cc . A Disponibilidade Básica mínima mensal do serviço deverá ser de 99,5%, o que corresponde a uma indisponibilidade máxima de 4 horas por mês.

d d . Caso ocorra indisponibilidade do serviço superior 4 horas por mês, a CONTRATADA devera descontar proporcionalmente o valor da mensalidade.

e e . A CONTRATANTE poderá, a qualquer momento, solicitar acesso à tecnologia usada pela CONTRATADA para realização de auditorias e vistorias técnicas.

2.1.3. Requisitos para o Gerenciamento da Rede (NOC)

a O Centro de Operação de Redes (NOC – Network OperationsCenter) da CONTRATADA deverá atender aos requisitos mínimos de serviços especificados neste Termo de Referência, bem como TODOS os requisitos de infraestrutura apresentados a seguir:

a Monitoramento proativo será realizado através de protocolos SNMP reportando todos os eventos de indisponibilidade. O gerenciamento de Redes deverá acompanhar de forma proativa os links contratados, desde o backbone até os equipamentos da Contratante, 24 horas por dia, 7 dias por semana. Assim que os eventos de indisponibilidade sejam identificados e a equipe do Gerenciamento de Redes abre a OS, o Gestor do Contrato deverá ser informado sobre o número do protocolo, o incidente e dados iniciais da tratativa técnica. A ferramenta deverá permitir a exportação dos dados armazenados em formato CSV.

b O atendimento de chamados técnicos terá início imediato, a partir da abertura do chamado através de canal único estabelecido entre o fornecedor e o CONTRATANTE (portal de chamados, 0800, etc).

c A CONTRATADA deverá fornecer acesso a aplicativo para monitoração online do link, contendo informações sobre performance e ocupação do mesmo. Os relatórios deverão conter, no mínimo, gráficos históricos que demonstrem as tendências e os horários de maior/menor utilização.

d A CONTRATADA será responsabilizada por quaisquer informações incorretas disponibilizadas nas páginas de consulta, que venham a trazer prejuízo a CONTRATANTE ou que ocultem informações de monitoração da Rede da Prefeitura.

e Agilização de incidentes: Os incidentes serão gerenciados por uma equipe de controle que tem por foco garantir o cumprimento do SLA, tempo de reparo do link monitorado.

f Validação de solução de incidentes: Após a recuperação do incidente a equipe de gerenciamento de redes fará a análise do link da CONTRATADA para comprovar a efetividade da solução.

g Posteriormente a validação e conclusão da OS, será disponibilizado ao CONTRATANTE um relatório técnico, contendo as seguintes informações: Identificação do link afetado, horário inicial do incidente, horário término do incidente, causa e solução. Esse relatório deverá estar disponível no portal da CONTRATADA para consultas, e também enviado por e-mail para análise e acompanhamento da CONTRATANTE.

2.1.4. HelpDesk

a) Deverá ser disponibilizado serviço de “helpdesk”, com funcionamento 24 horas por dia, 7 (sete) dias na semana, incluindo sábados, domingos e feriados, para a imediata abertura de chamados técnicos e afins, no caso de problemas e solicitações de serviços. Eventuais quedas no circuito deverão ser reparadas no prazo máximo de 4 (quatro) horas, a partir da notificação feita pela CONTRATANTE, via telefone (0800) ou CHAT do portal de clientes. A ferramenta deverá permitir a exportação dos dados armazenados em formato CSV.

2.1.5. Gerenciamento Proativo

a) A CONTRATADA deverá prover gerenciamento proativo, com funcionamento 24 horas por dia, 7

(sete) dias na semana, incluindo sábados, domingos e feriados. Entende-se por gerenciamento proativo a capacidade de a CONTRATADA detectar falhas ocorridas nos circuitos (serviços e equipamentos) de forma autônoma e independentemente de notificação por parte da CONTRATANTE. Da mesma forma autônoma a CONTRATADA deve dar início aos procedimentos de correção de falhas e em seguida informar a CONTRATANTE sobre o evento.

A CONTRATADA deverá notificar a CONTRATANTE através de telefones e e-mails definidos pela CONTRATANTE no prazo máximo de 25 minutos após a identificação do incidente.

b A CONTRATADA deverá, ainda, permitir a visualização, através de WEB browser, via SSH, dos registros de problemas e das ações executadas para a recuperação dos serviços, relativos à pelo menos aos últimos 90 (noventa) dias.

2.1.6. Acordo de Níveis de Serviço – ANS

a) A CONTRATANTE, diretamente ou por meio de seus representantes, poderá acompanhar e fiscalizar o serviço, não descaracterizando com isso as responsabilidades e obrigações da CONTRATADA. A fiscalização da CONTRATANTE não exclui ou atenua a responsabilidade da CONTRATADA por eventuais falhas na prestação do serviço.

b Tempo máximo para mudança de endereço do acesso de até 15 (quinze) dias corridos a partir da data de solicitação. A CONTRATADA deve arcar com os respectivos custos de alteração da rede, desde que não seja necessário o desenvolvimento de projetos especiais para atendimento.

2.1.7. Disponibilidade do Serviço

a.4.a O serviço será considerado DISPONÍVEL quando, cumulativamente:

a.4.I Estejam sendo respeitadas todas as configurações de segurança e de priorização/controle de tráfego acordadas com a CONTRATANTE na fase de implantação ou em momentos posteriores;

a.4.II A disponibilidade do serviço será apurada mensalmente, do 1° ao último dia do mês, considerando-se o horário de 0:00 às 24:00, de 2ª feira a domingo, através da seguinte fórmula:

· Disp = [Tempo de Serviço Disponível]

· [Tempo Total]

· Onde:

· Disp = Disponibilidade Básica;

· [Tempo de Serviço Disponível] = (43.200 – [total de minutos no mês em que o serviço NÃO esteve DISPONÍVEL]);

· [Tempo Total] = 43.200 minutos;

b As falhas e paralisações que não sejam imputáveis a CONTRATADA serão expurgadas, assim como os tempos de paralisação em que a CONTRATADA não puder atuar por motivo atribuível a CONTRATANTE.

b A Disponibilidade Básica mínima mensal do serviço deverá ser de 99,5%, o que corresponde a uma indisponibilidade máxima de 4 horas por mês.

c Caso ocorra indisponibilidade do serviço superior 4 horas por mês, a CONTRATADA devera descontar proporcionalmente o valor da mensalidade.

2.1.8. Gerenciamento Unificado de Ameaças

a) A CONTRATADA deverá prover equipamentos do tipo GERENCIAMENTO UNIFICADO DE AMEAÇAS, para os serviços de Firewall, IntrusionPrevention (IPS), Web Filteringe, ApplicationControl e solução de armazenamento de logs conforme especificação abaixo:

I Serviço 1: Solução de segurança de rede de computadores

I Serviço 2: Solução de armazenamento de logs e emissão de relatórios

II Serviço 3: Instalação, suporte e garantias

b As soluções propostas abaixo poderão ser de um mesmo fabricante ou de fabricantes distintos desde que não tenham nenhuma interoperabilidade entre as tecnologias e funcionalidades;

c) Os Appliances devem possuir no mínimo as seguintes certificações:

I FIPS140-2 Level 2 para Firewall;

I Certificação CommonCriteria como EAL4+;

II Certificação ICSA para o Firewall;

III Certificação ICSA IPSEC. (VPN IPSec).

d Serão aceitas soluções que agreguem mais de uma funcionalidade ou Serviço.

d O serviço 1 deverá ser entregue obrigatoriamente em modelo Hardware físico dedicado.

e O serviço 2 poderá ser entregue como Hardware ou serviço em Nuvem (Cloud) ou ainda em formato compatível para importação nos servidores da CONTRATANTE.

f Todos os detalhes técnicos específicos de cada funcionalidade da solução estão descritos a seguir e constituem o conjunto de funcionalidades obrigatórias da solução completa.

2.1.8.1.Serviço 1 - Solução de segurança de rede de computadores

a) Solução de proteção de rede com características de NextGeneration Firewall (NGFW) ou UnifiedThreat Management (UTM) para segurança de informação perimetral que inclui filtro de pacote, controle de aplicação, administração de largura de banda (QoS), VPN IPSec e SSL, prevenção contra invasão (IPS), prevenção contra ameaças de vírus, spywares, Filtro de URL com categorização automática, bem como controle de transmissão de dados e acesso à internet compondo uma plataforma de segurança integrada e robusta com identificação de usuários e controle granular de permissões de acesso;

b) Por plataforma de segurança entende-se hardware para alocação em servidores 2U/4U ou hardware e software integrados do tipo appliance;

2.1.8.1.1. Capacidades e Quantidades

a) A plataforma de segurança deve possuir as capacidades e as características mínimas abaixo, por equipamento:

I Throughput de 2.5 Gbps de Firewall;

I Throughput de 400 Mbps de VPN IPSec;

II Throughput de 900 Mbps de IPS;

III Throughput de 300 Mbps de Antivirus/Antimalware;

IV Suporte a, no mínimo, 2.5 milhões de conexões simultâneas;

V Suporte a, no mínimo, 20 mil novas conexões por segundo;

VI Fonte 120/240 AC;

VII Disco interno de, no mínimo, 100 GB;

VIII 12 (doze) interfaces de rede 1000 base-TX;

IX 2 (duas) interfaces de rede 1 Gbps SPF;

X 2 (duas) interfaces para HA;

XI Suporte a, no mínimo, 6 (seis) contextos virtuais com domínios de roteamento individuais;

XII Estar licenciada para ou suportar sem o uso de licença, 300 (trezentos) clientes de VPN SSL simultâneos;

XIII Estar licenciada para ou suportar sem o uso de licença, 2.000 (dois mil) túneis de VPN IPSEC simultâneos;

XIV Atender a demanda de pelo menos 600 (seiscentos) usuários de Internet.

2.1.8.1.2. Características Gerais

a) O hardware e software que execute as funcionalidades de proteção de rede, bem como a console de gerência e monitorização, devem ser do tipo appliance.

b) Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19”, incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação.

2.1.8.1.3. Firewall

a Suporte a objetos e regras em IPv4 e IPv6;

a Suporte a objetos e regras multicast;

b Controle de políticas por porta e protocolo;

c Controle de políticas por usuários, grupos de usuários, IPs e redes;

d Controle de políticas por código de País utilizando GeoIP (Por exemplo: Brasil, Estados Unidos, China, Russia);

e Deve suportar offload de certificado em inspeção de conexões SSL de entrada (Inbound);

f Controle de inspeção e de-criptografia de SSH por política;

g Permitir controle de acesso à internet por períodos do dia, permitindo a aplicação de políticas por horários e por dia da semana;

h Deve permitir o funcionamento em modo transparente tipo "bridge" sem alterar o endereço MAC do tráfego;

i Permitir filtro de pacotes sem controle de estado "stateless" para verificação em camada 2;

j Permitir forwarding de camada 2 para protocolos não IP;

k Permitir criação de serviços por porta ou conjunto de portas dos seguintes protocolos, TCP, UDP, ICMP e IP;

l Permitir o agrupamento de serviços;

m Permitir a abertura de novas portas por fluxo de dados para serviços que requerem portas dinâmicas, inclusive aplicações multimídia como H.323 e SIP;

n Possuir mecanismo de anti-spoofing;

o Permitir o serviço de autenticação para tráfego HTTP e FTP;

p Deve permitir IP/MAC binding, em que cada endereço IP possa ser associado a um endereço MAC gerando maior controle dos endereços internos e impedindo o IP spoofing;

q Deve possuir a funcionalidade de balanceamento e contingência de links;

r Deve permitir o filtro de pacotes sem a utilização de NAT;

2.1.8.1.4. Deve suportar os seguintes tipos de NAT

a) DNAT (Destination NAT) com PAT (PortAddressTranslation);

b) Permitir DNAT dentro da mesma subrede na interface IP de entrada;

c) Permitir endereços de destino para outro range de enderços (M:M);

d) Permitir o endereço estático de origem NAT com PAT e porttranslated;

e) Permitir o endereço estático de origem NAT sem PAT com porta fixa;

f) Permitir PAT com recursos de range de portas;

g) Permitir a opção de NAT na Origem e no Destino do tráfego. Inclusive simultaneamente;

2.1.8.1.5. IPS

a Deverá ser orientado à proteção de redes IP;

a Possuir tecnologia de detecção baseada em assinatura com pelo menos 4000 vacinas

b disponíveis contra ataques conhecidos;

c Possuir capacidade de remontagem de pacotes para identificação de ataques;

d Possuir capacidade de agrupar assinaturas para um determinado tipo de ataque; Exemplo: grupo de proteção para Servidores Web, grupo de proteção para servidores de DNS;

e Possuir capacidade de criação de assinaturas customizadas pela interface gráfica do produto;

f Atualizar automaticamente as assinaturas utilizando rede / Internet ou através de atualização manual;

g Deverá ter a funcionalidade de configurar a função de IPS como modo passivo para monitoramento.

2.1.8.1.6. Mecanismos de detecção/proteção de ataques

III.a Reconhecimento de padrões;

III.b Análise de protocolos;

III.c Detecção de anomalias;

III.d Detecção de ataques de Fragmentação RPC;

III.e Detecção de ataques de Fragmentação e Desfragmentação IP;

III.f Detecção de ataques de Segmentação TCP;

III.g Proteção contra ataques de Windows ou NetBios;

III.h Possuir capacidade de remontagem, normalização e decodificação dos protocolos;

III.i Proteção contra ataques de SMTP (SimpleMessageTransferProtocol) IMAP (Internet Message Access Protocol, Sendmail ou POP (Post Office Protocol);

III.j Proteção contra-ataques DNS (DomainNameSystem);

III.k Proteção contra-ataques a FTP, SSH, Telnet e rlogin;

III.l Proteção contra-ataques de ICMP (Internet ControlMessageProtocol);

III.m Suportar verificação de ataque nas camadas de aplicação;

III.n Possuir as seguintes estratégias de bloqueio: deny, pass, drop e reset.

2.1.8.1.7. Métodos de notificação

a Alarmes na console de administração.

a Alertas via correio eletrônico.

b Monitorização do comportamento do appliance mediante SNMP, o dispositivo deverá ser capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede.

c Terminação de sessões via TCP resets.

d Armazenamento de logs de sessões;

e Captura de pacotes (PCAP) de um ataque detectado por uma assinatura.

2.1.8.1.8. Filtro de URL (Web Filter)

a Possuir solução de filtro de conteúdo web integrado a solução de segurança nos protocolos HTTP e HTTPS independente de portas TCP;

a Possuir pelo menos 60 categorias para classificação de sites web;

b Possuir base mínima contendo whitelist (lista branca) , 100 milhões de sites internet web já registrados e classificados;

c Possuir a funcionalidade de cota de tempo de utilização por categoria;

d Possuir categoria exclusiva, no mínimo, para os seguintes tipos de sites web como:

I Proxy Anônimo;

I Webmail;

II Instituições de Saúde;

III Notícias e Esportes;

IV Phishing;

V Hackers;

VI Pornografia;

VII Racismo;

VIII Governo

IX Compras;

X Pedofilia;

e Permitir o monitoramento do tráfego internet sem bloqueio de acesso aos usuários;

f Permitir a criação de pelo menos 5 (cinco) categorias personalizadas;

g Permitir a reclassificação de sites web, tanto por URL quanto por endereço IP, considerando os IPs compartilhados por domínios;

h Prover termo de Responsabilidade on-line para aceite pelo usuário, a ser apresentado toda vez que houver tentativa de acesso a determinado serviço permitido ou bloqueado;

i Integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo contas e grupos de usuários cadastrados;

j Prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory (Single SignOn);

k Exibir mensagens de bloqueio customizável pelos Administradores para resposta aos usuários na tentativa de acesso a recursos proibidos pela política de segurança;

l Permitir a filtragem de todo o conteúdo do tráfego WEB de URLs conhecidas como fonte de material impróprio e códigos (programas/scripts) maliciosos em applets Java, cookies, activeX através de: base de URL própria atualizável;

m Permitir o bloqueio de páginas web através da construção de filtros específicos com mecanismo de busca textual;

n Permitir a criação de listas personalizadas de URLs permitidas – lista branca e bloqueadas – lista negra;

o Deverá permitir o bloqueio de URLs inválidas cujo campo CN do certificado SSL não contém um domínio válido;

p Filtro de conteúdo baseado em categorias em tempo real;

q Garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de filtragem de conteúdo web;

r Deverá permitir a criação de regras para acesso/bloqueio por grupo de usuários do serviço de diretório LDAP;

s Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem;

t Deverá permitir a criação de regras para acesso/bloqueio por sub-rede de origem;

u Deverá ser capaz de categorizar a página web tanto pela sua URL como pelo seu endereço IP;

v Deverá permitir o bloqueio de redirecionamento HTTP;

w Deverá permitir o bloqueio de páginas web por Classificação como páginas que facilitam a busca de Audio, Vídeo e URLs originadas de Spam;

x Trabalhar como proxy transparente (sem a necessidade de configuração nas estações dos usuários);

y Deverá permitir a criação dinâmica de listas personalizadas de URLs permitidas (lista branca) e bloqueadas (lista negra);

2.1.8.1.9. Controle de Aplicações

a O Controle de Aplicações deve ser baseado em vacinas, atualizadas automaticamente e ter a funcionalidade de bloquear e monitorar aplicações em camada 7;

a Deverá reconhecer no mínimo 2000 aplicações;

b Deverá possuir pelo menos 10 categorias para classificação de aplicações;

c Deverá possuir categoria exclusiva, no mínimo, para os seguintes tipos de aplicações como:

I P2P;

I Audio e vídeo;

II Proxy;

III Update;

IV VoIP.

d Deve permitir a monitoração do tráfego de aplicações sem bloqueio de acesso aos usuários;

e Deve ser capaz de controlar aplicações independente do protocolo e porta utilizados, identificando-a apenas pelo comportamento de tráfego da mesma;

f Deve integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;

g Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory;

h Deve permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP;

i Deve permitir a criação de regras para acesso/bloqueio por endereço IP de origem;

j Deve permitir a criação de regras para acesso/bloqueio por sub-rede de origem e destino;

k Deve garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações, informando antecipadamente aos especialistas de TI da CONTRATANTE;

l Deve ser possível a liberação e bloqueio somente das aplicações sem a necessidade de liberação de portas e protocolos;

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

n Deve identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e ataques mediante a porta 443;

o Limitar a banda (download/upload) usada por aplicações (trafficshaping), baseado no IP de origem, usuários e grupos do serviço de diretório LDAP/AD;

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

q Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos e análise heurística;

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

s A CONTRATADA deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;

t Deve alertar o usuário quando uma aplicação foi bloqueada;

u Deve possibilitar a diferenciação de tráfegos de InstantMessaging (Facebook Chat, etc.) possuindo granularidade de controle/políticas para os mesmos;

v Deve ser possível a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como:

I Tecnologia utilizada nas aplicações (Client-Server, BrowseBased, Network Protocol, etc);

I Nível de risco da aplicação;

II Categoria e sub-categoria de aplicações;

III Aplicações que usem técnicas evasivas, utilizadas por malwares, como transferência de arquivos e/ou uso excessivo de banda.

2.1.8.1.10. VPN

v.a Possuir os algoritmos de criptografia para túneis VPN IPSec: AES, DES, 3DES;

v.b Possuir autenticação baseada em MD5 e SHA-1;

v.c Suporte a Diffie-HellmanGroup 1, Group 2, Group 5 e Group 14;

v.d Suporte a certificados PKI X.509 para construção de VPNs;

v.e Possuir suporte a VPNsIPSec site-to-site, VPNsIPSecclient-to-site;

v.f Possuir suporte a VPN SSL;

v.g A VPN SSL deve possibilitar o acesso a toda infraestrutura de acordo com a política de segurança;

v.h Possuir hardware acelerador criptográfico para incrementar o desempenho da VPN;

v.i A VPN SSL deverá suportar cliente para plataforma Windows, Linux e Mac OS X com licenciamento já incluso;

v.j Suporte a VPN do tipo PPTP, L2TP;

v . k Suporte à inclusão em autoridades certificadoras (enrollment) mediante SCEP; (SimpleCertificateEnrollmentProtocol) e mediante arquivos;

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

v.m Atribuição de endereço IP nos clientes remotos de VPN;

v.n Atribuição de DNS nos clientes remotos de VPN;

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

v.p Permite estabelecer um túnel VPN client-to-site do cliente a plataforma de segurança, fornecendo uma solução de single-sign-on aos usuários, integrando-se;

v.q Permite a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;

v.r Permitir Split-tunnel nos clientes de VPN IPSec e/ou SSL;

v.s O agente de VPN a ser instalado nos equipamentos desktop e laptops, dever ser capaz de ser distribuído de maneira automática via Microsoft SMS, Active Directory e ser descarregado diretamente desde o seu próprio portal, o qual residirá no centralizador de VPN;

v.t Deverá manter uma conexão segura com o portal durante a sessão.

v.u Possuir interoperabilidade com os seguintes fabricantes:

I Cisco;

I HP;

II Dell;

III Mikrotik;

IV Checkpoint;

V Juniper;

VI Palo Alto Networks;

VII Fortinet;

VIII Sonic Wall;

2.1.8.1.11.Traffic Shaping / QoS

VIII.a Permitir o controle e a priorização do tráfego, priorizando e garantindo banda para as aplicações (inbound/outbound) através da classificação dos pacotes (Shaping), criação de filas de prioridade, gerência de congestionamento e QoS;

VIII.b Permitir modificação de valores DSCP para o DiffServ;

VIII.c Deverá integrar-se ao serviço de diretório padrão LDAP, inclusive o Microsoft Active Directory, reconhecendo grupos de usuários cadastrados;

VIII.d Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory e LDAP;

VIII.e Deverá controlar (limitar ou garantir) individualmente a banda utilizada por grupo de usuários do Microsoft Active Directory e LDAP;

VIII.f Deverá controlar (limitar ou garantir) individualmente a banda utilizada por sub-rede de origem e destino ao atingir 80% do seu uso;

VIII.g Deverá controlar (limitar ou garantir) individualmente a banda utilizada por endereço IP de origem e destino;

VIII.h Deverá controlar (limitar ou garantir) individualmente a banda utilizada por aplicativos. Os aplicativos devem ser reconhecidos através de assinaturas;

VIII.i Deverá permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário.

VIII.j O QoS deve possibilitar a definição de classes por:

I Banda Garantida

I Banda Máxima

II Fila de Prioridade.

2.1.8.1.12. Antivírus e Antimalware

a Possuir funções de Antivírus, Anti-spyware e Antimalware em geral;

a Possuir antivírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para pelo menos os seguintes protocolos: HTTP, HTTPS, SMTP, IMAP, POP3 e FTP;

b Suportar o bloqueio de malwares (adware, spyware, hijackers, keyloggers, etc.);

c Suportar o bloqueio de download de arquivos por extensão, nome do arquivo e tipos de arquivo;

d Suportar o bloqueio de download de arquivos por tamanho;

e Suportar a análise de arquivos executáveis, DLLs, ZIP e criptografados em SSL;

f Suportar o bloqueio através de assinaturas;

g Suportar o bloqueio de Botnets;

h Caso ocorra a detecção de malware nos protocolos HTTP e HTTPS apresentar uma mensagem customizável ao usuário final;

2.1.8.1.13. Balanceamento de Carga (Proxy Reverso)

a Permitir a criação de endereços IPs virtuais;

a Permitir balanceamento de carga entre pelo menos 2 servidores reais;

b Suportar balanceamento ao menos para os seguintes serviços: HTTP, HTTPS, TCP e UDP;

c Permitir balanceamento ao menos com os seguintes métodos: hash do endereço IP de origem, Round Robin, Weighted, First alive e HTTP Host;

d Permitir persistência de sessão por cookie HTTP ou SSL session ID;

e Suportar SSL offloading;

f Deve ter a capacidade de identificar, através de healthchecks, quais os servidores que estejam ativos, removendo automaticamente o tráfego dos servidores que não estejam;

g Permitir que o healthcheck seja feito ao menos via ICMP, TCP em porta configurável e HTTP em URL configurável.

2.1.8.1.14. Roteamento

a Suporte a rota estática;

a Suporte a ECMP (Equal-costmulti-pathrouting) com metodo de balanceamento outbound de rotas;

b Suporte a Policy-BasedRouting por origem, destino, protocolo e interface;

c Suportar os seguintes protocolos de roteamento dinâmico:

I RIPv2 para IPv4;

I OSPF para IPv4;

II BGP para IPv4;

III RIPng para IPv6;

IV OSPFv3 para IPv6;

V BGP para IPv6;

2.1.8.1.15. Controle de Transmissão

a O sistema de DLP (Proteção contra Vazamento de Informações) de gateway deve funcionar de maneira que consiga parar que dados sensíveis saiam da rede e também deve funcionar de modo que previna que dados não requisitados entrem na sua rede;

a O sistema de DLP deverá inspecionar no mínimo os tráfegos de Email, HTTP, NNTP e de Mensageiros Instantâneos;

b Deverá realizar buscas para a aplicação de regras de DLP em arquivos do tipo PDF, doc, docx, e odt;

c Deverá fazer a varredura no conteúdo de um Cookie HTTP buscando por determinado texto;

d Deverá aplicar regras baseadas em usuários autenticados, isto é, fazendo buscas pelo tráfego de um específico usuário;

e Deverá verificar para aplicações do tipo e-mail, se o anexo das mensagens de correio entrantes/saintes possuí um tamanho máximo especificado pelo administrador;

f Deverá utilizar expressões regulares para composição das regras de verificação dos tráfegos;

g Deverá tomar minimamente as ações de bloquear, banir usuário e quarentenar a interface sobre as regras que coincidirem com o tráfego esperado pela regra;

h Deverá permitir o armazenamento em solução específica de armazenamento de logs, o conteúdo do tráfego que coincidir com o tráfego esperado pela regra de DLP para minimamente os protocolos de E-mail, HTTP e Mensageiros Instantâneos;

i Deverá permitir a composição de múltiplas regras de DLP formando uma regra única mais específica que usa lógica booleana para fazer a comparação com o tráfego que atravessa o sistema.

2.1.8.1.16. Funcionalidades Gerais

a Possuir controle de acesso à rede por endereço IP de origem e destino;

a Possuir controle de acesso à rede por subrede;

b Possuir integração com Servidores de Autenticação RADIUS, LDAP e Microsoft;

c Active Directory para autenticação de usuários administradores e usuários de firewall;

d Suportar no mínimo 250 (duzentos e cinquenta) usuários autenticados com serviços ativos e identificados passando por este dispositivo de segurança. Políticas baseadas por grupos de usuários deverão ser suportadas por este dispositivo. Está comprovação poderá ser exigido em testes sobre o ambiente de produção com o fornecimento do produto para comprovação deste e demais itens;

e Suportar no mínimo 600 (seiscentos) usuários não autenticados. Esta comprovação poderá ser exigido em testes sobre o ambiente de produção com o fornecimento do produto para comprovação deste e demais itens;

f Suporte a alta disponibilidade (HA), trabalhando no esquema de redundância do tipo ativo-passivo e também ativo-ativo com divisão de carga;

g Suporte a autenticação baseada em Token;

h Possuir conexão entre estação de gerência e appliance de forma criptografada tanto em interface gráfica (HTTPS) quanto em linha de comando (SSH);

i Suporte a sFlow;

j Suporte a tags de VLAN (802.1q);

k Suporte a agregação de interfaces (IEEE 802.3ad);

l Possuir ferramenta de diagnóstico do tipo TCPdump;

m Possuir funcionalidades de DHCP Cliente, Servidor e Relay;

n Deve suportar, no mínimo, 10 sistemas virtuais lógicos (contextos) no firewall físico;

o Enviar log para sistemas de monitoração externos, simultaneamente, como SYSLOG e SIEM;

p O dispositivo de proteção deve ter a capacidade de operar de forma simultânea 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);

q Deve implementar VRRP (Virtual Router RedundancyProtocol);

r Deve implementar Firewall dual stack para IPv4/IPv6;

s Permitir importação de certificados digitais para funcionalidades gerais do equipamento;

t Possuir monitoramento SNMP v2c e v3;

u Possuir MIB para integração com sistema de monitoramento SNMP;

v Deverá vir acompanhado de todos os cabos e acessórios necessários à completa instalação e operação dos mesmos;

w Deverá vir acompanhado de documentação impressa ou em mídia DVD/CD ou via download, em idioma português ou inglês, contendo orientações para configuração e operação do produto fornecido;

x Possuir certificado ICSA para Firewall;

y Possuir certificação FIPS 140-2 para firewall;

z Possuir certificação CommonCriteria como EAL4+.

2.1.8.1.17.Suporte e Voip

a Possuir suporte a SIP e H 323;

a Deve possuir mecanismo específico para alterar o conteúdo das mensagens SIP SDP permitindo a alteração do endereço privado para público de forma que permita um cliente SIP interno a operar via Internet. Deve ainda controlar automaticamente a abertura de portas RTP/RTCP para o funcionamento de ligações via SIP;

2.1.8.1.18. Serviço 2 - Solução de armazenamento de logs e emissão de relatórios

a A solução de armazenamento de logs e emissão de relatórios deve ser compatível obrigatoriamente com a Solução 1;

2.1.8.2.Funcionalidades

a Interface gráfica de usuário (GUI) para fazer administração da solução.

a A solução pode ser fornecida nas seguintes condições:

I Hardware do tipo appliance dedicado;

I Solução Cloud – Com administração e armazenamento baseado em nuvem. Sem a necessidade de instalação de dispositivo local;

b Possuir comunicação entre os componentes de forma criptografada;

c Possui armazenamento de logs total de pelo menos 500GB;

d Possuir perfis administrativos com capacidade de criar ao menos 2 (dois) perfis para monitoração

dos logs;

e Possuir a visualização de log em tempo real de tráfegos de rede;

f Permitir a visualização de logs de histórico dos acessos de tráfegos de rede;

g Permitir a visualização dos eventos de auditoria;

h Possuir pelo menos 20 tipos de relatórios pré-definidos na solução;

i Permitir geração de relatórios agendados ou sob demanda nos formatos HTML, CSV e PDF;

j Permitir o envio dos relatórios, conforme item anterior, através de e-mail para usuários pré-definidos;

k Permitir customização dos relatórios, incluindo logotipo customizado;

l Possuir relatórios detalhados contendo informações como: IP de origem, IP de destino, Serviço, Usuário, Grupo e Horário;

m Possuir gerar relatórios baseado nas últimas 24 horas, 1 semana e 1 mês;

n Possuir pelo menos os relatórios seguintes relatórios:

I 100 (dez) sites web mais acessados

I 100 (dez) categorias de sites web mais acessados

II 100 (dez) usuários mais ativos na rede

III 100 (dez) aplicativos mais acessados

IV Tráfego baseado em IP

V Ataques baseado em origem e destino

VI Vírus detectado por origem e destino

2.1.8.3. Serviço 3 - Instalação, suporte e garantias a Instalação

I Os Serviços deverão ser instalados e configurados pela CONTRATADA in loco no ambiente da CONTRATANTE;

I A CONTRANTE será responsável por dar como completo toda a instalação e configuração após validação de todas as funcionalidades;

h.b Suporte

I Assistência técnica e suporte ambos por telefone e web, incluindo a operação assistida do conjunto fornecido, substituição de peças e equipamentos durante todo o prazo de vigência do contrato;

I Abertura de chamados e o atendimento junto à CONTRATADA deverão ser feitos em português, durante todo o prazo de vigência do contrato;

II Por suporte entende-se a solução de falhas, dúvidas, operação assistida, inclusive na aplicação de patches e atualizações, reparos de funcionalidades ou de sistema operacional além de outras demandas de ordem lógica;

III Por assistência técnica entende-se o serviço de manutenção corretiva, reparo e substituição de

equipamentos e peças sem ônus a CONTRATANTE;

IV Atendimento via telefone 0800 (ligação gratuita) , inclusive de telefone móvel ou número local do município de Itaboraí - RJ (DDD 21);

V Sistema de HelpDesk online para abertura de chamados. Os chamados deverão ficar armazenados e identificados com uma numeração única para cada chamado;

VI O sistema de HelpDesk deverá fornecer histórico de todos chamados abertos e fechados;

VII Os chamados devem ser abertos via e-mail ou via Portal Web próprio para abertura dos chamados;

VIII O Portal de abertura de chamados deve manter os dados da Prefeitura de Itaboraí/RJ totalmente sigilosos e criptografados incluindo sua transmissão (SSL / HTTPS);

IX O tempo de resposta inicial do chamado deverá ser de até 30 (trinta) minutos em regime 24x7x365 (vinte e quatro horas por dia, sete dias por semana em todos os dias do ano, incluindo feriados) e solução online de até 1 (uma) hora;

X Garantia de atendimento de número ilimitado de chamados;

XI Chamados que necessitem presença física de um funcionário da CONTRATADA nas dependências da Prefeitura de Itaboraí-RJ deverão ser atendidas em um prazo de 8 horas uteis de segunda a sexta das 08:00hs às 18:00hs, inclusive nos finais de semana e feriados, podendo o horário ser estendido de acordo com a necessidade da CONTRATANTE.

h.c Garantias

I A garantia para substituição de todos os produtos com mal funcionamento é de total responsabilidade da CONTRATADA pelo tempo vigente do contrato;

I Caso um dos produtos ofertados entre em fim de suporte pelo fabricante (EndOfLife), a CONTRATADA será responsável pela troca por um produto de qualidade igual ou superior já descrita nesse termo.

2.2 REQUISITOS PARA A PRESTAÇÃO DOS SERVIÇOS

2.2.a O acesso ao serviço de conexão IP (Internet Protocol) dedicado deverá estar implantado sobre um enlace determinístico de 500 Mbps.

2.2.b A CONTRATADA deverá entregar fisicamente esse enlace à rede local do CONTRATANTE através de interface de Fibra Óptica.

2.2.c A conexão entre comunicação WAN (WideArea Network) de ECD (Equipamento de Comunicação de Dados) instalado pela CONTRATADA deverá ser exclusivo e dedicado para conexão IP de acesso à Internet.

2.2.d O serviço IP dedicado a ser contratado deverá suportar aplicações TCP/IP (TransmissionControlProtocol / Internet Protocol), tais como: HTTP, HTTPS, FTP (File TransferProtocol), SSH (Secure SHell), SMTP (Simple Mail TransferProtocol), POP3 (Post Office Protocolversion 3), LDAP (LightweightDirectory Access Protocol), e VPN, e tráfego de vídeo e voz sobre IP (VoIP), no sentido para a Internet e vice-versa. O Provedor contratado deverá apresentar uma lista com todas as aplicações adicionais suportadas pelo seu sistema, com as respectivas condições de utilização.

3. CLASSIFICAÇÃO DOS SERVIÇOS

3.1. Os serviços a serem contratados são enquadrados como comuns nos termos do art. 1º da Lei 10.520/2002, pois os padrões de desempenho e qualidade podem ser objetivamente definidos por meio de especificações usuais no mercado.

4. JUSTIFICATIVA E OBJETIVO DA CONTRATAÇÃO

4.1. Justifica-se a presente contratação ante a necessidade da Prefeitura de Itaboraí manter o link utilizado para acessos à internet e divulgação de seus serviços ao público externo**.**

4.2. Esta contratação visa à manutenção dos serviços de atendimento aos munícipes, bem como a implantação e aperfeiçoamento de soluções efetivas, voltadas para o Município.

4.3. Os serviços de Internet são essenciais para a Administração, no instante em que atendem a necessidade de permanente comunicação entre pessoas que integram a própria Administração, bem como entre os membros da Administração e o público externo em geral e por estas razões, configuram-se como contínuos.

5. DA HABILITAÇÃO - QUALIFICAÇÃO TÉCNICA DOS LICITANTES-

5.1. Além das exigências habituais relacionadas à comprovação da habilitação econômico financeira e jurídica das licitantes, com o intuito de garantir a seleção de fornecedores aptos a efetivamente atender a demanda da Secretaria Municipal de Fazenda e Tecnologia, evitando-se o inadimplemento contratual, deverão ser exigidos dos licitantes os seguintes documentos referentes à comprovação de aptidão técnica:

5.1.1. Comprovação de aptidão para prestação de serviços em características compatíveis com o objeto do futuro contrato, por meio da apresentação de atestados fornecidos por pessoas jurídicas de direito público ou privado, que demonstrem que o licitante já prestou serviços idênticos ou similares ao objeto deste Termo;

5.2. Para fins da comprovação de que trata o item anterior, os atestados deverão dizer respeito a contratos executados e deverão ser emitidos em papel timbrado da pessoa jurídica de direito privado ou público emitente, indicar o serviço realizado, o valor do contrato, número do processo ou procedimento licitatório ou do processo de contratação direta, número e prazo de vigência do contrato, devendo ser datado e assinado por pessoa física identificada pelo seu nome completo, cargo ou função e número da matrícula, indicando ainda se a execução do objeto ocorreu de forma regular e satisfatória;

5.3. Os atestados emitidos por pessoa jurídica de direito privado deverão estar acompanhados de documentos que comprovem a aptidão do signatário para responder pela pessoa jurídica atestante;

5.4. Apresentar Licença/concessão de serviços de telecomunicação da Agência reguladora, prevista na resolução nº. 614/2013 da ANATEL e Termo de autorização da ANATEL;

5.5. Os licitantes deverão disponibilizar todas as informações necessárias à comprovação da legitimidade dos atestados, caso solicitado pela Comissão de Licitações.

6. FORMA DE PRESTAÇÃO DOS SERVIÇOS E CRITÉRIOS DE ACEITAÇÃO DO OBJETO

6.1 A Prestadora deverá iniciar os serviços no prazo de 5 (cinco) dias corridos, após o recebimento da Ordem de Serviço;

6.2 O s serviços de instalação deverão ser concluídos em até 20 (vinte) corridos dias após o recebimento da Ordem de Serviço;

6.3 O circuito deverá ser instalado no CPD da Prefeitura Municipal de Itaboraí localizado, atualmente, na Secretaria Municipal de Fazenda e Tecnologia, sito à Rua Fidélis Alves, 101 – Centro – Itaboraí/RJ, com possibilidade de mudança de endereço, conforme necessidade da CONTRATANTE;

6.4 Os serviços serão recebidos provisoriamente, no prazo máximo de 05 (cinco) dias úteis, contados da efetiva entrega, para efeito de posterior verificação de sua conformidade com as especificações constantes na Ordem de Serviço;

6.5 Os serviços serão recebidos definitivamente, no prazo máximo de 05 (cinco) dias úteis , contados do recebimento provisório, após a verificação da sua qualidade e conseqüente aceitação mediante termo circunstanciado;

6.6. O recebimento definitivo dos serviços não exclui a responsabilidade da Prestadora pelos prejuízos resultantes da incorreta execução, sobretudo daqueles prejuízos advindos de vícios dos da qualidade, de vícios ocultos ou não aparentes na época da entrega;

6.7. A nota fiscal apresentada pela empresa deverá mencionar o número do processo administrativo que deu origem à contratação, do contrato administrativo dele decorrente e da respectiva Ordem de Serviço.

7. DAS OBRIGAÇÕES DA CONTRATADA

7.1 Prestar os serviços de forma que o link da CONTRATANTE, em um período mensal, não fique inoperante por um período superior a 4 (quatro) horas, considerando o somatório de todas as paralisações do mês;

7.2 Informar eventuais interrupções programadas dos serviços com antecedência mínima de 05 (cinco) dias;

7.3 Obedecer a todas as normas da ANATEL, padrões ABNT, processos e procedimentos da Prefeitura Municipal de Itaboraí;

7.4 Apresentar em um prazo máximo de 30 (trinta) dias antes do término de seu contrato, um plano para transferência de conhecimentos e tecnologias para a próxima empresa que vier a prestar serviços à Prefeitura Municipal de Itaboraí. Este plano deverá conter, pelo menos, a revisão de toda a documentação gerada de todos os serviços prestados, acrescido de outros documentos que, não sendo artefatos previstos em Metodologia, sejam adequados ao correto entendimento do serviço executado;

7.5 Disponibilizar, sem ônus para o CONTRATANTE, Serviço de Atendimento ao Cliente (SAC), durante toda a vigência do Contrato, por meio de atendimento telefônico e correio eletrônico, a fim de que seja possível registrar reclamações sobre o funcionamento do serviço contratado, obter suporte técnico e esclarecimentos.

7.6 Utilizar os canais de comunicação propostos pela Prefeitura Municipal de Itaboraí para o seu relacionamento;

7.7 Cumprir todas as obrigações constantes neste Termo de Referência e no Contrato, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto;

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

7.9 Indicar preposto para representá-la durante a execução do contrato;

7.10 Prestar imediatamente as informações e os esclarecimentos que venham a ser solicitados pela CONTRATANTE, salvo quando implicarem em indagações de caráter técnico, hipótese em que deverão ser respondidas no prazo de 24 (vinte e quatro) horas;

7.11 Responder por todas as despesas diretas e indiretas que incidam ou venham a incidir sobre a execução do contrato tais como taxas, fretes, tributos, inclusive as obrigações relativas a salários, pagamentos de recursos humanos, Previdência Social, impostos, encargos sociais, transporte, indenizações, recolhimento de valores para órgãos de classe e outras providências, respondendo obrigatoriamente pelo fiel cumprimento das leis trabalhistas e específicas de acidente de trabalho e legislação correlata, aplicáveis ao pessoal empregado na execução contratual, ficando o Contratante isento de qualquer vínculo empregatício com os mesmos;

7.12 Responsabilizar-se pelos danos causados diretamente ao Contratante ou a terceiros, decorrentes da sua culpa ou dolo quando da execução do objeto, independente dos procedimentos de fiscalização e acompanhamento da execução contratual, e independente de outras cominações contratuais ou legais as quais estiver sujeita;

7.13 Indicar preposto para representá-la durante a execução do contrato.

8. DAS OBRIGAÇÕES DO CONTRATANTE

8.1. Receber o objeto no prazo e condições estabelecidas no Edital e seus anexos;

8.2. Verificar, no prazo fixado, a conformidade dos bens recebidos com as especificações constantes do Edital e da proposta, para fins de aceitação;

8.3. Comunicar, à **CONTRATADA**, por escrito, via e-mail ou outro canal disponibilizado à **CONTRATANTE**, através da Fiscalização, as imperfeições, falhas ou irregularidades verificadas no objeto fornecido, para que seja substituído, reparado ou corrigido em até 2 (dois) dias úteis da comunicação;

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

8.5. Indicar, por meio de Portaria, os servidores responsáveis pela fiscalização do cumprimento das obrigações decorrentes do Contrato.

9. DA SUBCONTRATAÇÃO

9.1. Não será admitida a subcontratação.

10. ALTERAÇÃO SUBJETIVA

10.1. É admissível a fusão, cisão ou incorporação da **CONTRATADA** com/em outra pessoa jurídica, desde que sejam observados pela nova pessoa todos os requisitos de habilitação exigidos na licitação original; sejam mantidas as demais cláusulas e condições do contrato/ata de registro de preço; não haja prejuízo à execução do objeto pactuado, e haja anuência expressa da Administração Pública quanto à continuidade do contrato administrativo/ata de registro de preço.

11. DO CONTROLE E FISCALIZAÇÃO DA EXECUÇÃO

11.1. Do fiscal de contrato:

11.1.1. O fiscal do contrato acompanhará a execução do contrato, para que sejam cumpridas todas as condições nele estabelecidas, de modo a assegurar os melhores resultados para a Administração, nos termos do Decreto Municipal nº 300/2023.

11.1.1.1. O fiscal anotará, no histórico de gerenciamento do contrato, todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados, nos termos do Art. 117, §1º da Lei nº 14.133/2021 e do Decreto Municipal nº 300/2023;

11.1.1.2. Identificada qualquer inexatidão ou irregularidade, o fiscal do contrato emitirá notificações para a correção, determinando prazo para tanto;

11.1.1.3. O fiscal informará ao gestor do contato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e/ou saneadoras, se for o caso, nos termos do Decreto Municipal nº 300/2023.

11.1.1.4. No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprazadas, o fiscal comunicará o fato imediatamente ao gestor do contrato, nos termos do Decreto Municipal nº 300/2023.

11.1.1.5. O fiscal comunicará ao gestor, com antecedência e em tempo hábil, o iminente término do contrato sob sua responsabilidade, com vistas à renovação ou à prorrogação.

11.2. Do gestor do contrato:

11.2.1. O gestor coordenará o processo de acompanhamento e fiscalização do contrato, bem como sua atualização, devendo providenciar todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento à finalidade da contratação nos termos do Decreto Municipal nº 300/2023.

11.2.1.1. O gestor acompanhará a manutenção das condições de habilitação da contratada, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais.

11.2.1.2. O gestor deverá, nos termos do Art. 12, Inciso XXVII do Decreto Municipal nº 300/23, encaminhar à Secretaria Municipal de Compras, Licitações e Contratos – SEMLIC, em até 10 (dez) dias corridos após a publicação do extrato, a cópia física do contrato.

11.2.1.3. O gestor emitirá documento comprobatório da avaliação realizada pelos fiscais quanto ao cumprimento de obrigações assumidas pelo contratado, com menção ao desempenho do prestador na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações, a ser enviado, por cópia, à Comissão de Registro Cadastral da SEMLIC.

11.2.1.4. O gestor tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o art. 158 da Lei nº 14.133 de 2021.

11.2.1.5. O ordenador de despesas deverá, nos termos do Art. 21 do Decreto Municipal nº 300/23, encaminhar à Comissão de Registro Cadastral da SEMLIC, o relatório final contendo as informações acerca do desempenho do contratado quanto ao cumprimento das obrigações assumidas, para fins de anotação no cadastro de atesto de cumprimento das obrigações.

12. DO PAGAMENTO

12.1. O pagamento será realizado no prazo máximo de 30 (trinta) dias, contados a partir do protocolo do pedido de pagamento, que deverá ser instruído com a documentação comprobatória das condições de habilitação da **CONTRATADA**.

12.1.1. Entende-se como documentação comprobatória das condições de habilitação a comprovação da reguaridade fiscal, trabalhista, tributária e previdenciária.

12.2. O pagamento será realizado através de ordem bancária, para crédito em banco, em agência e conta corrente indicados pela **CONTRATADA**.

12.3. Havendo erro na apresentação da Nota Fiscal ou dos documentos pertinentes à habilitaçao ou,

ainda, circunstância que impeça a liquidação da despesa, como, por exemplo, obrigação financeira pendente, decorrente de penalidade imposta ou inadimplência, o pagamento ficará sobrestado até que a **CONTRATADA** providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para a **CONTRATANTE**.

12.4. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

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

12.6. Nos casos de eventuais atrasos de pagamento, desde que a **CONTRATADA** não tenha concorrido, de alguma forma, para tanto, fica convencionado que a taxa de compensação financeira devida pela **CONTRATANTE**, entre a data do vencimento e o efetivo adimplemento da parcela, é calculada mediante a aplicação da seguinte fórmula:

EM = I x N x VP, sendo:

EM = Encargos moratórios;

N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;

VP = Valor da parcela a ser paga.

I = Índice de compensação financeira = 0,00016438, assim apurado:

I = (TX)	I =	$\frac{(6/100)}{365}$	I = 0,00016438 TX = Percentual da taxa anual = 6%

13. DO PRAZO E VIGÊNCIA DO CONTRATO

13.1. O prazo de vigência da Contrato será de 12 (doze) meses, contados a partir do primeiro dia útil subsequente à publicação no PNCP, a qual deverá ser providenciada pelo Ordenador de Despesas no prazo máximo de 20 (vinte) dias úteis a contar da data de assinatura.

14. DA ANTECIPAÇÃO DO PAGAMENTO

14.1. Não se aplica ao presente processo.

15. DO REAJUSTE

15.1. Os preços são fixos e irreajustáveis no prazo de 1(um) ano contados da data de apresentação da proposta.

16. DAS SANÇÕES ADMINISTRATIVAS

16.1. Comete infração administrativa, a **CONTRATADA** que:

16.1.1. Inexecutar total ou parcialmente qualquer das obrigações assumidas em decorrência da contratação;

16.1.2. Ensejar o retardamento da execução do objeto;

16.1.3. Falhar ou fraudar na execução do contrato;

16.1.4. Comportar-se de modo inidôneo;

16.1.5. Cometer fraude fiscal;

16.2. Pela inexecução total ou parcial do objeto deste contrato, a Administração pode aplicar à **CONTRATADA** as seguintes sanções:

16.2.1. Advertência, por faltas leves, assim entendidas aquelas que não acarretem prejuízos significativos para a Contratante.

16.2.2. Multa moratória de 0,2% (zero vírgula dois por cento) sobre o valor do contrato, por dia de atraso injustificado na execução dos serviços, até o limite de 30 (trinta) dias de atraso; Multa moratória de 0,4% (zero vírgula quatro por cento) por dia de atraso injustificado sobre o valor do contrato, do 31º (trigésimo primeiro) ao 60º (sexagésimo) dia de atraso, sem prejuízo das demais penalidades;

16.2.3. Multa compensatória de 5% (cinco por cento) sobre o valor total do contrato, no caso de inexecução total do objeto;

16.2.4. Em caso de inexecução parcial, a multa compensatória, no mesmo percentual do sub item acima, será aplicada de forma proporcional à obrigação inadimplida;

16.2.5. Impedimento de licitar e impedimento de contratar com o órgão, entidade ou unidade administrativa pela qual a Administração Pública opera e atua concretamente, pelo prazo de até dois anos;

16.2.6. Declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a **CONTRATADA** ressarcir a **CONTRATANTE** pelos prejuízos causados;

16.3. As sanções previstas nos subitens 16.2.1, 16.2.5 e 16.2.6, poderão ser aplicadas a **CONTRATADA** juntamente com as de multa, descontando-a dos pagamentos a serem efetuados.

16.4. Também ficam sujeitas às penalidades as empresas ou profissionais que:

16.4.1. Tenham sofrido condenação definitiva por praticar, por meio dolosos, fraude fiscal no recolhimento de quaisquer tributos;

16.4.2. Tenham praticado atos ilícitos visando a frustrar os objetivos da licitação;

16.4.3. Demonstrem não possuir idoneidade para contratar com a Administração em virtude de atos

ilícitos praticados.

16.5. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa à Contratada.

16.6. Caso a Contratante determine, a multa deverá ser recolhida no prazo máximo de **30 dias corridos**, a contar da data do recebimento da comunicação enviada pela autoridade competente.

16.7. A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

16.8. As penalidades serão obrigatoriamente registradas no Tribunal de Contas do Estado do Rio de Janeiro, PNCP; CNEP; SICAF e CEIS.

16.9. O descumprimento do Contrato ensejará aplicação das penalidades estabelecidas no Edital.

17. DOS RECURSOS ORÇAMENTÁRIOS

17.1. As despesas decorrentes da contratação correrão por conta da seguinte dotação orçamentária – Orçamento 2025.

Órgão	06
Unidade	001
Subunidade Orçamentária	001
Programa de Trabalho	19.126.0012.2841
Natureza de Despesas	3.3.90.40
Fonte	15010001
Ficha	95

18. DAS DISPOSIÇÕES GERAIS

18.1. O presente Termo de Referência (TR) seguirá devidamente aprovado pela autoridade competente (ordenador de despesas), por meio de despacho, em atenção ao Decreto nº. 295/2023

Elaborado em ____/_____/___ Aprovado em ____/____/____

Rodolfo Velozo Pinto
Assessor Técnico
Matrícula: 44.799

Cezar Caetano Sabiá Neto
Superintendente
Matrícula: 44.794

Roberto Ataíde Santiago Fontes
Secretário Municipal de Fazenda e Tecnologia
Matrícula: 57.357

Documento assinado eletronicamente por **CEZAR CAETANO SABIÁ NETO**, **Superintendente**, em 24/03/2025, às 11:52, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **RODOLFO VELOZO PINTO**, **Assessor(a) Técnico(a)**, em 24/03/2025, às 11:54, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **ROBERTO ATAÍDE SANTIAGO FONTES**, **Secretário(a)**, em 24/03/2025, às 14:46, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015 .

A autenticidade deste documento pode ser conferida no site https://sei.ib.itaborai.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0218141** e o código CRC **D20991A0**.

Referência: Processo nº 0001.007475/2024-01 SEI nº 0218141