ANEXO II - TERMO DE REFERÊNCIA

PROCESSO 2238/2019

1. DO OBJETO

1.1 O objeto do presente termo de referência é a contratação de empresa especializada em soluções de telecomunicações visando o fornecimento e instalação de LINK DE INTERNET DEDICADO com velocidade, serviço de gerenciamento de rede e segurança – FIREWALL, obrigatoriamente via fibra óptica, incluindo instalação, manutenção e serviços técnicos durante a vigência do contrato, para atender as necessidades da Prefeitura Municipal de Itaboraí.

1.2 O objeto a ser contratado compreende:

1.2.1 Prestação de serviços de telecomunicações, com outorga e autorizada pela ANATEL – Agência Nacional de Telecomunicações, aquisição de solução de segurança de rede e performance, envolvendo o fornecimento de equipamentos com software e licenças, bem como serviços de instalação, operação assistida e suporte técnico, visando o fornecimento e instalação de link de internet dedicado, entregue por meio físico, obrigatoriamente por FIBRA ÓPTICA, suportando aplicações TCP/IP, gerenciamento Anti-DDos e gerenciamento dos circuitos de dados/Rede (NOC) contendo monitoramento proativo, registro e relatório de incidentes, relatório de tráfego cursado, relatório técnico de incidentes, agilização de incidentes, monitoramento proativo, conforme especificações contidas abaixo.

2. DA JUSTIFICATIVA DA CONTRATAÇÃO E BENEFÍCIOS ESPERADOS

2.1 Atualmente, a Prefeitura Municipal de Itaboraí mantém contratado um link que é utilizado para acessos à Internet e divulgação de seus serviços ao público externo. Na arquitetura atual, o link é responsável por sustentar toda utilização da Internet dentro do órgão e todos serviços disponíveis ao público externo.

2.2 A crescente demanda por serviços e sistemas de TI utilizados pela Prefeitura, sobretudo após a adoção do Sistema Integrado de Gestão Pública rodando em "nuvem", cria a necessidade, mais do que prioritária, de que se realize novo

procedimento licitatório para a contratação do objeto deste Termo, que será utilizado como **link de redundância**.

2.3 Esse cenário contempla o fato de que o link de INTERNET exerce papel preponderante para que a Prefeitura consiga satisfazer, com efetividade, sua missão institucional fornecendo diversos serviços à população, bem como a utilização dos diversos módulos do Sistema de Gestão relacionados à atividade final da Administração Municipal. Vários desses, além de críticos, necessitam de conexões que garantam alta disponibilidade, pois devem estar em funcionamento permanentemente, vez que falhas em sua operação impactam diretamente no cumprimento da missão institucional do Município.

3. ESPECIFICAÇÃO DOS SERVIÇOS A SEREM CONTRATADOS

3.1 ***Caberá a CONTRATADA dimensionar a estrutura necessária, incluindo recursos humanos, a atender as necessidades da Prefeitura Municipal de Itaboraí tendo como base as características, as especificidades dos serviços, as atividades a serem executadas, o perfil da equipe e a qualificação necessária dos profissionais.***

Item	Serviço	Descrição Resumida
1	Fornecimento de Link de Internet Dedicado de 500Mbps.	O link de acesso à internet deverá ter a velocidade de 500Mpbs dedicados e descontados qualquer "overhead" de protocolo; Fornecer endereços IP válidos classe C; Pelo menos 10 (dez) endereços IPs, contínuos, fixos e válidos, para uso da PMI; Garantia de utilização de 100% da largura de banda contratada; A contratada deverá possuir central de monitoração (NOC) do seu próprio backbone, em regime 24x7, objetivando impedir ataques de DoS (Denial of Service) e DDoS (Ditributed Denial of Service).

4. DAS CONDIÇÕES PARA EXECUÇÃO DOS SERVIÇOS

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

4.2 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.

4.3 A CONTRATADA deverá dispor e fornecer a CONTRATANTE ferramentas automatizadas de Gerência Proativa – com implantação de um NOC (Network Operation Center) 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.

4.4 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.

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

4.6 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.

4.7 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.

4.8 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.

4.9 Eventuais interrupções programadas dos serviços deverão ser informadas com antecedência mínima de 05 (cinco) dias.

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

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

4.12 No caso de utilização de múltiplos links físicos, a CONTRATADA deverá garantir que a carga deles seja balanceada automaticamente de forma a se obter-se a velocidade total adquirida.

4.13 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.

4.14 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.

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

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

4.17 A prestação do serviço compreende a disponibilização, instalação, ativação e configuração do(s) equipamento(s) que compõem o acesso, e outros que possibilitem a utilização do serviço objeto da presente contratação.

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

4.19 A escolha da solução (equipamentos) adotada fica a critério da CONTRATADA.

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

4.21 O serviço IP dedicado a ser contratado deverá suportar aplicações TCP/IP (Transmission Control Protocol / Internet Protocol), tais como: HTTP, HTTPS, FTP (File Transfer Protocol), SSH (Secure SHell), SMTP (Simple Mail Transfer Protocol), POP3 (Post Office Protocol version 3), LDAP (Lightweight Directory 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.

4.22 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.

4.23 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.

4.24 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.

4.25 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.

4.26 Serviço Anti-DDos:

4.26.1 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 – Denial of Service) e do tipo negação de serviço distribuído (DDoS – distributed Denial of Service).

4.26.2 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.

4.26.3 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.

4.26.4 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.

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

4.26.6 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.

4.26.7 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.

4.26.8 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, Ping of Death e Fragmentação excessiva.

4.26.9 A CONTRATADA deve disponibilizar uma Central de Atendimento, com equipe especializada (SOC – Security Operation Center) 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.

4.26.10 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).

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

4.26.12 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.

4.27 Requisitos para o Gerenciamento da Rede (NOC)

4.27.1 O Centro de Operação de Redes (NOC – Network Operations Center) da CONTRATADA deverá atender aos requisitos mínimos de serviços

especificados neste Termo de Referência, bem como TODOS os requisitos de infraestrutura apresentados a seguir:

4.27.1.1 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.

4.27.1.2 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).

4.27.1.3 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.

4.27.1.4 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.

4.27.1.5 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.

4.27.1.6 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.

4.27.1.7 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.

4.28 Help Desk

4.28.1 Deverá ser disponibilizado serviço de "help desk", 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.

4.29 Gerenciamento Proativo

4.29.1 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.

4.29.2 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.

4.30 Acordo de Níveis de Serviço – ANS

4.30.1 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.

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

4.31 Disponibilidade do Serviço

4.31.1 O serviço será considerado DISPONÍVEL quando, cumulativamente: 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 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 DISPONIVEL]);
- [Tempo Total] = 43.200 minutos;

4.31.2 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.

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

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

4.32 Gerenciamento Unificado de Ameaças

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

Serviço 1: Solução de segurança de rede de computadores

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

Serviço 3: Instalação, suporte e garantias

4.32.2 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;

4.32.3 Os Appliances devem possuir no mínimo as seguintes certificações:

- FIPS140-2 Level 2 para Firewall;
- Certificação Common Criteria como EAL4+;
- Certificação ICSA para o Firewall;
- Certificação ICSA IPSEC. (VPN IPSec).

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

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

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

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

4.32.8 **Serviço 1 - Solução de segurança de rede de computadores**

4.32.8.1 Descrição

a) Solução de proteção de rede com características de Next Generation Firewall (NGFW) ou Unified Threat 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;

4.32.8.2 Capacidades e Quantidades

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

a) Throughput de 2.5 Gbps de Firewall;
b) Throughput de 400 Mbps de VPN IPSec;
c) Throughput de 900 Mbps de IPS;
d) Throughput de 300 Mbps de Antivirus/Antimalware;
e) Suporte a, no mínimo, 2.5 milhões de conexões simultâneas;
f) Suporte a, no mínimo, 20 mil novas conexões por segundo;
g) Fonte 120/240 AC;
h) Disco interno de, no mínimo, 100 GB;
i) 12 (doze) interfaces de rede 1000 base-TX;
j) 2 (duas) interfaces de rede 1 Gbps SPF;
k) 2 (duas) interfaces para HA;
l) Suporte a, no mínimo, 6 (seis) contextos virtuais com domínios de roteamento individuais;
m) Estar licenciada para ou suportar sem o uso de licença, 300 (trezentos) clientes de VPN SSL simultâneos;
n) Estar licenciada para ou suportar sem o uso de licença, 2.000 (dois mil) túneis de VPN IPSEC simultâneos;
o) Atender a demanda de pelo menos 600 (seiscentos) usuários de Internet.

4.32.8.3 Características Gerais

a) O hardware e software que execute as funcionalidades de proteção de rede, bem como a console de gerência e monitoração, 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.

4.32.8.4 Firewall

a) Suporte a objetos e regras em IPv4 e IPv6;
b) Suporte a objetos e regras multicast;
c) Controle de políticas por porta e protocolo;
d) Controle de políticas por usuários, grupos de usuários, IPs e redes;
e) Controle de políticas por código de País utilizando GeoIP (Por exemplo: Brasil, Estados Unidos, China, Russia);
f) Deve suportar offload de certificado em inspeção de conexões SSL de entrada (Inbound);
g) Controle de inspeção e de-criptografia de SSH por política;
h) Permitir controle de acesso à internet por períodos do dia, permitindo a aplicação de políticas por horários e por dia da semana;
i) Deve permitir o funcionamento em modo transparente tipo "bridge" sem alterar o endereço MAC do tráfego;
j) Permitir filtro de pacotes sem controle de estado "stateless" para verificação em camada 2;
k) Permitir forwarding de camada 2 para protocolos não IP;
l) Permitir criação de serviços por porta ou conjunto de portas dos seguintes protocolos, TCP, UDP, ICMP e IP;
m) Permitir o agrupamento de serviços;
n) Permitir a abertura de novas portas por fluxo de dados para serviços que requerem portas dinâmicas, inclusive aplicações multimídia como H.323 e SIP;
o) Possuir mecanismo de anti-spoofing;
p) Permitir o serviço de autenticação para tráfego HTTP e FTP;
q) 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;
r) Deve possuir a funcionalidade de balanceamento e contingência de links;
s) Deve permitir o filtro de pacotes sem a utilização de NAT;

4.32.8.5 Deve suportar os seguintes tipos de NAT

a) DNAT (Destination NAT) com PAT (Port Address Translation);

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 port translated;
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;

4.32.8.6 IPS

a) Por IPS (Intrusion Prevention System), entenda-se Sistema de Prevenção de Intrusos;
b) Deverá ser orientado à proteção de redes IP;
c) Possuir tecnologia de detecção baseada em assinatura com pelo menos 4000 vacinas
d) disponíveis contra ataques conhecidos;
e) Possuir capacidade de remontagem de pacotes para identificação de ataques;
f) 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;
g) Possuir capacidade de criação de assinaturas customizadas pela interface gráfica do produto;
h) Atualizar automaticamente as assinaturas utilizando rede / Internet ou através de atualização manual;
i) Deverá ter a funcionalidade de configurar a função de IPS como modo passivo para monitoramento.

4.32.8.7 Mecanismos de detecção/proteção de ataques

a) Reconhecimento de padrões;
b) Análise de protocolos;
c) Detecção de anomalias;
d) Detecção de ataques de Fragmentação RPC;
e) Detecção de ataques de Fragmentação e Desfragmentação IP;
f) Detecção de ataques de Segmentação TCP;
g) Proteção contra ataques de Windows ou NetBios;

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

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

j) Proteção contra-ataques DNS (Domain Name System);

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

l) Proteção contra-ataques de ICMP (Internet Control Message Protocol);

m) Suportar verificação de ataque nas camadas de aplicação;

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

4.32.8.8 Métodos de notificação

a) Alarmes na console de administração.

b) Alertas via correio eletrônico.

c) Monitoração 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.

d) Terminação de sessões via TCP resets.

e) Armazenamento de logs de sessões;

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

4.32.8.9 Filtro de URL (WebFilter)

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

b) Possuir pelo menos 60 categorias para classificação de sites web;

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

d) Possuir a funcionalidade de cota de tempo de utilização por categoria;

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

- Proxy Anônimo;
- Webmail;
- Instituições de Saúde;
- Notícias e Esportes;
- Phishing;

- Hackers;
- Pornografia;
- Racismo;
- Governo
- Compras;
- Pedofilia;

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

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

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

i) 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;

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

k) Prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory (Single Sign On);

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

m) 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;

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

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

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

q) Filtro de conteúdo baseado em categorias em tempo real;

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

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

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

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

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

w) Deverá permitir o bloqueio de redirecionamento HTTP;

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

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

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

4.32.8.10 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;

b) Deverá reconhecer no mínimo 2000 aplicações;

c) Deverá possuir pelo menos 10 categorias para classificação de aplicações;

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

- P2P;
- Audio e vídeo;
- Proxy;
- Update;
- VoIP.

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

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

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

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

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

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

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

l) 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;

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

n) 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;

o) 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;

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

q) 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;

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

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

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

u) Deve alertar o usuário quando uma aplicação foi bloqueada;

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

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

- Tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc);
- Nível de risco da aplicação;
- Categoria e sub-categoria de aplicações;
- Aplicações que usem técnicas evasivas, utilizadas por malwares, como transferência de arquivos e/ou uso excessivo de banda.

4.32.8.11 VPN

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

b) Possuir autenticação baseada em MD5 e SHA-1;

c) Suporte a Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;

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

e) Possuir suporte a VPNs IPSec site-to-site, VPNs IPSec client-to-site;

f) Possuir suporte a VPN SSL;

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

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

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

j) Suporte a VPN do tipo PPTP, L2TP;

k) Suporte à inclusão em autoridades certificadoras (enrollment) mediante SCEP; (Simple Certificate Enrollment Protocol) e mediante arquivos;

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

m) Atribuição de endereço IP nos clientes remotos de VPN;

n) Atribuição de DNS nos clientes remotos de VPN;

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

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;

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

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

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;

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

u) Possuir interoperabilidade com os seguintes fabricantes:

- Cisco;
- HP;
- Dell;
- Mikrotik;
- Checkpoint;
- Juniper;

- Palo Alto Networks;
- Fortinet;
- Sonic Wall;

4.32.8.12 Traffic Shapping / QoS

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;

b) Permitir modificação de valores DSCP para o DiffServ;

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

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

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

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

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

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

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

j) O QoS deve possibilitar a definição de classes por:

- Banda Garantida
- Banda Máxima
- Fila de Prioridade.

4.32.8.13 Antivirus e Antimalware

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

b) 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;
c) Suportar o bloqueio de malwares (adware, spyware, hijackers, keyloggers, etc.);
d) Suportar o bloqueio de download de arquivos por extensão, nome do arquivo e tipos de arquivo;
e) Suportar o bloqueio de download de arquivos por tamanho;
f) Suportar a análise de arquivos executáveis, DLLs, ZIP e criptografados em SSL;
g) Suportar o bloqueio através de assinaturas;
h) Suportar o bloqueio de Botnets;
i) Caso ocorra a detecção de malware nos protocolos HTTP e HTTPS apresentar uma mensagem customizável ao usuário final;

4.32.8.14 Balanceamento de Carga (Proxy Reverso)

a) Permitir a criação de endereços IPs virtuais;
b) Permitir balanceamento de carga entre pelo menos 2 servidores reais;
c) Suportar balanceamento ao menos para os seguintes serviços: HTTP, HTTPS, TCP e UDP;
d) Permitir balanceamento ao menos com os seguintes métodos: hash do endereço IP de origem, Round Robin, Weighted, First alive e HTTP Host;
e) Permitir persistência de sessão por cookie HTTP ou SSL session ID;
f) Suportar SSL offloading;
g) Deve ter a capacidade de identificar, através de health checks, quais os servidores que estejam ativos, removendo automaticamente o tráfego dos servidores que não estejam;
h) Permitir que o health check seja feito ao menos via ICMP, TCP em porta configurável e HTTP em URL configurável.

4.32.8.15 Roteamento

a) Suporte a rota estática;
b) Suporte a ECMP (Equal-cost multi-path routing) com metodo de balanceamento outbound de rotas;

c) Suporte a Policy-Based Routing por origem, destino, protocolo e interface;

d) Suportar os seguintes protocolos de roteamento dinâmico:

- RIPv2 para IPv4;
- OSPF para IPv4;
- BGP para IPv4;
- RIPng para IPv6;
- OSPFv3 para IPv6;
- BGP para IPv6;

4.32.8.16 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;

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

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

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

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

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

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

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

i) 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;

j) 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.

4.32.8.17 Funcionalidades Gerais

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

b) Possuir controle de acesso à rede por subrede;

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

d) Active Directory para autenticação de usuários administradores e usuários de firewall;

e) 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

f) deste e demais itens;

g) 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;

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

i) Suporte a autenticação baseada em Token;

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

k) Suporte a sFlow;

l) Suporte a tags de VLAN (802.1q);

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

n) Possuir ferramenta de diagnóstico do tipo TCPdump;

o) Possuir funcionalidades de DHCP Cliente, Servidor e Relay;

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

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

r) 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);

s) Deve implementar VRRP (Virtual Router Redundancy Protocol);

t) Deve implementar Firewall dual stack para IPv4/IPv6;

u) Permitir importação de certificados digitais para funcionalidades gerais do equipamento;

v) Possuir monitoramento SNMP v2c e v3;

w) Possuir MIB para integração com sistema de monitoramento SNMP;

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

y) 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;

z) Possuir certificado ICSA para Firewall;

aa) Possuir certificação FIPS 140-2 para firewall;

bb) Possuir certificação Common Criteria como EAL4+.

4.32.8.18 Suporte e Voip

a) Possuir suporte a SIP e H 323;

b) 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;

4.32.9 Serviço 2 - Solução de armazenamento de logs e emissão de relatórios

4.32.9.1 Descrição

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

4.32.9.2 Funcionalidades

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

b) A solução pode ser fornecida nas seguintes condições:
- Hardware do tipo appliance dedicado;
- Solução Cloud – Com administração e armazenamento baseado em nuvem. Sem a necessidade de instalação de dispositivo local;

c) Possuir comunicação entre os componentes de forma criptografada;

d) Possui armazenamento de logs total de pelo menos 500GB;

e) Possuir perfis administrativos com capacidade de criar ao menos 2 (dois) perfis para monitoração dos logs;

f) Possuir a visualização de log em tempo real de tráfegos de rede;

g) Permitir a visualização de logs de histórico dos acessos de tráfegos de rede;

h) Permitir a visualização dos eventos de auditoria;

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

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

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

l) Permitir customização dos relatórios, incluindo logotipo customizado;

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

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

o) Possuir pelo menos os relatórios seguintes relatórios:
- 100 (dez) sites web mais acessados
- 100 (dez) categorias de sites web mais acessados
- 100 (dez) usuários mais ativos na rede
- 100 (dez) aplicativos mais acessados
- Tráfego baseado em IP
- Ataques baseado em origem e destino
- Vírus detectado por origem e destino

4.32.10 Serviço 3 - Instalação, suporte e garantias

4.32.10.1 Instalação

a) Os Serviços deverão ser instalados e configurados pela CONTRATADA in loco no ambiente da CONTRATANTE;
b) A CONTRANTE será responsável por dar como completo toda a instalação e configuração após validação de todas as funcionalidades;

4.32.10.2 Suporte

a) Assistência técnica e suporte ambos por telefone e web, incluindo a operação assistida do conjunto fornecido, substituição de peças e equipamentos pelo prazo de 12 (doze) meses;
b) Abertura de chamados e o atendimento junto à CONTRATADA deverão ser feitos em português, durante todo o prazo de vigência do contrato;
c) 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;
d) Por assistência técnica entende-se o serviço de manutenção corretiva, reparo e substituição de equipamentos e peças sem ônus a CONTRATANTE;
e) Atendimento via telefone 0800 (ligação gratuita), inclusive de telefone móvel ou número local do município de Itaboraí - RJ (DDD 21);
f) Sistema de Help Desk online para abertura de chamados. Os chamados deverão ficar armazenados e identificados com uma numeração única para cada chamado;
g) O sistema de Help Desk deverá fornecer histórico de todos chamados abertos e fechados;
h) Os chamados devem ser abertos via e-mail ou via Portal Web próprio para abertura dos chamados;
i) O Portal de abertura de chamados deve manter os dados da Prefeitura de Itaboraí/RJ totalmente sigilosos e criptografados incluindo sua transmissão (SSL / HTTPS);

j) 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;

k) Garantia de atendimento de número ilimitado de chamados;

l) 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.

4.32.10.3 Garantias

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

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

4.32.11 **Disponibilidade do Serviço**

4.32.11.1 O serviço será considerado DISPONÍVEL quando, cumulativamente:

a) 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;

b) 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;

c) 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.

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

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

5. DA SUBCONTRATAÇÃO

5.1 É vedada a subcontratação, visto que os trabalhos deverão ser desenvolvidos por profissionais, observada a legislação trabalhista em vigor.

6. DOS PADRÕES

6.1 A CONTRATADA se compromete a obedecer a todas as normas da ANATEL, padrões ABNT, processos e procedimentos da Prefeitura Municipal de Itaboraí.

7. DO ACOMPANHAMENTO E FISCALIZAÇÃO DO CONTRATO

7.1 Não obstante a CONTRATADA seja a única e exclusiva responsável pela execução dos serviços contratados, o CONTRATANTE reserva-se ao direito de exercer a mais ampla e completa fiscalização sobre a execução desses serviços, não restringindo em nada a responsabilidade da CONTRATADA;

7.2 Nos termos do Art. 67, §1º, da Lei Federal nº 8.666/93, o CONTRATANTE designará servidor (es) para acompanhar e fiscalizar a execução do Contrato, anotando em registro próprio todas as ocorrências relacionadas com a execução e

determinando o que for necessário à regularização das falhas ou defeitos observados;

7.2.1 As decisões e providências que ultrapassarem a competência do (s) servidor (es) designado (s) deverão ser encaminhadas ao Gestor do Contrato, em tempo hábil para adoção das medidas convenientes;

7.3 A execução dos serviços contratados será fiscalizada por equipe de servidores especificamente designada para essa finalidade pelo CONTRATANTE, cujas atribuições básicas são:

7.3.1 Solicitar à CONTRATADA e ao Gestor do Contrato por ela indicado todas as providências necessárias ao bom andamento dos serviços;

7.3.2 Solicitar à CONTRATADA a regularização de serviços que não atendam às especificações definidas neste instrumento e/ou às necessidades requeridas para execução destes;

7.3.3 Quaisquer outras atribuições necessárias ao bom desempenho dos serviços contratados;

7.4 Da mesma forma, a CONTRATADA deverá indicar um preposto para representá-la na execução do Contrato;

7.5 Nos termos da Lei Federal nº 8.666/93, constituirá documento de autorização para a execução dos serviços o Contrato devidamente assinado pelas partes, acompanhado da Ordem de Início dos Serviços;

7.6 Quaisquer exigências da fiscalização, inerentes ao objeto do Contrato, deverão ser prontamente atendidas pela CONTRATADA, sem ônus para o CONTRATANTE.

8. OBRIGAÇÕES DA CONTRATANTE

8.1 Permitir ao pessoal técnico da CONTRATADA, desde que identificado e incluído na relação de técnicos autorizados, o acesso às unidades para a execução das atividades, respeitadas as normas de segurança vigentes nas suas dependências.

8.2 Notificar a contratada quanto a defeitos ou irregularidades verificadas na execução das atividades objeto deste Termo de Referência, bem como quanto a qualquer ocorrência relativa ao comportamento de seus técnicos, quando em atendimento, que venha a ser considerado prejudicial ou inconveniente para a Prefeitura Municipal de Itaboraí.

8.3 Efetuar os pagamentos devidos à CONTRATADA, na forma convencionada, dentro do prazo previsto, desde que atendidas às formalidades necessárias, após a aceitação dos itens faturados.

8.4 Encaminhar à CONTRATADA as solicitações de suporte com as necessidades a serem realizadas.

8.5 Indicar os locais onde serão desenvolvidos os serviços e proporcionar à CONTRATADA as facilidades e instruções necessárias para a realização deles.

8.6 Verificar a regularidade da situação fiscal e dos recolhimentos sociais trabalhistas da contratada conforme determina a lei, antes de efetuar o pagamento devido.

8.7 Promover a fiscalização do contrato, sob os aspectos quantitativo e qualitativo, por intermédio de profissional designado, anotando em registro próprio as falhas detectadas e exigindo as medidas corretivas necessárias, bem como acompanhar o desenvolvimento do contrato, conferir os serviços executados e atestar os documentos fiscais pertinentes, quando comprovada a execução total, fiel e correta dos serviços, podendo ainda sustar, recusar, mandar fazer ou desfazer qualquer procedimento que não esteja de acordo com os termos contratuais.

8.8 Comunicar tempestivamente à CONTRATADA as possíveis irregularidades detectadas na execução das atividades.

8.9 Observar para que durante a vigência do contrato sejam cumpridas as obrigações assumidas pela CONTRATADA, bem como sejam mantidas todas as condições de qualificação exigidas no processo de contratação.

9. OBRIGAÇÕES DA CONTRATADA

9.1 Compete à empresa CONTRATADA, a execução das atividades na forma estipulada no presente Termo de Referência.

9.2 Indenizar à Prefeitura Municipal de Itaboraí nos casos de danos, prejuízos, avarias ou subtração de seus bens ou valores, bem como por acesso e uso indevido a informações sigilosas ou de uso restrito, quando tais atos forem praticados por quem tenha sido alocado à execução do objeto do contrato, desde que devidamente identificado.

9.3 Responsabilizar-se integralmente pela execução das atividades contratadas, nos termos da legislação vigente, de modo que eles sejam realizados com esmero e

perfeição, sob sua inteira e exclusiva responsabilidade, obedecendo às normas e rotinas da Prefeitura Municipal de Itaboraí, em especial as que digam respeito à segurança, à confiabilidade e à integridade.

9.4 Assinar termo de responsabilidade e sigilo, comprometendo-se a não comentar nenhum assunto tratado nas dependências da Prefeitura Municipal de Itaboraí ou a serviço deste, salvo se expressamente autorizado por representante legal da Prefeitura Municipal de Itaboraí.

9.5 Estar ciente de que a estrutura computacional disponibilizada pela Prefeitura Municipal de Itaboraí não poderá ser utilizada para fins particulares, e que a navegação em sítios da Internet e as correspondências em meio eletrônico utilizando o endereço da Prefeitura Municipal de Itaboraí ou acessado a partir dos seus equipamentos poderão ser auditadas.

9.6 Responsabilizar-se pelo comportamento dos seus empregados e por quaisquer danos que estes ou seus prepostos venham porventura ocasionar à Prefeitura Municipal de Itaboraí, ou a terceiros, durante a execução dos serviços, podendo a Prefeitura Municipal de Itaboraí, descontar o valor correspondente ao dano dos pagamentos devidos.

9.7 Manter durante a vigência contratual, todas as condições que ensejaram a sua contratação.

9.8 Manter seus empregados, durante o horário de prestação do serviço, quando nas dependências da Prefeitura Municipal de Itaboraí, devidamente identificados mediante uso permanente de crachá.

9.9 Cumprir e fazer cumprir por seus empregados as normas e regulamentos disciplinares da Prefeitura Municipal de Itaboraí, bem como quaisquer determinações emanadas das autoridades competentes.

9.10 Providenciar a imediata correção das deficiências apontadas pela Prefeitura Municipal de Itaboraí quanto à execução das atividades previstas.

9.11 Comunicar, de forma detalhada, toda e qualquer ocorrência de acidentes verificada no curso da execução contratual.

9.12 Encaminhar expediente à Prefeitura Municipal de Itaboraí, informando os nomes dos técnicos que estão autorizados a executar as atividades contratadas.

9.13 Fiscalizar o cumprimento do objeto do contrato, cabendo-lhe integralmente os ônus decorrentes, fiscalização essa que se dará independentemente da que será exercida pela Prefeitura Municipal de Itaboraí.

9.14 Manter durante toda a vigência do contrato os profissionais alocados no mesmo com as competências, ferramentas necessárias e certificações exigidas nas descrições dos serviços, bem como capacitá-los nas tecnologias que eventualmente venham a ser utilizadas durante sua execução. Tal qualificação sempre que exigida pela Prefeitura Municipal de Itaboraí, deverá ser comprovada por Currículos delimitados pela Prefeitura Municipal de Itaboraí.

9.15 Pagar todos os impostos e taxas devidas sobre as atividades prestadas à Prefeitura Municipal de Itaboraí, bem como as contribuições à previdência social, encargos trabalhistas, prêmios de seguro e acidentes de trabalho, emolumentos, quaisquer insumos e outras despesas diretas e indiretas que se façam necessárias à execução dos serviços contratados.

9.16 Manter ainda rigorosamente em dia todas as obrigações devidas aos funcionários previstas no Acordo Coletivo de Trabalho em vigor. A não comprovação de qualquer dos pagamentos impedirá a CONTRATANTE do pagamento da fatura até a regularização completa de todas as obrigações devidas. O descumprimento das obrigações trabalhistas, previdenciárias e as relativas ao FGTS ensejarão o pagamento em juízo dos valores em débito, sem prejuízo das sanções cabíveis.

9.17 Tomar todas as providências e obrigações estabelecidas na legislação específica de acidentes de trabalho, quando, em ocorrências da espécie forem vítimas os seus empregados, no desempenho dos serviços ou em conexão com eles, ainda que verificadas nas dependências da Prefeitura Municipal de Itaboraí.

9.18 A seleção, a designação e a manutenção do quadro de profissionais alocados ao contrato são de exclusiva responsabilidade da CONTRATADA.

9.19 Sempre que necessária à alocação de novos recursos, para fazer frente às suas necessidades, a Prefeitura Municipal de Itaboraí formalizará a solicitação através de documento formal.

9.20 Manter com vínculo empregatício, atendendo as legislações trabalhistas em vigor todos os profissionais constantes do seu quadro permanente, que estejam dedicados à execução dos serviços contratados.

9.21 Informar outorgas da ANATEL para execução dos serviços contratados, lembrando que todos os equipamentos utilizados na execução do objeto deverão estar homologados pela Anatel.

9.22 A manter consistentes e atualizados todos os artefatos produzidos e/ou alterados durante a execução dos serviços contratados:

9.23 Garantir que todas as entregas efetuadas estejam compatíveis e totalmente aderentes aos serviços utilizados, cabendo à Prefeitura Municipal de Itaboraí tomar ciência e autorizar o uso de ferramentas cuja versão seja diferente daquelas previstas e em uso.

9.24 Em caso de alteração em quaisquer tecnologias utilizadas pela Prefeitura Municipal de Itaboraí, ela notificará a CONTRATADA com antecedência de 60 (sessenta) dias, para que a mesma possa se adequar e manter os mesmos níveis de serviço, ficando a critério da Prefeitura Municipal de Itaboraí a decisão de quais tecnologias adotar.

9.25 Fornecer a largura de banda solicitada, via conexão física com suporte a tráfego real de dados na velocidade de 500Mbps. O valor contratado sempre será referente a largura de banda líquida ou efetiva.

9.26 A CONTRATADA deverá disponibilizar um bloco de 10 (dez) endereços IP contínuo, classe C, para uso da Prefeitura de Itaboraí.

10. DA TRANSIÇÃO DOS SERVIÇOS E TRANSFERÊNCIA DE TECNOLOGIA

10.1 A contratada deverá 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.

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

11. DA FORMA DE COMUNICAÇÃO E RELACIONAMENTO

11.1 A CONTRATADA deverá utilizar os canais de comunicação propostos pela Prefeitura Municipal de Itaboraí para o seu relacionamento;

11.2 A CONTRATADA deverá 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.

12. DOS PRAZOS DE VIGÊNCIA CONTRATUAL E DO INÍCIO DA EXECUÇÃO DOS SERVIÇOS

12.1 A vigência do Contrato assinado em decorrência da Licitação será de **12 (doze)** meses consecutivos, contados a partir da assinatura do respectivo instrumento contratual e recebimento da Ordem de Início dos Serviços, a ser emitida pelo Gestor do Contrato;

12.2 O prazo de vigência contratual poderá ser prorrogado até o limite de **60 (sessenta)** meses, conforme previsão expressa no inciso II do artigo 57 da Lei nº 8.666/93, haja vista a definição de essencialidade constante da Resolução SEMCTIDS nº 01/2019, desde que haja autorização formal da autoridade competente e observados os seguintes requisitos:

12.2.1 Os serviços tenham sido prestados regularmente;

12.2.2 A Administração mantenha interesse na realização do serviço;

12.2.3 O valor do contrato permaneça economicamente vantajoso para a Administração Municipal;

12.2.4 A CONTRATADA manifeste expressamente interesse na prorrogação.

12.3 A CONTRATADA não tem direito subjetivo à prorrogação contratual, que objetiva a obtenção de preços e condições mais vantajosas para a Administração, conforme estabelece a Lei de Licitações nº 8.666/93;

12.4 Os prazos de início e de entrega admitem prorrogação, a critério do Município de Itaboraí, devendo ser justificada por escrito e previamente autorizada pela Administração Municipal, desde que ocorra algum dos seguintes motivos:

12.4.1 Superveniência de fato excepcional e imprevisível, estranho à vontade das partes, que altere fundamentalmente as condições de execução do Contrato;

12.4.2 Interrupção da execução do Contrato ou diminuição do ritmo de trabalho por ordem e interesse da Administração Municipal;

12.4.3 Impedimento de execução do Contrato por fato ou ato de terceiros reconhecidos pela Administração Municipal em documentos contemporâneos a sua ocorrência;

12.4.4 Omissão ou atraso de providências a cargo da Administração Municipal, inclusive quanto aos pagamentos previstos de que resulte diretamente impedimento ou retardamento na execução do Contrato, sem prejuízo das sanções legais aplicáveis aos responsáveis;

13.DAS CONDIÇÕES DE PAGAMENTO

13.1 O pagamento será realizado em favor da CONTRATADA em até 30 (trinta) dias após o adimplemento da obrigação e apresentação da Nota Fiscal / Fatura, devidamente atestada por dois servidores.

14.DOS PREÇOS

14.1 Nos preços deverão estar inclusas todas as incidências fiscais, tributárias, trabalhistas, previdenciárias e demais encargos, que correrão por sua conta e responsabilidade, estando também abrangidas as despesas de transporte, hospedagem, alimentação, necessários à implantação e operacionalização do objeto deste Termo de Referência.

14.2 Os preços serão fixos e irreajustáveis pelo período de 12 (doze) meses;

14.3 Havendo prorrogação do Contrato, o preço mensal poderá ser reajustado a partir do 13º (décimo terceiro) mês, de acordo com a variação do Índice Geral de Preços de Mercado - IGPM/FGV, em conformidade com a legislação em vigor, tomando-se por base o índice vigente no mês da apresentação da proposta em relação ao do mês do reajustamento devido;

15.DOS RECURSOS ORÇAMENTÁRIOS

15.1 Os recursos para a contratação dos serviços estão programados em dotações orçamentárias previstas no orçamento municipal para o exercício de 2019, na classificação abaixo:

#	**Programa de Trabalho**	**Natureza da Despesa**	**Fonte de Recursos**
1	26.001.001 – 04.122.0012.2.173	3.3.90.40.13 – Comunicação de Dados e redes em geral	01 – Tesouro Municipal

15.2 A despesa para o exercício fiscal subsequente será alocada na dotação orçamentária prevista para atendimento dessa finalidade, a ser consignada à CONTRATANTE, na Lei Orçamentaria Anual.

16.DISPOSIÇÕES GERAIS

16.1 A CONTRATADA será a única e exclusiva responsável pela execução das atividades, reservando-se à Prefeitura Municipal de Itaboraí o direito de exercer a mais ampla e completa fiscalização dessas atividades.

16.2 A critério da Prefeitura Municipal de Itaboraí, nos casos de manutenções preventivas e com prévia comunicação de 05 (cinco) dias úteis, poderá ocorrer a alteração do horário de prestação de serviço.

16.3 A critério da Prefeitura Municipal de Itaboraí, nos casos de manutenções corretivas, o horário de prestação de serviços poderá ser modificado imediatamente após a comunicação oficial.

16.4 A alteração de horário indicado poderá incorrer em sábados, domingos e/ou feriados, para implementações, melhorias, manutenções e demais atividades que se fizerem necessárias. Isso se deve ao fato de não causar impacto, indisponibilidade ou outros incidentes durante o horário de funcionamento da Prefeitura Municipal de Itaboraí.

16.5 A CONTRATADA não poderá divulgar quaisquer informações a que tenha acesso em virtude dos trabalhos a serem executados ou de que tenha tomado conhecimento em decorrência da execução do objeto, sem autorização, por escrito, da Prefeitura Municipal de Itaboraí, sob pena de aplicação das sanções cabíveis, além do pagamento de indenização por perdas e danos.

16.6 O prazo máximo para a execução dos serviços será de 48 (quarenta e oito) horas a contar da data da Ordem de Início dos serviços emitida pela CONTRATANTE.

16.7 A validade das propostas não deverá ser inferior a 60 (sessenta) dias, contados a partir da sua apresentação.

16.8 Todos os atos inerentes ao presente Termo, bem como todos os envolvidos sujeitam-se integralmente as normas legais vigentes, especialmente a Lei 8.666/93, e suas alterações.

16.9 Todas as informações constantes neste Termo de Referência, são suficientes para o completo dimensionamento dos volumes de serviços pela CONTRATADA.

16.10 A CONTRATADA não poderá se valer do contrato a ser celebrado para assumir obrigações perante terceiros, dando-o como garantia, nem utilizar os direitos de crédito, a serem auferidos em função das atividades prestadas, em quaisquer operações de desconto bancário, sem prévia autorização da Prefeitura Municipal de Itaboraí, sob pena de incorrer em quebra de cláusula contratual ensejando, inclusive, sua rescisão de pleno direito.

Itaboraí, 16 de setembro de 2019.

Cezar Caetano Sabiá Neto
Assessor Técnico
Matrícula 35.998

Edson Neira Brandão
Secretário Municipal de Ciência, Tecnologia,
Inovação e Desenvolvimento Sustentável
Matrícula 18.353