TERMO DE REFERÊNCIA

I - INFORMAÇÕES PRIMÁRIAS SOBRE A DESPESA

1.ÓRGÃO SOLICITANTE:

Secretaria de Estado da Educação, Cultura e Esportes - SEE

2.TERMO DE REFERÊNCIA

2.1. Número da Unidade Orçamentária: 717.001.4288.0000 e 717.601.4434.0000
2.2. Programa: Garantir a Funcionalidade das Unidades Escolares e Administrativas da SEE
2.3. Elemento de despesa: 44.90.52.00
2.4. Fontes de Recurso: 100 (RP) E 300 (FUNDEB)

3.DESCRIÇÃO DE CATEGORIA DE INVESTIMENTO:

( ) Capacitação

( ) Equipamento de Apoio

( ) Equipamento de TI

( ) Consultoria/Auditoria/Assessoria

(X) Despesa de Custeio

( ) Bens de Consumo

( ) Material Permanente

4.UNIDADE ADMINISTRATIVA SOLICITANTE: Departamento de Tecnologias Educacionais e da Informação – DETEI.

5. DO OBJETO

5.1. Registro de preços para eventual e futura contratação de empresa especializada para prestação de serviços de telecomunicações, objetivando o fornecimento de solução segura de comunicação de dados bidirecional através do uso de VSATS (Very Small Aperture Terminals), em banda KA, compreendendo conexões IP para integração das unidades da Secretaria de Estado de Educação, Cultura e Esportes - SEE. Nas diversas regiões do estado, incluindo o fornecimento de enlaces de comunicação de dados e solução de segurança, respectivos

equipamentos e insumos necessários, serviços de entrega, ativação, operação, manutenção, treinamento e gerência, conforme especificações técnicas e demais condições contidas neste Termo de Referência.

6. DA JUSTIFICATIVA

6.1. De acordo com relatório técnico elaborado por este Departamento de Tecnologia e Informação, após visita às Escolas da Rede Pública Estadual e Núcleos de representação da Secretaria de Educação na Capital Rio Branco e nos 18 municípios que possuem acesso terrestre, verificou-se que grande parte das Escolas da Rede Pública Estadual, sobretudo as da Zona Rural, não possuem nenhum tipo de acesso à internet.

Atualmente há 623 (seiscentas e vinte e três) Escolas na Rede Pública Estadual, administradas pela Secretaria de Educação, e destas, apenas 270 possuem conexão de internet satisfatória. Sendo que as demais 353 Escolas, não possuem nenhum tipo de conexão de internet.

6.2. Ao nos depararmos com este cenário, buscamos algumas alternativas de levar conexão, através das políticas do Ministério da Educação e do Ministério das Ciências e Tecnologia. No Ministério da Educação há o Programa Escola Conectada, que repassa um pequeno recurso para as Escolas contratarem provedores de serviços de internet, porém, poucas escolas foram contempladas até o presente momento, tanto para acesso terrestre, quanto para acesso satelital.

6.3. Nesse interim, urge a necessidade de levarmos conectividade com a internet para uma parte das escolas, visto que a limitação orçamentária e financeira, nos impede de abranger as escolas em sua totalidade.

6.4. Importante mencionar, que a conectividade com a internet é fator primordial para melhorar a qualidade da educação, uma vez que promove a inclusão de alunos e professores no mundo digital, com acesso a plataformas de educação, vídeos educativos, bibliotecas virtuais, acesso à Sistemas de Gestão Educacionais, dentre outros diversos benefícios.

6.5. O Governo do Estado do Acre tem a necessidade de contratação de internet na modalidade de acesso por Satélite para atender as

unidades que integram as Secretarias do Governos Estado, nas mais diversas regiões conforme consta do quadro de distribuição em anexo, considerando que esta secretaria atende aproximadamente 50 mil alunos em escolas de campo, rurais e indígenas, e ainda as necessidades de administração escolar e administrativa de cada unidade, no que tange a abertura e acompanhamentos processuais que são online com a utilização obrigatória do Sistema Eletrônico de Informações-SEI, além de todas as atividades assessórias que precisem de comunicação com a internet.

6.6. A necessidade da licitação objeto deste edital decorre do objetivo do Governo do Estado do Acre em propiciar condições para elevar a produtividade das Secretarias de Estado e suas respectivas unidades, no desempenho de suas atribuições, permitindo a comunicação de dados eficiente, particularmente, em localidades onde inexiste infraestrutura terrestre para transporte de dados.

6.7. A solução apresentada deve contemplar

- Serviço mensal de suporte, manutenção e operação para cada unidade remota;
- Segmento espacial (banda internet) para unidades remotas;
- Rack para acomodação e proteção dos equipamentos;
- Equipamento de Segurança de Perímetro (Firewall) conforme exigido pelo Marco Civil da Internet, Lei nº 12.965 que está em vigor desde 23 de junho de 2014 e que determina em seu artigo 13º a guarda do registro das conexões pelo prazo mínimo de 12 (Doze) meses.

6.8. A adoção desta solução completa e robusta, contemplando equipamento de segurança de perímetro (Firewall), atende ao requisito legal de segurança, pois os órgãos e seus gestores podem responder por eventual ataques que tenham partido de sua rede, ou ainda pelo uso desta mesma rede para acessos a conteúdos ilegais, como por exemplo sites de pedofilia, apologia ao terrorismo e crimes contra o sistema financeiro, pois os registros e bloqueio destas requisições estarão sendo

monitoradas e seus usuários identificados através dos logs que deverão estar armazenados pelo período legal exigido pelo Marco Civil. Desta forma, o Governo do Estado do Acre inicia o processo de adequação aos quesitos legais, na proteção de dados sensíveis, no que toca diversos quesitos incluindo o de rastreabilidade, impostos pela Lei No 13709/18, Lei Geral de Proteção de Dados (LGPD).

6.9. Assim, a contratação visa atender as necessidades de telecomunicações do Governo do Estado do Acre, com uma solução tecnológica de acesso via satélite de alto desempenho, que possa atender a demanda atual com qualidade e que propicie ainda flexibilidade para futuras expansões, padronização, convergência e de serviços, segurança, eficiência e otimização dos recursos disponibilizados.

7.MODALIDADE DA LICITAÇÃO E PROPOSTA:

7.1. A modalidade adotada será do tipo **Pregão Eletrônico para Registro de Preços** do tipo **menor preço por lote;**

8.DO QUADRO QUANTITATIVO E PRECIFICAÇÃO.

Lote 1 – Unidades V-SAT banda Ka com Segurança da Informação

LOTE	ITEM	UNIDADE	DESCRIÇÃO				
1				QTDE TOTAL ARP **A**	**VALOR UNITÁRIO** **B**		**VALOR TOTAL** **C = (AXB)**
	1	UND	Instalação e configuração completa de Estação VSAT fixa e Solução de Segurança da Informação	300			
	VALOR TOTAL (A) = VALOR TOTAL DO ITEM 1						
				QTDE TOTAL ARP **A**	VALOR UNITARIO (MENSAL) **B**	VALOR UNITÁRIO (12 MESES) **C = (B X 12 meses)**	VALOR TOTAL GLOBAL (12 MESES) **D = (C X A)**

2	MÊS	Link de comunicação por Satélite, com IP, com operação em Banda Ka e velocidade de 20Mbps, por 12 meses, com franquia mínima inicial de 350 Gbytes/mês.	100			
3	MÊS	Link de comunicação por Satélite, com IP, com operação em Banda Ka e velocidade de 20Mbps, por 12 meses, com franquia mínima inicial de 150 Gbytes/mês.	100			
4	MÊS	Link de comunicação por Satélite, com IP, com operação em Banda Ka e velocidade de 10Mbps, por 12 meses, com franquia mínima inicial de 50 Gbytes/mês.	100			
5	MÊS	Locação com garantia de Estação VSAT fixa, Solução de Segurança e Sistema de geração de energia solar fotovoltaica (contendo manutenção de campo, operação e suporte da rede VSAT fixa, Solução de Segurança e Sistema de geração de energia solar fotovoltaica), por 12 meses.	300			
6	MÊS	Pacote adicional de franquia de dados de 50 GB	100			
7	MÊS	Pacote adicional de franquia de dados de 25 GB	100			
8	MÊS	Pacote adicional de franquia de dados de 10 GB	100			
VALOR TOTAL (B) = VALOR TOTAL GLOBAL (12 MESES) ITEM 3 + VALOR TOTAL GLOBAL (12 MESES) ITEM 4 + VALOR TOTAL GLOBAL (12 MESES) ITEM 5 + VALOR TOTAL GLOBAL (12 MESES) ITEM 6 + VALOR TOTAL GLOBAL (12 MESES) ITEM 7 + VALOR TOTAL GLOBAL (12 MESES) ITEM 8						
			QTDE TOTAL ARP **A**	**VALOR UNITÁRIO** **B**	**VALOR TOTAL** **C = (AXB)**	
9	UND	Remanejamento Interno de Infraestrutura VSAT (dentro do mesmo imóvel)	10			

	10	UND	Remanejamento Externo de Infraestrutura VSAT (outro imóvel ou munícipio)	10		
	VALOR TOTAL (C) = VALOR TOTAL ITEM 9 + VALOR TOTAL ITEM 10					
VALOR GLOBAL DO LOTE 1:					**VALOR TOTAL (A) + VALOR TOTAL (B) + VALOR TOTAL (C) = R$**	

Lote 2 – Unidades V-SAT banda Ka com Segurança da Informação e Energia Solar

LOTE	ITEM	UNIDADE	DESCRIÇÃO				
				QTDE TOTAL ARP **A**	**VALOR UNITÁRIO** **B**		**VALOR TOTAL** **C = (AXB)**
	1	UND	Instalação e configuração completa de Estação VSAT fixa, Solução de Segurança e Sistema de geração de energia solar fotovoltaica	50			
	VALOR TOTAL (A) = VALOR TOTAL DO ITEM 1						
				QTDE TOTAL ARP **A**	VALOR UNITARIO (MENSAL) **B**	VALOR UNITÁRIO (12 MESES) **C = (B X 12 meses)**	VALOR TOTAL GLOBAL (12 MESES) **D = (C X A)**
2	2	MÊS	Link de comunicação por Satélite, com IP, com operação em Banda Ka e velocidade de 10Mbps, por 12 meses, com franquia mínima inicial de 50 Gbytes/mês.	50			
	3	MÊS	Locação com garantia de Estação VSAT fixa, Solução de Segurança e Sistema de geração de energia solar fotovoltaica (contendo manutenção de campo, operação e suporte da rede VSAT fixa, Solução de Segurança e Sistema de geração de energia solar fotovoltaica), por 12 meses.	50			
	4	MÊS	Pacote adicional de franquia de dados de 25 Gbytes	50			

	5	MÊS	Pacote adicional de franquia de dados de 10 Gbytes	50			
	VALOR TOTAL (B) = VALOR TOTAL GLOBAL (12 MESES) ITEM 2 + VALOR TOTAL GLOBAL (12 MESES) ITEM 3 + VALOR TOTAL GLOBAL (12 MESES) ITEM 4 + VALOR TOTAL GLOBAL (12 MESES) ITEM 5						
				QTDE TOTAL ARP **A**	**VALOR UNITÁRIO** **B**		**VALOR TOTAL** **C = (AXB)**
	6	UND	Remanejamento Interno de Infraestrutura VSAT (dentro do mesmo imóvel)	5			
	7	UND	Remanejamento Externo de Infraestrutura VSAT (outro imóvel ou munícipio)	5			
	VALOR TOTAL (C) = VALOR TOTAL ITEM 5 + VALOR TOTAL ITEM 6						
VALOR GLOBAL DO LOTE 2:						**VALOR TOTAL (A) + VALOR TOTAL (B) + VALOR TOTAL (C) = R$**	

8.1. Todos os equipamentos/acessórios necessários à execução dos serviços exigidos no objeto deste termo de referência devem ser fornecidos em regime de Locação com garantia e em conformidade com as especificações técnicas mínimas, descritas neste Termo de Referência.

8.2. Deverão estar inclusas na proposta comercial todas as despesas para a consecução do objeto, como, serviços de instalação e configuração, taxa de apontamento, insumos, transportes, tributos, fornecimentos de equipamentos, manutenção e funcionamento dos enlaces de dados, gerenciamento, suporte técnico, ferramental; bem como todos os custos que vierem incorrer o fornecedor pela prestação dos serviços.

8.3. A Ata de Registro de Preços a ser gerada terá validade de 12 (doze) meses a partir da data de sua homologação.

9. DA COBERTURA SATELITAL

9.1. O satélite a ser utilizado para prestação do serviço deve apresentar cobertura em todo o território continental brasileiro, com autorização de operação emitida pela ANATEL.

10. DA ESPECIFICAÇÃO TÉCNICA DOS LINKS DE SATÉLITE

10.1. Especificação Técnica

10.1.1. A solução contratada deverá prover conexão de dados bidirecional e segura, via satélite, em banda Ka, para atender tráfego IP, que deve ficar ativa 24 horas por dia, 7 dias por semana, garantindo conectividade ininterrupta às estações VSAT, ou seja, não há procedimento de desconexão.

10.1.2. Caberá à CONTRATATA fornecer o segmento espacial, elaborar dimensionamento das instalações para cada caso, fornecer os equipamentos e materiais, providenciar documentação pertinente ao transporte dos equipamentos e material, efetuar a instalação e manutenção dos equipamentos/acessórios necessários ao perfeito funcionamento das estações VSAT.

10.1.3. Todo conjunto de equipamentos e materiais utilizados na instalação da estação VSAT, fornecidos pela CONTRATADA, deverão ser de qualidade e propriedades físicas que melhor se adaptem às condições a que estarão sujeitos, não podendo ser usados, reciclados, recondicionados ou de fabricação artesanal, devendo seguir rigorosamente as práticas de engenharia e Normas Técnicas pertinentes e em vigor no Brasil.

10.1.4. Para o pleno atendimento, exclusivamente, dos Itens 1 e 2 do lote 2, deverá ser fornecido sistema de energia solar capaz de manter os equipamentos de comunicação e segurança em funcionamento por no mínimo 24 (vinte e quatro) horas ininterruptas, no caso de não haver incidência solar por motivos de chuva e/ou mau tempo. O sistema fornecido deverá ser composto por no mínimo:

a) 03 Painéis Solares VMP 37,0V VOC 45,5V MAX 1500V
b) 02 Baterias estacionárias
c) 01 Controlador de carga 40A 12V/24V PMW
d) Cabos, conectores e demais acessórios e equipamentos necessários, inclusive postes, quando for o caso, para a correta instalação e perfeito funcionamento e acomodação de todo o sistema de alimentação

10.1.5. É responsabilidade da Licitante proceder com toda a instalação e ativação, nos locais indicados pela Contratante, bem como o correto dimensionamento do sistema, o qual deverá obedecer as características mínimas acima descritas, de forma a garantir o funcionamento, por até 24 (vinte e quatro) horas ininterruptas, de todo o sistema de comunicação e segurança fornecido.

10.1.6. Deverá ser fornecido, em conjunto com a estação remota, um equipamentos do tipo UTM e um modem satelital (IDU), visando interligação à rede local da unidade, que operem em 110V e 220V, cuja interface de integração com a rede local deverá ser no padrão Fast Ethernet (IEEE 802.3u) ou superior (dentro do padrão Ethernet). O referido modem satelital (IDU) deve ser homologado pela ANATEL, passível de consulta em sistema próprio, SGCH - Sistema de Gestão de Certificação e Homologação (Site ANATEL).

10.1.7. O endereçamento IP da porta LAN da IDU deve ser estabelecido em conjunto com a equipe técnica do CONTRATANTE.

10.1.8. A solução de comunicação de dados via satélite deverá atender as seguintes características técnicas mínimas:

10.1.9. A(s) HUB(s) do sistema deverá(ão) ser ou estar instalada(s) no solo brasileiro;

10.1.10. Operação em banda Ka;

10.1.11. Disponibilidade mensal: deve ser igual ou superior 97,5% para todas as estações;

10.1.12. A velocidade contratada dos links satélite serão de, no mínimo:

10.1.13. 20Mbps (vinte mega bits por segundo), para o item 2, no sentido de downstream (no sentido de tráfego da Rede Internet para a rede da unidade) com garantia de no mínimo 5Mbps (cinco mega bits por segundo); e upstream (sentido de tráfego da Rede da unidade para a rede Internet) de no mínimo de 3Mbps (três mega bits por segundo), com garantia de 768Kbps (setecentos e sessenta e oito kilo bits por segundo), sendo uma rede estatística deverá ser considerada a simultaneidade de 50% de toda a rede, ou seja, a rede deverá fornecer 50% de banda garantida.

10.1.14. 10Mbps (dez mega bits por segundo), para o item 3, no sentido de downstream (no sentido de tráfego da Rede Internet para a rede da unidade) com garantia de no mínimo 2.5Mbps (dois mega e quinhentos kilo bits por segundo); e upstream (sentido de tráfego da Rede da unidade para a rede Internet) de no mínimo de 2Mbps (2 mega bits por segundo), com garantia

de 512Kbps (quinhentos e doze kilo bits por segundo), sendo uma rede estatística deverá ser considerada a simultaneidade de 50% de toda a rede, ou seja, a rede deverá fornecer 50% de banda garantida.

10.1.15. Deverá ser disponibilizada franquias mínimas iniciais de:

10.1.16. 350 Gbytes para os links com velocidades de 20Mbps, que compõem o item 2 do lote 1, deste Edital;

10.1.17. 150Gbytes para os links com velocidades de 20Mbps, que compõem o item 3 do lote 1, deste Edital; e

10.1.18. 50Gbytes para os links com 10Mbps que compõem o item 4 do lote 1 e o item 2 do lote 2, deste Edital.

10.1.19. Será admitida redução da velocidade para 256Kbps, no caso de atingimento da franquia estipulada, para downloads, tanto para os links de 20Mbps quanto para os de 10Mbps.

10.1.20. Será facultado ao gestor do contrato, por meio da Central de Atendimento da Contratada, adquirir pacotes extras de franquia, correspondentes aos ITENS 6, 7 e 8 do lote 1 – “Pacote adicional de dados de 50 GBytes, 25 GBytes e 10 GBytes respectivamente” e ITENS 4 e 5 do lote 2 – “pacote adicional de dados de 25 GBytes e 10 Gbytes, respectivamente”, possibilitando a normalização do serviço por meio de pacote adicional, além da franquia mensal.

10.1.21. Após a solicitação de aquisição de pacotes extras de franquias, a contratada deverá habilitar a franquia adicional no prazo máximo de 4 (quatro) horas úteis, a contar da abertura do chamado técnico ou envio de ordem de serviço;

10.1.22. Será considerada hora útil toda hora ou fração compreendida entre 08:00hs e 18:00hs do horário local do Estado do Acre, de segunda a sexta feira.

10.1.23. A pedido da contratante, a contratada deverá programar envio de mensagens por e-mail com a finalidade informar quando o consumo de cada link estiver próximo ao limite contratado;

10.1.24. Os circuitos instalados deverão adotar tecnologia com mecanismos de modulação FEC adaptativa, para correção de taxas de erros de transmissão e controle de potência no link de retorno de maneira automatizada, compensando dinamicamente os desvanecimentos por chuva e outras condições meteorológicas adversas.

10.1.25. A CONTRATADA deverá garantir o sigilo e a inviolabilidade dos dados trafegados em sua rede.

10.1.26. Deverá ser apresentado, em fase de proposta, todos os Datasheets dos equipamentos e dispositivos que estão sendo propostos de forma a possibilitar a averiguação do atendimento integral das especificações técnicas ora exigidas.

11. DA SEGURANÇA E DO TRANSPORTE VPN DA ESTAÇÃO VSAT AO ÓRGÃO

11.1. A Solução de Conectividade Segura Satelital descrita no Lote 1 deverá ser composta por equipamentos do tipo UTM, cujas funcionalidades de segurança deverão estar disponíveis para todas as localidades remotas, conforme características técnicas mínimas descritas neste Termo de Referência. Os Links Satelitais descritos no Lote 1 (Itens 2 e 3) deverão ser concentrados no Teleporto da Contratada (HUB) e encaminhados via Backhaul VPN (Virtual

Private Network) Internet, que deverá ser estabelecida desde cada unidade à rede da SEE-AC.

11.2. Os equipamentos do tipo UTM (ponta A e B) deverão estar localizados na sede da SEE-AC e nas unidades, conforme DIAGRAMA I.

11.3. Os equipamentos concentradores UTM, deverão ser fornecidos pela CONTRATADA, incluindo serviço de instalação e configuração.

11.4. A Solução de Segurança UTM e conexão VPN devem ter minimamente as características técnicas descritas nos itens a seguir. Deverão ser apresentados, em fase de proposta, todos os Datasheets dos equipamentos que estão sendo propostos de forma a possibilitar a averiguação do atendimento integral das especificações técnicas ora exigidas.

11.5. **CARACTERÍSTICAS DO HARDWARE**

a) O equipamento deve se instalar em mesa ocupando, no máximo, 1U (44,45mm) da referida mesa;
b) Dispor de fonte de alimentação com tensão de entrada de 110V / 220V AC automática e frequência de 50-60 Hz;
c) Deverão ser fornecidos todos os cabos de energia, serial (RS-232/RJ45), para instalação e funcionamento do dispositivo;
d) Possuir led indicador on/off, disco e devices de rede;
e) Possuir throughput mínimo de 500 Mbps para tráfego UDP;
f) Possuir throughput mínimo de 50.000 (cinquenta mil) conexões simultâneas;
g) Suportar no mínimo 10.000 (dez mil) novas conexões por segundo;
h) Possuir throughput mínimo de 100 Mbps para tráfego HTTP/ HTTPS via Proxy;
i) Possuir throughput mínimo de 38 Mbps para tráfego HTTP/ HTTPS com inspeção SSL via Proxy;

j) Possuir throughput mínimo de 100 Mbps para tráfego IPS;
k) Possuir throughput mínimo de 140 Mbps para tráfego VPN IPSEC com criptografia (AES-128);
l) Possuir throughput mínimo de 96 Mbps para tráfego VPN SSL com criptografia (AES-128);
m) Possuir no mínimo 4 (quatro) interfaces de rede Gigabit Ethernet 10/100/1000 com leds indicativos de link e atividade, as portas entregues deverão ser roteáveis, ou seja, não será aceito equipamento com porta do tipo switch;
n) Possuir dispositivo de armazenamento interno de no mínimo 32 GB padrão SSD;
o) Possuir no mínimo 1 (uma) porta console de conexão padrão RJ45 para acesso a interface de comando CLI específica para esta finalidade, utilizando cabo do tipo serial RS-232/RJ-45;
p) Possuir pelo menos 2 (duas) portas USB para conexão de dispositivos externos;

11.6. ESPECIFICAÇÕES GERAIS DO SOFTWARE UTM - FUNÇÕES BÁSICAS

a) Hardware (Appliances) que atuam na segurança e performance do ambiente de rede;
b) VPN SSL, VPN IPSec (Client-to-site e Site-to-site);
c) Controle de Aplicações;
d) Proxy Web e Filtro de Conteúdo Web (URL Filtering);
e) Detecção e prevenção de intrusos – IPS;
f) Qualidade de serviço – QOS;
g) Anti-Malware;
h) SD-WAN;
i) Cluster.
j) A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;
k) Interface em português e inglês;

l) Possuir um único painel para criação e edição de política de segurança com possibilidade de habilitar NAT;

m) O sistema deve permitir o acesso à interface de gerenciamento WEB por qualquer interface de rede configurada;

n) O software deverá ser fornecido em sua versão mais atualizada, não sendo permitido qualquer tipo de comprovação futura.

o) Todo o ambiente deverá ser gerenciado sem a necessidade de produtos de terceiros para compor a solução.

p) Tanto os Gateways de Segurança bem como a Gerência Centralizada deverão suportar monitoramento através de SNMP v1, v2 e v3.

q) A Solução deverá prover inspeção SSL:

r) A solução deverá ser em hardware dedicado tipo appliance com sistema operacional customizado para garantir segurança e melhor desempenho.

s) Deve ser totalmente gerenciável remotamente, através de rede local, sem a necessidade de instalação de mouse, teclado e monitor de vídeo;

t) Deve suportar cluster do tipo Failover (HA) com replicação da tabela de estado.

11.7. **DAS FUNCIONALIDADES DO FIREWALL:**

a) Possuir capacidade de processamento de pacotes e interfaces de acordo com a tabela de performance dos equipamentos;

b) Permitir a conexão simultânea de vários administradores, com poderes de alteração de configurações e/ou apenas de visualização das mesmas;

c) Possuir um sistema de armazenamento remoto para salvar backups da solução com suporte a conexões do tipo Network File System, SSH e PenDrive;

d) Possibilitar a visualização dos países de origem e destino nos logs de eventos, de acessos e ameaças.

e) Possuir mecanismo que permita a realização de cópias de segurança (backups) do sistema e restauração remota, através da interface gráfica, a solução deve permitir o agendamento diário ou semanal;

f) O sistema deve permitir configurar o período ou número de cópias que deseja manter no repositório remoto e executar a manutenção de período automaticamente.

g) As cópias de segurança devem ser salvas compactadas e criptografadas de forma a garantir segurança, confiabilidade e confidencialidade dos arquivos de backup;

h) O sistema ainda deve contemplar um recurso de cópia de segurança do tipo snapshot, que contemple a cópia completa das configurações dos serviços e recursos do sistema;

i) Deve possibilitar a restauração do snapshot através da interface web de qualquer ponto remoto, de modo a contribuir para uma restauração imediata sem a necessidade de reinicialização do sistema;

j) Deve permitir habilitar ou desabilitar o registro de log por política de firewall.

k) Possuir controle de acesso à internet por endereço IP de origem e destino;

l) Possuir controle de acesso à internet por sub-rede;

m) Possuir suporte a tags de VLAN (802.1q);

n) Suportar agregação de links, segundo padrão IEEE 802.3ad;

o) Possuir ferramenta de diagnóstico do tipo tcpdump;

p) Possuir integração com Servidores de Autenticação RADIUS, TACACS+, LDAP e Microsoft Active Directory;

q) Possuir métodos de autenticação de usuários para qualquer aplicação que se execute sob os protocolos TCP (HTTP, HTTPS, FTP e Telnet);

r) Possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation), um para um, N-para-um e vários para um.

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

t) Permitir controle de acesso à internet por domínio, exemplo: gov.br, org.br, edu.br;

u) Possuir a funcionalidade de fazer tradução de endereços dinâmicos, muitos para um, PAT.

v) Possuir suporte a roteamento dinâmico RIP V1, V2, OSPF, BGP;

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

x) Deverá suportar aplicações multimídia como: H.323, SIP;

y) Possuir tecnologia de firewall do tipo Stateful;

z) Possuir alta disponibilidade (HA), trabalhando no esquema de redundância do tipo ativo-passivo;

aa) Permitir o funcionamento em modo transparente tipo “bridge”;

bb) Permitir a criação de pelo menos 20 VLANS no padrão IEEE 802.1q;

cc) Possuir conexão entre estação de gerência e appliance criptografada tanto em interface gráfica quanto em CLI (linha de comando);

dd) Deverá suportar forwarding de multicast;

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

ff) Permitir o agrupamento de serviços;

gg) Permitir o filtro de pacotes sem a utilização de NAT;

hh) Permitir a abertura de novas portas por fluxo de dados para serviços que requerem portas dinâmicas;

ii) Possuir mecanismo de anti-spoofing;

jj) Permitir criação de regras definidas pelo usuário;

kk) Permitir o serviço de autenticação para HTTP e FTP;

ll) Possuir a funcionalidade de balanceamento e contingência de links;

mm) Deverá ter técnicas de detecção de programas de compartilhamento de arquivos (peer-to-peer) e de mensagens instantâneas, suportando ao menos: Yahoo! Messenger, MSN Messenger, ICQ, AOL Messenger, BitTorrent, eDonkey, GNUTella, KaZaa, Skype e WinNY.

11.8. **IDENTIFICAÇÃO DE USUÁRIO**

a) Deve possuir a capacidade de criação de políticas de acesso de Firewall, VPN, IPS e Controle de aplicação integradas ao repositório de usuários sendo: Active Directory, LDAP, TACAC´S e Radius;

b) Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

c) Para usuários não registrados ou não reconhecidos no domínio, a solução deve ser capaz de fornecer uma autenticação baseada em navegador (Captive Portal), sem a necessidade de agente;

d) Deve possuir Captive Portal com suporte a Autenticação Social (Facebook, Twitter, Google);

e) A solução deverá ser capaz de identificar nome do usuário, login, máquina/computador registrados no Microsoft Active Directory;

f) Na integração com o AD, todos os domain controllers em operação na rede do cliente devem ser cadastrados de maneira simples e sem utilização de scritps de comando;

g) A solução de identificação de usuário deverá se integrar com as funcionalidades Firewall, controle de aplicação e IPS, sendo elas do mesmo fabricante;

h) A solução deve suportar a opção de instalação de softwares agentes nos PCs/Laptops para que os próprios PCs/Laptops enviem suas credenciais de IP/nome de usuário do domínio/nome da máquina para o gateway diretamente, sem que o Gateway tenha que fazer Queries no AD;

11.9. **DAS FUNCIONALIDADES DA VPN:**

a) VPN baseada em appliance;
b) Possuir algoritmos de criptografia para túneis VPN: AES, DES, 3DES;
c) Suporte a certificados PKI X.509 para construção de VPNs;
d) Possuir suporte a VPNs IPSec site-to-site:
e) Criptografia, 3DES, AES128, AES256, AES-GCM-128
f) Integridade MD5, SHA-1, SHA-256, SHA384 e AES-XCBC;
g) Algoritmo Internet Key Exchange (IKE) versões I e II;
h) AES 128 e 256 (Advanced Encryption Standard);
i) Suporte a Diffie-Hellman Grupo 1, Grupo 2, Grupo 5, Grupo 14; Grupo 15, Grupo 16, Grupo 17, Grupo 18, Grupo 19, Grupo 20, Grupo 21, Grupo 22, Grupo 23, Grupo 24, Grupo 25, Grupo 26, Grupo 27, Grupo 28, Grupo 29, Grupo 30;
j) Possuir suporte a VPN SSL;
k) Possuir capacidade de realizar SSL VPNs utilizando certificados digitais;
l) A VPN SSL deve possibilitar o acesso a toda infra-estrutura da contratante de acordo com a política de segurança, através de um plug-in ActiveX e/ou Java;
m) Deve permitir a arquitetura de vpn hub and spoke;
n) Suporte a VPNs IPSec client-to-site;
o) Deverá possuir cliente próprio para Windows para o estabelecimento da VPN client-to-site.
p) Suporte à inclusão em autoridades certificadoras (enrollment) mediante SCEP (Simple Certificate Enrollment Protocol);
q) Possuir funcionalidades de Auto-Dicovery VPN capaz de permitir criar tuneis de VPN dinâmicos entre múltiplos dispositivos (spokes) com um gateway centralizador (hub).;
r) A funcionalidade de AD-VPN deve suportar criar os seguintes tipos de tuneis:
    - Site-to-Site;

- Full-Mesh;
- Star.

11.10. **DAS FUNCIONALIDADES DA DETECÇÃO DE INTRUSÃO:**

a) A Detecção de Intrusão deverá ser baseada em appliance:
b) Possuir, no mínimo, 21.000 assinaturas de IPS/IDS;
c) O Sistema de detecção e proteção de intrusão deverá estar orientado à proteção de redes;
d) Possuir tecnologia de detecção baseada em assinatura;
e) O sistema de detecção e proteção de intrusão deverá possuir integração à plataforma de segurança;
f) Possuir capacidade de remontagem de pacotes para identificação de ataques;
g) Deverá possuir capacidade de agrupar assinaturas para um determinado tipo de ataque; Exemplo: agrupar todas as assinaturas relacionadas a web-server para que seja usado para proteção específica de Servidores Web;
h) Deverá possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep;
i) Mecanismos de detecção/proteção de ataques;
j) Reconhecimento de padrões;
k) Análise de protocolos;
l) Detecção de anomalias;
m) Detecção de ataques de RPC (Remote procedure call);
n) Proteção contra ataques de Windows ou NetBios;
o) Proteção contra ataques de SMTP (Simple Message Transfer Protocol) IMAP (Internet Message Access Protocol, Sendmail ou POP (Post Office Protocol);
p) Proteção contra ataques DNS (Domain Name System);
q) Proteção contra ataques a FTP, SSH, Telnet e rlogin;

r) Proteção contra ataques de ICMP (Internet Control Message Protocol);
s) Alarmes na console de administração;
t) Alertas via correio eletrônico;
u) Monitoração do comportamento do appliance através de SNMP, o dispositivo deverá ser capaz de enviar traps de SNMP quando ocorrer um evento relevante para a correta operação da rede;
v) Capacidade de resposta/logs ativa a ataques;
w) Terminação de sessões via TCP resets;
x) Atualizar automaticamente as assinaturas para o sistema de detecção de intrusos;
y) O Sistema de detecção de Intrusos deverá atenuar os efeitos dos ataques de negação de serviços;
z) Possuir filtros de ataques por anomalias;
aa) Permitir filtros de anomalias de tráfego estatístico de: flooding, scan, source e destination session limit;
bb) Permitir filtros de anomalias de protocolos;
cc) Suportar reconhecimento de ataques de DoS, reconnaissance, exploits e evasion;
dd) Suportar verificação de ataque nas camadas de aplicação;

11.11. **DAS FUNCIONALIDADES DE QOS**

a) Adotar solução de Qualidade de Serviço baseada em appliance;
b) 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;
c) Permitir modificação de valores DSCP para o DiffServ;
d) Limitar individualmente a banda utilizada por programas de compartilhamento de arquivos do tipo peer-to-peer;

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

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

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

h) Deverá controlar (limitar ou expandir) individualmente a banda utilizada por sub-rede de origem e destino;

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

11.12. **DAS FUNCIONALIDADES DO ANTIVÍRUS**

a) Possuir funções de Antivírus, Anti-spyware;

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

c) Permitir o bloqueio de malwares (adware, spyware, hijackers, keyloggers, etc.)

d) Permitir o bloqueio de download de arquivos por extensão e tipo de arquivo;

e) Permitir o bloqueio de download de arquivos por tamanho.

11.13. **DAS FUNCIONALIDADES DO PROXY E FILTRO DE CONTEÚDO WEB**

a) Possuir solução de filtro de conteúdo web integrado a solução de segurança

b) Possuir pelo menos 75 categorias para classificação de sites web

c) Possuir base mínima contendo, 40 milhões de sites internet web já registrados e classificados;

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

- Webmail;
- Instituições de Saúde;
- Notícias;
- Pornografia;
- Restaurante;
- Mídias Sociais;
- Esporte;
- Educação;
- Games;
- Compras;

e) Permitir a monitoração do tráfego internet sem bloqueio de acesso aos usuários;

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

g) Prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;

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

i) 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;

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

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

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

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

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

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

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

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

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

s) Deverá permitir a criação de listas personalizadas de URLs permitidas – lista branca e bloqueadas – lista negra;

t) Deverá funcionar em modo Proxy Explícito para HTTP, HTTPS, e FTP e em Proxy Transparente;

u) Deverá permitir configurar a porta do Proxy Explícito.

11.14. DAS FUNCIONALIDADES DO CONTROLE DE APLICAÇÕES

a) As funcionalidades abaixo devem ser baseadas em appliance:

b) Deverá reconhecer no mínimo 700 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;
- Web;
- Transferência de arquivos;
- Chat;

- Social;

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

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

g) Deverá prover funcionalidade de identificação transparente de usuários cadastrados no Microsoft Active Directory;

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

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

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

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

l) Deverá garantir que as atualizações regulares do produto sejam realizadas sem interromper a execução dos serviços de controle de aplicações.

11.15. **SD-WAN:**

a) Possuir funcionalidades de SD-WAN, não se limitando aos recursos solicitados abaixo;

b) Possuir o balanceamento automático para conexões externas à internet através das interfaces físicas;

c) O balanceamento deverá ser baseado em critérios de desempenho, devendo no mínimo, permitir verificar o monitoramento do consumo de banda, perda de pacotes, jitter e latência;

d) Deve possuir uma janela web ou dashboard capaz de fornecer informações dos eventos relacionado ao recurso SD-WAN;

e) Deverá oferecer um monitor capaz de prover em tempo real as seguintes informações:

- Consumo de banda;
- Perda de pacotes;
- Jitter;
- Latência.

11.16. **DOS SERVIÇOS ASSOCIADOS AO UTM**

a) A Contratada deverá prover todo o serviço de controle de conteúdo e volume de dados trafegado de acordo com as políticas a serem definidas pelo Departamento de Tecnologias Educacionais e da Informação - DETEI. O volume de dados trafegado em cada uma das unidades e em sua totalidade na rede deverá ser contabilizado em MBytes, para cada uma das soluções, Itens II e III.

b) A Contratada deverá prover todo o serviço de Monitoramento Remoto, a partir de suas instalações e utilizando-se de seus equipamentos e softwares, cujas características mínimas estão listadas anteriormente, com pessoal dedicado, para todos os sistemas instalados nas unidades remotas em regime 24X7. Quando da verificação de ataques, invasões e vírus, esta deverá dar início imediato aos trabalhos/atividades com vistas a sanear os mesmos. A Contratada se obriga ainda a:

- informar a equipe técnica do Departamento de Tecnologias Educacionais e da Informação - DETEI, em até 2 (duas) horas da verificação de quaisquer ocorrências
- informar a equipe técnica do Departamento de Tecnologias Educacionais e da Informação - DETEI, em 2 (duas) horas após a conclusão dos trabalhos/atividades para sanear as ocorrências
- fornecer, mensalmente, relatórios contendo todas as ocorrências e providências tomadas para solução das mesmas. Tais relatórios devem conter detalhes de data,

hora da invasão e/ou ataque, detalhes dos mesmos (ex: vírus, Dos, etc).

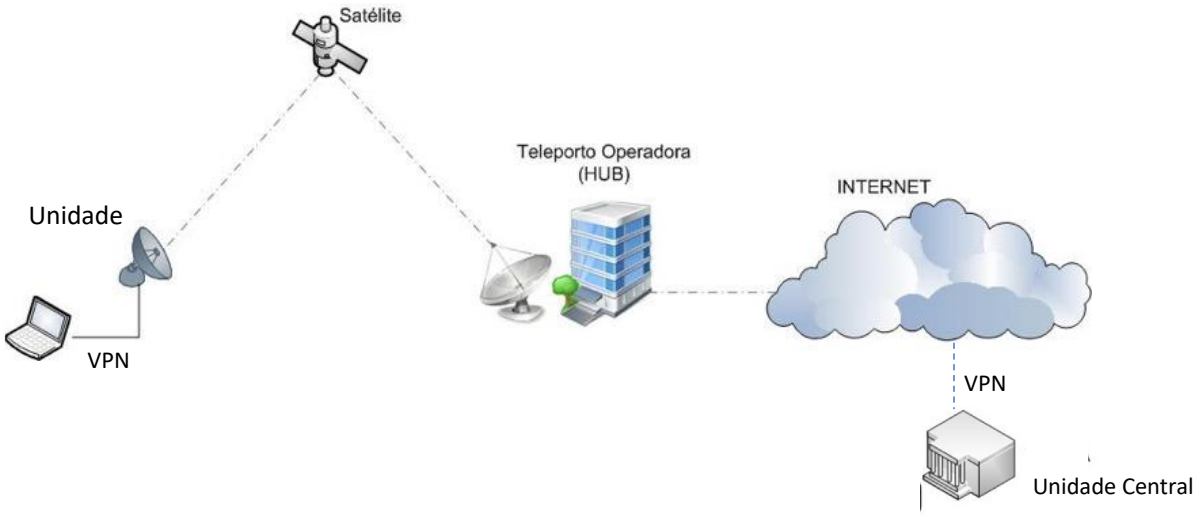

Diagrama I

A ilustração acima define o formato da Rede WAN nos acessos as Unidades remotas. As capacidades e a topologia de saída da VPN do ponto concentrador do provedor da solução devem ser projetadas tal que não existam pontos de gargalo entre as Unidades e o Ponto Concentrador. O acesso à internet que suportará a VPN a partir da unidade central será provido diretamente pela **Secretaria de Estado de Educação, Cultura e Esportes – SEE.**

12. TESTE DE HOMOLAGAÇÂO

12.1. A licitante, provisoriamente colocada em primeiro lugar poderá, a critério da equipe técnica, ser convocada pelo Pregoeiro para participar de teste de homologação da solução proposta. Caso seja convocada a mesma terá prazo de 5 (cinco) dias úteis para entregar amostra contemplando uma estação VSAT completa, um equipamento do tipo UTM da marca e modelo proposta de forma a permitir a avaliação por parte da equipe técnica ao atendimento

integral de todas as especificações técnicas exigidas neste termo de referência.

13. PRAZO DE ENTREGA

13.1. A rede e todos os seus elementos deverão ser entregues e estar apta para entrar em ambiente de produção em um prazo de até 60 (sessenta) dias úteis. A contagem do prazo iniciará a partir do primeiro dia útil após a assinatura do contrato.

14. TREINAMENTO

14.1. A empresa vencedora, quando contratada, deverá fornecer treinamento, de no mínimo 08 (oito) horas, para turma de até 8 (oitos) participantes, de toda a solução fornecida o que engloba o sistema VSAT e os componentes de segurança do tipo UTM. O Treinamento deverá englobar:

- as atividades de abertura instalação, ativação e comissionamento das estações VSAT;
- as atividades de abertura instalação, ativação e comissionamento da solução de segurança UTM;
- troubleshooting inicial e básico de forma a poder identificar possíveis problemas e suas eventuais causas;
- da abertura de chamados, acompanhamento dos mesmos e acesso aos dados disponíveis de gerência dos serviços ofertados.

14.2. A empresa vencedora, deverá fornecer material impresso contemplando o conteúdo a ser empregado no Treinamento.

15. DA DOTAÇÃO ORÇAMENTÁRIA

15.1. Os recursos para cobrir as despesas decorrentes da aquisição, objeto deste Termo, correrão à conta da Unidade Orçamentária: 817.006/4041.0002, Programa: Garantir a Funcionalidade das Unidades Escolares e Administrativas da SEE, Elemento de

despesa: 44.90.52.00, Fontes de Recurso: 100 (RP) E 300 (FUNDEB)

16. DOS LOCAIS DE INSTALAÇÃO

16.1. Os serviços serão instalados de acordo com tabela de endereços em anexo, das escolas da rede pública estadual, presentes nos 22 municípios do Estado do Acre.

17. DAS CONDIÇÕES DE PAGAMENTO

17.1. A contratante efetuará o pagamento mediante depósito em conta bancária, até 30 (trinta) dias após apresentação da respectiva Nota Fiscal, devidamente aceita e atestada pelo servidor designado para atesto dos serviços, bem como demais exigências fixadas no edital convocatório.

18. OBRIGAÇÕES DA LICITANTE

18.1. Prestar o serviço, objeto desta contratação, 24 horas por dia 7(sete) dias por semana, durante todo período de vigência do contrato, salvaguardados os casos de interrupções programadas e devidamente autorizadas pela ANATEL, casos fortuitos ou de força maior.

18.2. Responsabilizar-se pelo cumprimento dos postulados legais vigentes, de âmbito federal, estadual ou municipal, como também assegurar os direitos e o cumprimento de todas as obrigações estabelecidas pela regulamentação da ANATEL, inclusive quanto aos preços praticados.

18.3. Indicar preposto que a represente na gestão comercial do contrato, como negociação de aditivos contratuais, apresentação de propostas de reajustes de tarifas, renovação de contratos e outros. Caberá a este representante fazer o encaminhamento das demandas contratuais recebidas para as respectivas áreas / setores internos e providências da Contratada.

18.4. Zelar pela perfeita execução dos serviços e registrar às solicitações de imediato, corrigindo qualquer ocorrência de interrupção ou

deficiência na prestação dos serviços contratados nos prazos estabelecidos em regulamentos da ANATEL.

18.5. Prestar os serviços dentro dos parâmetros e rotinas estabelecidos, em observância às normas legais e regulamentares aplicáveis e, inclusive, às recomendações aceitas pela boa técnica.

18.6. Implantar, adequadamente, a supervisão permanente dos serviços, de forma a se obter uma operação correta e eficaz.

18.7. Aceitar, nas mesmas condições contratuais, os acréscimos ou supressões de quantitativos / valores na prestação dos serviços objeto da presente licitação, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

18.8. Atender aos acréscimos e supressões solicitados no prazo máximo de 10 (dez) dias úteis, contados da data de solicitação, prazo que deverá ser contado para a manifestação inicial da Contratada e depois para assinatura dos aditivos, após o acerto entre as partes.

18.9. Responsabilizar-se por todos os tributos, contribuições fiscais e parafiscais que incidam ou venham a incidir, direta e indiretamente, sobre os serviços prestados.

18.10. Manter, durante a execução do contrato, as mesmas condições da habilitação.

18.11. Não transferir a outrem, no todo ou em parte, a execução do contrato, salvo com expressa autorização da Contratante.

18.12. Relatar à Fiscalização do contrato toda e qualquer irregularidade observada quanto à execução dos serviços objeto da contratação.

18.13. Responder administrativa, civil e penalmente por quaisquer danos materiais ou pessoais ocasionados à Contratante e/ou a terceiros, por seus empregados, dolosa ou culposamente.

18.14. Atender em prazo máximo de 03 (três) dias úteis as solicitações de esclarecimento ou outras demandas de ordem contratual efetuadas por parte da Fiscalização do contrato.

18.15. Comunicar à Contratante, por escrito, qualquer anormalidade nos serviços e prestar os esclarecimentos julgados necessários.

18.16. Emitir documento de cobrança contemplando única e exclusivamente os serviços efetivamente prestados pela Contratada, ficando esclarecido que são vedadas: 1) a apresentação, no documento de cobrança da Contratada, de serviços de outras prestadoras, exceto quando imprescindíveis para a prestação do serviço e 2) a apresentação de serviços prestados pela Contratada em documento de cobrança ou em nome de outra prestadora.

18.17. Recalcular e reemitir faturas com novo prazo de pagamento, em no máximo 60 (sessenta) dias corridos, quando constatados erros de tarifas ou cobranças, sem incidências de quaisquer encargos adicionais, nem bloqueios ou cortes dos serviços, sendo de responsabilidade exclusiva da Contratada o recálculo das faturas e a prestação das informações necessárias ao pleno entendimento dos valores que estiverem sendo apresentados para pagamento.

18.18. A Fiscalização do contrato será exercida no interesse da SEE e não exclui nem reduz a responsabilidade da Contratada, inclusive perante terceiros, por quaisquer irregularidades, e, na sua ocorrência, não implica corresponsabilidade do Poder Público ou de seus agentes e prepostos.

18.19. Ressarcir à Contratante as interrupções imotivadas ou aquelas que não tiverem sido informadas e que vierem a impedir o tráfego de entrada e saída de dados.

18.20. O valor de ressarcimento deverá ser calculado de forma proporcional ao período de interrupção, considerando-se uma disponibilidade mensal (30 dias), de 24 horas ininterruptas.

18.21. Zelar pelo sigilo dos dados cadastrais da Contratante só divulgando-os para terceiros com expressa anuência da SEE.

18.22. Garantir sigilo e inviolabilidade das transmissões de dados decorrentes da contratação, considerando os recursos disponibilizados pela contratada, respeitadas as hipóteses e

condições constitucionais (Art. 5º, inciso XII) e legais de quebra de sigilo de telecomunicações (Lei nº 9.296, de 1996).

19. DA VIGÊNCIA CONTRATUAL

19.1. O contrato terá vigência imediata, após a sua assinatura, pelo período de 12 (doze) meses, podendo ser prorrogado por períodos iguais e sucessivos, mediante termos aditivos, até o limite total de 60 (sessenta) meses, “ex vi” do disposto no inciso II do artigo 57 da Lei n° 8.666/93 e alterações.

19.2. A prorrogação da vigência contratual deverá ser sempre precedida de pesquisa de mercado para verificar se as condições oferecidas pela contratada continuam vantajosas para a Contratante.

20. OBRIGAÇÕES DA CONTRATANTE

20.1. Exercer a fiscalização dos serviços por servidores especialmente designados e documentar as ocorrências havidas.

20.2. Certificar-se de que os valores cobrados pela Contratada sejam iguais aos ofertados em sua proposta comercial.

20.3. Fiscalizar o cumprimento das obrigações assumidas pela Contratada, inclusive quanto à continuidade e qualidade na prestação dos serviços, os quais, ressalvados os casos de força maior, não devem ser interrompidos.

20.4. Emitir pareceres em todos os atos relativos à execução do contrato, em especial, aplicações de sanções e alterações do contrato.

20.5. Permitir o acesso dos empregados da Contratada, quando necessário, para execução dos serviços.

20.6. Prestar aos funcionários da Contratada as informações e os esclarecimentos que eventualmente venham a ser solicitados.

20.7. Proporcionar à Contratada as facilidades necessárias a fim de que possa desempenhar normalmente os serviços contratados.

20.8. Efetuar os pagamentos devidos nas suas respectivas datas de vencimento, salvo quando constatada alguma irregularidade nas faturas enviadas pela Contratada.

20.9. A Contratante se reserva o direito de rejeitar o serviço prestado, se em desacordo.

21. DAS DISPOSIÇÕES FINAIS

21.1. A contratada deverá indicar pessoa responsável pelo acompanhamento da instalação dos SERVIÇOS, com poderes para dirimir eventuais dúvidas, solucionar questões não previstas no contrato e apresentar soluções práticas para qualquer problema envolvendo os referidos SERVIÇOS.

Rio Branco, Acre, 15 de junho de 2020.

Javã Sousa Costa
Chefe do Departamento de Tecnologia e Informação
Matricula nº 914410-2
Decreto nº 440/2019