ANEXO V

DESCRITIVO TÉCNICO

1. DO OBJETO

Constitui objeto do presente certame a contratação de empresa especializada na prestação de serviços de acesso à internet através de links dedicados, full duplex, com abordagem via fibra óptica até sede do CORE-SP e suas Seccionais, de acordo com o edital e seus anexos.

2. JUSTIFICATIVA

Atualmente, a sede do CORE-SP mantém um link que é utilizado para acessos à Internet e divulgação de seus serviços a todas Seccionais pertencentes a este órgão. Na arquitetura atual, o link é responsável por sustentar toda utilização da Internet dentro do órgão e disponibilização do sistema as Seccionais.

O contrato atual não contempla o serviço de link dedicado e MPLS e esse fato cria a necessidade, mais do que prioritária, de que se realize novo processo licitatório para manutenção deste serviço e a adição do MPLS. Caso não contratados, todo o acesso à Internet será interrompido e todas Seccionais que hoje faz parte do sistema mantido pelo CORE-SP ficará indisponível.

Esse cenário contempla o fato de que a Internet exerce papel preponderante para que o CORE-SP consiga satisfazer, com efetividade, sua missão institucional fornecendo diversos serviços, dentre eles: Informações, E-mail aos colaboradores, Serviços On Line, Acesso ao sistema Gerenti a todas as Seccionais, Acesso ao sistema Contábil ”Implanta”, futura interligação com as centrais de telefonias em outras.

3. ESPECIFICAÇÕES TÉCNICAS

3.1. O objetivo destes serviços é a interligação dos Escritórios Regionais e a sede do CORE-SP. A mesma se dará por link de comunicação de dados/voz/vídeo do tipo MPLS (*Multiprotocol Label Switching*). Na sede do CORE-SP e em cada Escritório Regional haverá um módulo concentrador que proverá a integração final entre os pontos, através de canais seguros de comunicação conhecidos por VPN (*Virtual Private Networks*). Conforme Anexo VI - Diagrama do projeto da MPLS para o CORE-SP.

3.2. A demanda deverá ser atendida tecnicamente, sendo observados os seguintes quesitos básicos:

3.3. A interligação da sede do CORE-SP com os escritórios deverá ser implementada através de links dedicados e obrigatoriamente implementados sob tecnologia MPLS (*Multiprotocol Label Switching*), não se admitindo quaisquer outras tecnologias de acesso por contenda;

3.4. A CONTRATADA deverá fornecer uma rede de comunicação de dados com tecnologia MPLS, com fornecimento de roteador, modems e demais equipamentos necessários, interligando a Sede do CORE-SP e os Escritórios Regionais à Internet, **conforme tabela abaixo.**

Grupo	Item	Local	Endereço	Cidade/UF	CEP	Produto	Velocidade (acesso Full)
1	1	Sede- São Paulo	Av. Brigadeiro Luís Antônio, 613, 5º andar	São Paulo - SP	01317-000	IP Internet	100Mbps
	2	Sede- São Paulo	Av. Brigadeiro Luís Antônio, 613, 5º andar	São Paulo - SP	01317-000	Anti-DDoS	100Mbps
2	3	Sede- São Paulo	Av. Brigadeiro Luís Antônio, 613, 5º andar	São Paulo - SP	01317-000	IP Internet	100Mbps
	4	Sede- São Paulo	Av. Brigadeiro Luís Antônio, 613, 5º andar	São Paulo - SP	01317-000	Anti-DDoS	100Mbps
	5	Sede- São Paulo	Av. Brigadeiro Luís Antônio, 613, 5º andar	São Paulo - SP	01317-000	VPN MPLS	50Mbps
	6	Sede- São Paulo	Av. Brigadeiro Luís Antônio, 613, 5º andar	São Paulo - SP	01317-000	VPN MPLS (secundário)	50Mbps
	7	Es01 - Campinas	Rua Alecrins, 914, 3°andar, sala 303,304,305 e 306 - Cambui	Campinas - SP	13024-411	VPN MPLS	10Mbps
	8	Es02 - Bauru	Rua Luso Brasileira, 4-44, 4º Andar Salas 411/412 – Jardim Estoril IV	Bauru - SP	17016-230	VPN MPLS	10Mbps
	9	Es03 - Ribeirão Preto	Av. Maurílio Biagi, 800 , 3º andar, conj. 311/312/313/314 - Santa Cruz do José Jacques	Ribeirão Preto - SP	14020-750	VPN MPLS	10Mbps
	10	Es04 -São José Dos Campos	Rua Euclides Miragaia, 700, 7° andar, salas 71/72/74 - Centro	São José Dos Campos - SP	12245-820	VPN MPLS	10Mbps
	11	Es05 - São José Do Rio Preto	R. General Glicério, 3173 4° andar, sala 41; Centro	São José Do Rio Preto - SP	15015-400	VPN MPLS	10Mbps
	12	Es06 - Presidente Prudente	R. Siqueira Campos, 699, 7º Andar, Sala 77 - Centro	Presidente Prudente - SP	19010-061	VPN MPLS	10Mbps
	13	Es07 - Araraquara	R. Padre Duarte, 151, 16° andar, Sala 161/162 – Jardim Nova América	Araraquara - SP	14800-360	VPN MPLS	10Mbps
	14	Es08 - Sorocaba	Rua José Maria Barbosa, 31 sala 51, 52, 53, 54 e 55 - Edifício Torre Sul Empresarial - Jardim Portal da Colina	Sorocaba - SP	18047-380	VPN MPLS	10Mbps
	15	Es09 – Santos	Rua Amador Bueno, 333 – Sala 1301 e 1303 – 13º andar – Bolco B – Paquetá	Santos – SP	11013-153	VPN MPLS	10Mbps
	16	Es10 - Araçatuba	R. Osvaldo Cruz, 1, 2° andar, cj. 21/22 – Centro	Araçatuba - SP	16010-040	VPN MPLS	10Mbps
	17	Es11 - Rio Claro	R. 06, 1460, 4° andar, Sala 41 – Centro	Rio Claro - SP	13500-190	VPN MPLS	10Mbps
	18	Es12 - Marília	Rua Bahia, 165, 10° andar, Sala 102 – Centro	Marília - SP	17500-080	VPN MPLS	10Mbps
	19	Alameda Santos - São Paulo	Alameda Santos, 1787, Conjunto 61	São Paulo - SP	01419-100	VPN MPLS	50Mbps
	20	Campinas	Rua Ferreira Penteado,709 -1º andar - Salas 11 a 17 - Centro	Campinas - SP	13010-906	VPN MPLS	10Mbps

3.5. <SUPRIMIDO>

3.6. Por tratar-se de link redundante, não poderá a mesma empresa ser declarada vencedora para o grupo 1 e o grupo 2, ambos os links deverão ser compatíveis com as especificações técnicas.

3.7. Na hipótese de uma mesma empresa oferecer a melhor proposta para os dois itens, deverá abdicar de um deles em detrimento do outro.

3.8. SLA (*Service Level Agreement*) de 99,4% de segunda a sexta-feira das 7h às 21h e aos sábados de 7 h às 19 h;

3.9. SLA (*Service Level Agreement*) de 99% para os demais horários e dias;

3.10. Tempo máximo de resposta dos pacotes TCP/IP (tempo de latência) entre um ponto de acesso remoto e os concentradores localizados em São Paulo será de 100 ms;

3.11. BER (*Bit Error Rate*) deverá ser de no máximo 10^{-7}.

3.12. A solução proposta não deverá promover o descarte de pacotes e a banda especificada acima deverá estar disponível em sua totalidade e a todo o momento;

3.13. A marcação de pacotes segundo suas características será feita por configuração dos roteadores e a cargo da CONTRATADA, mediante solicitação do CORE-SP. Os tráfegos previstos estão divididos em quatro categorias:

3.14. T1 - Fluxo de dados destinado à rede do CORE-SP, com reserva de banda;

3.15. T2 – Videoconferência. Em um primeiro momento não será implementada, mas poderá ser solicitada a reconfiguração dos equipamentos assim que se fizer necessário;

3.16. T3 - Voz sobre IP;

3.17. T4 – Fluxo de dados destinado à Internet com reserva de banda.

3.18. Os equipamentos instalados, em primeira instância, deverão atender às características descritas para os tráfegos T1, T3 e T4, podendo ser substituídos quando e se fizer necessário para o atendimento às características dos tráfegos T2.

3.19. Sobre os serviços de reconfiguração, mesmo sob solicitação do CORE-SP, não incidirá qualquer ônus;

4. REDE IP MULTIMÍDIA

4.1. A Rede IP Multimídia deverá fazer QoS, fim a fim (CPE a CPE, incluindo a priorização dentro do backbone da CONTRATADA), priorizando as aplicações conforme suas criticidades, que serão definidas pela CONTRATANTE após assinatura do contrato, em toda a rede MPLS da CONTRATANTE.

4.2. A Rede IP Multimídia consiste das unidades listadas, interligadas através de uma rede com arquitetura VPN IP/MPLS e topologia lógica em full-mesh.

4.3. A Rede de Acesso consiste na interligação das unidades prediais de forma dedicada e exclusiva com a porta do backbone MPLS da CONTRATADA através de uma “nuvem” de camada de 2 (dois) aos Pontos de Concentração da CONTRATANTE.

4.4. Caso solicitado pela CONTRATANTE, a CONTRATADA deverá restringir a comunicação lógica de determinadas unidades prediais a um conjunto de unidades previamente definidas (restrição de acesso lógico a partir de faixas de endereçamento IP, portas TCP e UDP).

4.5. A CONTRATADA deverá restringir a comunicação lógica de determinadas unidades prediais em até 07 (sete) dias consecutivos, a partir da formalização de

solicitação pela CONTRATANTE.

4.6. O limite de atuação da CONTRATADA será a interface LAN do roteador que será conectado ao switches/hubs da CONTRATANTE.

4.7. <SUPRIMIDO>

4.8. As especificações constantes deste descritivo técnico consideram que as soluções de telecomunicações a serem contratadas deverão ter alta qualidade, disponibilidade, desempenho, segurança e contingência no site central da CONTRATANTE ou onde ela indicar.

4.9. A CONTRATADA deverá providenciar a configuração lógica necessária para que as comunicações entre unidades prediais ocorram através da sua Rede de Acesso e backbone, em ambos os sentidos.

4.10. A CONTRATADA conforme disponibilidade e viabilidade técnica atenderá as futuras unidades prediais dentro das respectivas cidades, a critério da CONTRATANTE, nas mesmas condições técnicas e de preço oferecidas para o objeto deste descritivo técnico. Caso não seja possível, a CONTRATADA deverá emitir relatório/documento que ateste a indisponibilidade naquele local.

4.11. A CONTRATANTE poderá solicitar a desativação do serviço prestado a qualquer unidade predial, de acordo com a lei 8.666/93.

4.12. A Rede IP Multimídia deverá transportar dados, vídeo e voz sobre o protocolo IP conforme modelo de QoS a ser definido entre a CONTRATANTE e a CONTRATADA após assinatura do contrato.

4.13. A CONTRATADA deverá utilizar em sua solução roteadores, que possibilitem a geração de estatísticas de uso dos enlaces por endereços IP origem/destino, por protocolo de camada 4, por porta TCP/UDP origem/destino e por aplicação.

4.14. A coleta e/ou exportação dos dados estatísticos sobre tráfego deverão ser realizadas por meio de protocolos que permitam o envio de informações ao coletor de dados, o qual deverá realizar o armazenamento e processamentos destas. O coletor deverá permitir a visualização on-line destes dados, por meio de tabelas e de gráficos, inclusive via web.

4.15. <SUPRIMIDO>

4.16. <SUPRIMIDO>

4.17. A rede deverá suportar roteamento de tráfego IP multicast, em conformidade com os seguintes padrões:

a) RFC 2362, PIM-SM (Protocol Independent Multicast-Sparse Mode);

b) RFC 2236, Internet Group Management Protocol, Version 2;

c) RFC 2933, Internet Group Management Protocol MIB.

4.18. A CONTRATADA deverá prestar os serviços de comunicação de dados, por meio de VPN IP/MPLS conforme os seguintes padrões:

a) RFC 2547, BGP/MPLS VPNs

b) RFC 2447, Diff Serv Code Point

d) RFC 2917, A Core MPLS IP VPN Architecture;

e) draft-ietf-l3vpn-rfc2547bis, BGP/MPLS IP VPNs.

4.19. A topologia lógica da rede VPN IP/MPLS criada será do tipo full-mesh. A CONTRATANTE poderá, a seu critério, definir unidades prediais com conectividade lógica diferente de full-mesh (por exemplo, ponto-a-ponto ou partial-mesh).

4.20. Quando solicitada a CONTRATADA deverá implementar a conectividade lógica diferente de full-mesh em até 07 dias consecutivos a partir da formalização de solicitação pela CONTRATANTE.

4.21. Os circuitos físicos de rede da CONTRATADA deverão ser configurados com QoS e deverão utilizar os protocolos listados abaixo:

4.21.1. Velocidades de 256 Kbps até 2Mbps: MLPPP (Mult Link PPP)

4.21.2. Velocidades acima de 2Mbps:

- MLPPP (no caso de um bundle de seriais: n x 2Mbps)
- PPP (no caso da interface POS)
- ETHERNET (Fast ou Giga-Ethernet)

4.22. A CONTRATADA deve disponibilizar em todos os sites o protocolo de roteamento dinâmico BGP.

4.23. A rede de comunicação de dados deverá ter garantia de desempenho, segurança, e suporte a diversos protocolos e permitir a utilização de endereçamento IP privativo.

4.24. A rede da CONTRATADA deverá ter suporte ao uso de certificado digital privativo pela CONTRATANTE.

4.25. Requisitos de qualidade de Serviço (QoS)

4.25.1. A solução da CONTRATADA deverá suportar a arquitetura DiffServ, incluindo DiffServ sobre redes MPLS conforme os seguintes padrões:

a) RFC 2474, Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers;

b) RFC 2475, An Architecture for Differentiated Services;

c) RFC 2597, Assured Forwarding PHB Group;

d) RFC 2598, An Expedited Forwarding PHB;

e) RFC 3270, Multi-Protocol Label Switching (MPLS) Support of Differentiated Services.

4.25.2. De acordo com as prioridades e níveis de serviços requisitados, os diferentes tipos de tráfego que cursarão por meio da Rede IP

Multimídia deverão ser classificados nas classes de serviços (DiffServ), conforme descrito a seguir:

TIPO DE APLICAÇÃO	DESCRIÇÃO
a) Tempo Real Voz e Vídeo	Aplicações de voz e vídeo sensíveis a retardo (delay) e variações de retardo (jitter), que exigem priorização de tráfego e reserva de banda;
b) Missão Crítica	Aplicações interativas críticas para o negócio, que exigem entrega garantida, reserva de banda e tratamento prioritário;
c) Dados Alta Prioridade	Aplicações que necessitam de latência controlada – aplicações transacionais (ex: Base de Dados, SAP, PeopleSoft, Siebel, Financial, B2B, Supply Chain Management, Ariba, Microsoft SQL, DLSw+) e aplicações interativas (ex: Messenger, Net Meeting, Telnet, Citrix,PlaceWare);
d) Dados Média Prioridade	Aplicações que apresentam característica de rajada – Ex: Streaming de vídeo, E-mail (Lotus Notes, Outlook, SMTP, IMAP, etc), transferência de arquivos grandes (FTP), sincronização de base-de-dados, backups
e) Dados Baixa Prioridade	Aplicações não críticas com mensagens de tamanho muito variado e não imprescindíveis para o atendimento imediato.
f) Gerenciamento	Aplicações de gerenciamento de redes e de sistemas que necessitam de uma banda mínima para atividades de suporte técnico;
g) Classe Default	Reservado

Tabela 1

4.25.3. As políticas de QoS serão posteriormente definidas pelo CONTRATANTE em conjunto com a CONTRATADA para aplicação em cada site da rede, em até 5 dias úteis a contar das assinaturas do Contrato de Prestação do Serviço.

4.25.4. Em todos os circuitos de acesso devem ser habilitado o QoS, sendo obrigatório, no mínimo a definição de aplicações de baixa prioridade e de gerenciamento, as demais classes podem ser configuradas ou não de acordo com a necessidade e escolha da CONTRATADA.

4.25.5. A CONTRATANTE poderá solicitar a qualquer momento a modificação nas configurações de QoS (classificadores, marcadores, escalonadores, policiamento, shaping, dentre outros) dos roteadores

CPE, quando aplicável.

4.25.6. A CONTRATADA deverá modificar as configurações de QoS dos roteadores CPE e dos terminais remotos em até 7 dias consecutivos a partir da formalização de solicitação pela CONTRATANTE.

4.25.7. A CONTRATADA deve garantir que o tráfego Real-Time seja inferior ou igual a 30% da banda total da interface para não comprometer outras aplicações da rede da CONTRATANTE e garantia que a contratada tenha saída própria internacional.

4.25.8. A CONTRATADA deve garantir uma reserva máxima de banda de 97% para o tráfego das aplicações da CONTRATANTE em sua rede de acesso visando garantir a reserva de 3% para a classe default (supervisão da rede).

4.26. Padrões de endereçamento IP, roteamento e interconexão da Rede IP Multimídia e Rede de Acesso

4.26.1. A CONTRATANTE será responsável pelo mapa de endereçamento IP adotado na Rede IP Multimídia e na Rede de Acesso.

4.26.2. A CONTRATANTE poderá utilizar no interior de sua rede o plano de endereçamento IP que preferir. Entretanto, a CONTRATADA deverá projetar e implementar a solução de forma a permitir a utilização do plano de endereços fornecido pela CONTRATANTE nas redes locais das unidades prediais.

4.26.3. A especificação da arquitetura de roteamento será definida pela CONTRATANTE, com a aprovação da CONTRATADA.

4.26.4. A CONTRATADA deverá projetar e implementar uma solução de roteamento que atenda aos requisitos de conectividade, contingência, balanceamento automático de tráfego e interconexão, baseada em roteamento dinâmico.

4.26.5. A solução de roteamento deverá ser projetada e implementada de forma escalável permitindo o crescimento da rede.

4.26.6. A solução de redundância (contigência) será ATIVO-ATIVO.

4.27. REQUISITOS DE CONTINGÊNCIA

4.27.1. O site central Primário e o site Secundário (backup) deverão ser obrigatoriamente atendidos por fibra óptica em anel com redundância automática, sendo que os acessos do anel devem ser realizados por caminhos distintos até o ponto de presença (POP) da CONTRATADA.

4.27.2. Todos os elementos do CORE-SP da rede MPLs da nuvem até sede devem ser independentes entre si tanto no site Principal como no site Secundário com tráfego em caminho distinto.

4.27.3. A unidade principal e Secundária dos links de internet e MPLS da sede deverão utilizar roteadores CPE distintos e independentes com balanceamento automático de carga entre eles.

4.27.4. Os acessos da unidade Principal e Secundária deverão estar interligados diretamente aos roteadores de borda distintos da CONTRATADA, obedecendo aos requisitos abaixo:

a) Alta disponibilidade através de uma solução de contingência atendida por roteadores duplicados e interconectados um ao outro através de conexão Fast Ethernet, conectados a cada um dos enlaces, operando com protocolo de redundância e operando com balanceamento automático de tráfego (exemplo: GLBP – Gateway Load Balancing Protocol, BGP – Border Gateway Protocol);

b) A solução de redundância (contigência) será ATIVO-ATIVO.

c) Após a solução da falha causadora do contingenciamento, o tráfego deverá retornar automática e imediatamente para a situação anterior à falha;

4.27.5. Para o atendimento da unidade Principal e Secundária, os dois enlaces deverão ter capacidades idênticas na velocidade mínima de 1 x 50 Mbps/s para site Principal e 1 x 50 Mb para site Secundário, por enlace, e operar com balanceamento automático de tráfego, portanto se houver falha em um enlace ou CPE todo o tráfego será transportado através do enlace remanescente sem perda de qualidade.

5. ESPECIFICA ÇÕES TÉCNICAS

5.1. Os serviços de conectividade e internet para a CORE-SP, doravante denominada de REDE DE INFORMAÇÃO E COMUNICAÇÃO deverá interconectar todas as unidades e Sede denominados neste descritivo técnico como Pontos de Comunicação.

5.2. A REDE DE INFORMAÇÃO E COMUNICAÇÃO será composta de Pontos de comunicação com capacidade de transporte de 10 Mbps, cujas quantidades estão relacionadas a seguir:

Localidade	Endereço	Número	Complemento	Bairro	CEP	UF	Sigla	CNL	Velocidade Porta
Matriz internet principal	Av. Brigadeiro Luís Antônio	613	5º andar	Bela Vista	01317-000	SP	Sede 1	SPO	100 Mbps
Matriz Internet secundário							Sede 2	SPO	100 Mbps
Matriz MPLS ativo							Sede 3	SPO	50 Mbps
Matriz MPLS ativo							Sede 4	SPO	50 Mbps
Campinas	Rua Alecrins	914	3°andar, sala 303,304,305 e 306	Cambui	13024-411	SP	Es01	CAS	10 Mbps
Bauru	Rua Luso Brasileira	4-44	4º Andar Salas 411/412	Jardim Estoril IV	17016-230	SP	Es02	BRU	10 Mbps
Ribeirão Preto	Av. Maurílio Biagi	800	3º andar, conj. 311/312/313/314	Santa Cruz do José Jacques	14020-750	SP	Es03	RPO	10 Mbps
São José Dos Campos	Rua Euclides Miragaia	700	7° andar, salas 71/72/74	Centro	12245-820	SP	Es04	SJC	10 Mbps
São José Do Rio Preto	R. General Glicério	3173	4° andar, sala 41	Centro	15015-400	SP	Es05	SRR	10 Mbps
Presidente Prudente	R. Siqueira Campos	699	7º Andar, Sala 77		19010-061	SP	Es06	PPE	10 Mbps
Araraquara	R. Padre Duarte	151	16° andar, Sala 161/162	Jardim Nova América	14800-360	SP	Es07	ARQ	10 Mbps
Sorocaba	Rua José Maria Barbosa	31	sala 51, 52, 53, 54 e 55 - Edifício Torre Sul Empresarial	Jardim Portal da Colina	18047-380	SP	Es08	SOC	10 Mbps
Santos	Rua Amador Bueno	333	Sala 1301 e 1303 – 13º andar – Bolco B	Paquetá	11013-153	SP	Es09	STS	10 Mbps
Araçatuba	R. Osvaldo Cruz	1	2° andar, cj. 21/22		16010-040	SP	Es10	ARC	10 Mbps
Rio Claro	R. 06	1460	4° andar, Sala 41	Centro	13500-190	SP	Es11	RCL	10 Mbps
Marília	Rua Bahia	165	10° andar, Sala 102	Centro	17500-080	SP	Es12	MIA	10 Mbps
Alameda Santos - São Paulo	Alameda Santos	1787	Conjunto 61		01419-100	SP	Sede 5	SPO	50 Mbps
Campinas	Rua Ferreira Penteado	709	1º andar - Salas 11 a 17	Centro	13010-906	SP	Es01	CAS	10 Mbps

5.3.A REDE DE INFORMAÇÃO E COMUNICAÇÃO deverá ser provida com serviço de internet com capacidade total de 100 Mbps para utilização compartilhada de todos os Pontos de Comunicação que integrarão a rede.

Para a prestação dos serviços objeto deste descritivo técnico, a Contratada deverá interconectar todos os Pontos de Comunicação que irão integrar a REDE DE INFORMAÇÃO E COMUNICAÇÃO, por meio de fibra óptica. Não será permitido qualquer outro meio físico de comunicação que não seja a fibra óptica, inclusive para a prestação do serviço de internet.

5.4.O acesso à Internet será implantado conforme especificações descritas a seguir:

A critério da CONTRATADA, serão utilizados IP públicos providos pela CONTRATANTE ou serão utilizados endereços IP públicos e ASN (Autonomous System Number) registrados pelo CORE-SP.

5.4.1. As velocidades descritas na tabela anterior são taxas de transmissão para tráfego de entrada e tráfego de saída, simultaneamente, ou seja, a banda será simétrica (full duplex).

5.4.2. A CONTRATADA deverá disponibilizar, no mínimo, 8 (oito) endereços IP válidos para o enlace;

5.4.3. As interligações devem ser em conexão permanente, dedicadas e exclusivas, desde as dependências do CORE-SP até a conexão à infraestrutura de comunicação da CONTRATADA, obedecendo às recomendações elaboradas pela EIA/TIA (Electronic Industries Alliance / Telecomunications Industry Association), pela ABNT (Associação Brasileira de Normas Técnicas) e demais normas, quando couber;

5.4.4. A infraestrutura deverá possuir, necessariamente, no mínimo, 5 (cinco) POPs (Points of Presence) próprios no Brasil, incluindo um em São Paulo.

5.4.5. Somente serão aceitos como POPs válidos aqueles que possuam redundância nos enlaces de comunicação de dados com o “backbone” da CONTRATADA.

5.4.6. A velocidade mínima de saída do POP localizado em São Paulo para as demais localidades deverá totalizar a velocidade de 5 Gbps (cinco gigabits por segundo).

5.4.7. A infraestrutura deverá possuir enlaces de comunicação de dados com outras prestadoras de abrangência nacional, possibilitando a capitalização do acesso em todo o Brasil.

5.4.8. O backbone deverá possuir, pelos menos, 3 (três) pontos de troca de tráfego com provedores que possuam Sistemas Autônomos (AS - Autonomous Systems) independentes, sendo que cada um deverá ter, no mínimo,

velocidade de 1 Gbps (um gigabit por segundo). Um desses pontos de troca deverá ser com 1 (um) provedor internacional.

5.4.9. <SUPRIMIDO>

5.5. Os roteadores deverão atender as seguintes características:

5.5.1. ser capazes de suprir as necessidades técnicas de desempenho estabelecidas neste anexo;

5.5.2. suportar os protocolos SNMP v1, v2, v3 e RMON, além de suportar as tecnologias SFlow e NetFlow;

5.5.3. o Sistema Operacional dos equipamentos deverá ser o mais atual disponível no mercado, devendo ser atualizado sempre que houver necessidade ou que possam agregar melhorias ou correções aos serviços prestados;

5.5.4. memória primária mínima de 512 MB (quinhentos e doze), instalados;

5.5.5. memória “Flash” mínima de 256 MB (duzentos e cinquenta e seis megabytes), instalados;

5.5.6. possuir, no mínimo, 2 (duas) interface Ethernet de 1 Gbps,

5.5.7. possibilitar a utilização simultânea de todas as interfaces;

5.5.8. suporte a aplicações TCP/IP, em conformidade com as recomendações do IETF (Internet Engineering Task Force);

5.5.9. requisitos mínimos de “software” (sistema operacional e/ou aplicativos):

i.1) roteamento com emprego dos protocolos BGP-4, OSPF v2;

i.2) suporte a gerenciamento por SNMP (versões 1, 2 e 3) e RMON com no mínimo os grupos padrões: estatísticas, alarmes, histórico e eventos;

i.3) MIBs (Management Information Base): MIB-II, MIB estendida do equipamento e aquela que permite o gerenciamento dos recursos instalados e configurados no equipamento;

i.4) suportar a utilização de filtros de pacotes, construção de Listas de Acesso (Access List – ACL) e as funcionalidades básicas de segurança;

i.5) suportar criação de canal criptografado usando SSH v2, visando administração remota do roteador;

i.6) integrar multisserviços, como voz, dados e vídeo;

i.7) suportar a configuração de VLANs (Virtual Local Area Networks), em conformidade com o padrão IEEE 802.30;

i.8) suportar controle (definição) de banda por VLAN;

i.9) suportar IPv6;

i.10) suportar a função de gateway entre IPv4 e IPv6 e inverso;

i.11) suportar protocolo de redundância VRRP ou equivalente;

i.12) suportar a implementação de VPN (Redes Privadas Virtuais);

i.13) compatibilidade com os roteadores e switches atualmente utilizados pelo CORE-SP para acesso à Internet;

6. os equipamentos deverão ser retirados, quando cessar a prestação de serviços, no prazo máximo de 30 (trinta) dias após a comunicação formal do Órgão Responsável.

6.0. Requisitos para serviço de mitigação Anti-DDoS

Características Técnicas de mitigação Anti-DDoS:

6.1. O proponente deve possuir 2 centros de limpeza Nacional com capacidade de mitigação de 30 Gbps;

6.2. Para a mitigação dos ataques não será permitido o encaminhamento do tráfego para limpeza fora do território brasileiro;

6.3. O proponente deve ser o proprietário do link de conexão a internet diretamente ao cliente desde backbone;

6.4. <SUPRIMIDO>

6.5. Deverá operar sem tabela de sessão, do tipo “*stateless*”;

6.6. A proponente deve mitigar ataques por 3 horas, caso o ataque

ultrapasse o SLA de mitigação contratado;

6.7. O sistema de proteção em deverá estar implementado direto no backbone provedor do link de internet;

6.8. <SUPRIMIDO>

6.9. Caso o volume de tráfego do ataque ultrapasse as capacidades de mitigação especificadas ou sature as conexões do AS GESP devem ser tomadas contramedidas tais como aquelas que permitam o bloqueio seletivo por blocos de IP de origem no AS pelo qual o ataque esteja ocorrendo, utilizando técnicas como Remote Triggered Black Hole;

6.10. A solução de detecção e mitigação devem possuir serviço de atualização de assinaturas de ataques;

6.11. A proponente deve disponibilizar um Centro Operacional de Segurança (ou SOC – Security Operations Center) no Brasil, com equipe especializada 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 incluir certificações do SOC ISSO por exemplo;

6.12. A mitigação de ataques deve ser baseada em arquitetura na qual há o desvio de tráfego suspeito comandado pelo equipamento de monitoramento, por meio de alterações do plano de roteamento;

6.13. Em momentos de ataques DOS e DDOS, todo trafego limpo deve ser reinjetado na infraestrutura da contratante através de tunelamento seguro, configurado entre a plataforma de DOS e DDOS da contratada e o CPE do contratante;

6.14. <SUPRIMIDO>

6.15. As funcionalidades de monitoramento, detecção e mitigação de ataques devem ser mantidas em operação ininterrupta durante as 24 (vinte e quatro) horas do dia, nos 7 (sete) dias da semana, no período

de vigência contratual;

6.16. Em nenhum caso será aceito bloqueio de ataques de DOS e DDOS por ACLs em roteadores de bordas da contratada;

6.17. A contratada deve realizar a detecção de ataques em até de 15 (quinze) minutos;

6.18. <SUPRIMIDO>

6.19. <SUPRIMIDO>

6.20. <SUPRIMIDO>

6.21. <SUPRIMIDO>

6.22. <SUPRIMIDO>

6.23. <SUPRIMIDO>

6.24. <SUPRIMIDO>

6.25. <SUPRIMIDO>

6.26. <SUPRIMIDO>

7.0. Características de Contramedidas

7.1. Deve possuir as seguintes contra-medidas no sistema:

7.1.1. Invalid Packets – drops invalid IP/TCP/UDP/ICMP packets;

7.1.2. Dynamic Blacklist (setada por outras contra-medidas);

7.1.3. IP Address Filter Lists;

7.1.4. Black / White Lists;

7.1.5. Inline Filter;

7.1.6. Black / White Filter Lists;

7.1.7. Blacklist Fingerprints;

7.1.8. IP Location Filter Lists;

7.1.9. Zombie Detection (dinamicamente bloqueando hosts, não permanentemente);

7.1.10. Per Connection Flood Limiting;

7.1.11. TCP SYN Authentication (incluir autenticação HTTP, via 302, redirect, javascript);

7.1.12. DNS Authentication (atraves de requisição ao cliente via TCP);

7.1.13. TCP Connection Limiting;

7.1.14. TCP Connection Reset;

7.1.15. Payload Regular Expression Filtering;

7.1.16. Source /24 Baseline Enforcement;

7.1.17. Protocol Baseline Enforcement;

7.1.18. DNS Malformed;

7.1.19. SIP Malformed;

7.1.20. Shaping;

7.1.21. IP Location Policing.

7.1.22. Invalid packets (pacotes inválidos) deve checar por obrigatoriedade:

7.1.23. Malformed IP Header;

7.1.24. Incomplete Fragment;

7.1.25. Bad IP Checksum;

7.1.26. Duplicate Fragment;

7.1.27. Fragment Too Long;

7.1.28. Short Packet;

7.1.29. Short TCP Packet;

7.1.30. Short UDP Packet;

7.1.31. Short ICMP Packet;

7.1.32. Bad TCP / UDP Checksum;

7.1.33. Invalid TCP Flags;

7.1.34. Invalid ACK Number.

7.1.35. Mitigações obrigatórias em IPv6:

7.1.36. Invalid Packets;

7.1.37. IPv6 Address Filter Lists;

7.1.38. Black / White Lists;

7.1.39. Zombie Detection;

7.1.40. TCP SYN Authentication;

7.1.41. Payload Regular Expression;

7.1.42. O sistema deverá proteger contra as principais ferramentas e ataques abaixo:

7.1.43. Ping Attack, Smurf Attack, reflection attacks, UDP flood, Stream, dc++, blackenergy;

7.1.44. Teardrop, Targa3, Jolt2, Nestea;

7.1.45. Loic, Hoic, Ref Ref, Slow-Loris, R.U.D.Y;

7.1.46. O sistema deve possuir capacidade de bloquear tráfego através de expressões FCAP;

7.1.47. O sistema deve possuir capacidade de bloquear tráfego através de pay-load regex;

7.1.48. <SUPRIMIDO>

O sistema deverá possuir a capacidade de criar limites de tráfego, baseado em:

7.1.49. Zombie Detection;

7.1.50. NS Rate Limiting;

7.1.51. HTTP Rate Limiting;

7.1.52. SIP Request Limiting;

7.1.53. <SUPRIMIDO>;

7.1.54. <SUPRIMIDO>;

7.1.55. <SUPRIMIDO>;

7.1.56. <SUPRIMIDO>;

7.1.57. <SUPRIMIDO>;

7.1.58. <SUPRIMIDO>;

7.1.59. <SUPRIMIDO>;

7.1.60. <SUPRIMIDO>;

7.1.61. <SUPRIMIDO>;

7.1.62. <SUPRIMIDO>;

7.1.63. <SUPRIMIDO>;

8.0. <SUPRIMIDO>

9.0. Requisitos para serviço de monitoramento

9.1. Monitoramento permanente de Grupos de cibercrime;

9.2. Novas ferramentas maliciosas;

9.3. Novos vetores de ataque;

9.4. Novas vulnerabilidades críticas;

9.5. Notificação por correio eletrônico nos seguintes casos: o Operações

hacktivistas ativas que possam representar uma ameaça para o setor ao que pertence a organização.

9.6. Campanhas de ataques informáticos orquestrados pelo cibercrime;

9.7. Vulnerabilidades críticas que se façam conhecer em software de alta utilização;

9.8. Novas técnicas usadas pelos atacantes para burlar a segurança das organizações;

9.9. Modus operando utilizados para realizar fraude no setor da organização;

9.10. Notícias e sua análise, quando estes ofereçam inteligência acionável para a organização;

9.11. Envio de relatório consultivo com o detalhe das técnicas, táticas ou procedimentos que possam causar um impacto crítico na organização, bem como de vulnerabilidades de alta periculosidade onde se explica o impacto da mesma, a forma que é explorada, bem como se incluem recomendações para mitigar o efeito das mesmas;

9.12. Será entregue um boletim semanal com o detalhe das vulnerabilidades para os sistemas mais comuns nas organizações;

9.13. Inclui-se SCIBits, um relatório de inteligência genérico entregue de maneira mensal onde se detalha a análise realizada pela equipe de nosso centro de ciberinteligência (SCILabs) a respeito do sucedido no mês anterior e suas previsões para o seguinte;

9.14. Serão entregues relatórios trimestrais a respeito do comportamento das ameaças no setor, onde se dará detalhe das tendências identificadas no trimestre, as que estão por vir e recomendações de prevenção para a organização;

9.15. Realiza-se o monitoramento 24X7 de novas vulnerabilidades, incidentes ou ameaças que possam afetar o setor. Para isso o SCILabs se apoia em técnicas como OSINT e VHUMINT, onde através de perfis encobertos se extrai informação restringida a grupos fechados ou segredos, canais de IRC e fóruns especializados;

9.16. Realiza-se a busca de grupos de cibercrime com a finalidade de

identificar suas técnicas, táticas e procedimentos;

9.17. Os analistas do SCILabs estão à procura de novas ferramentas maliciosas para analisar e entregar Indicadores de compromisso e recomendações;

9.18. Realiza-se a busca e identificação de tendências de vetores de ataque que possam afetar à organização e/ou seu setor;

9.19. Identificam-se padrões a respeito das ameaças observadas em outras partes do mundo e analisa-se como estes podem afetar à organização no curto e médio prazo;

9.20. Enviam-se alertas através de correio eletrônico dependendo da criticidade dos mesmos. Estes poderão ser liberados inclusive à noite, fins de semana e feriados e de acordo com a matriz de escalonamento;

9.21. A cada alerta ou aviso se incluirão recomendações específicas;

9.22. Naqueles casos onde se realize análise da exploração da ameaça, os alertas poderão ser complementados posteriormente a sua notificação inicial em caso que os nossos analistas (Cyber Security Researchers) do centro de ciberinteligência do SCILabs encontrem informação relevante adicional;

9.23. Quando se identifique informação que não representa uma ameaça no curto prazo, mas que se considera de interesse para a organização se enviará um aviso de caráter informativo.

10.0. DA VISTORIA TÉCNICA:

10.1. Durante o prazo de elaboração de propostas, ficarão disponíveis os locais onde serão executados os serviços para realização de vistorias técnicas agendadas, para fins de conhecimento dos locais de instalação, da sala de entrada e das dependências onde serão executados os serviços, da natureza, da área e das condições de sua execução.

10.2. As vistorias técnicas serão agendadas junto ao Departamento de Tecnologia de Informação do CORE-SP, telefone (11) 3243-5511.

10.3. Não tendo realizado a vistoria de que trata este título, a licitante não poderá arguir desconhecimento do local, da área, ou da infraestrutura existente.

11.0. DA PRESTAÇÃO DOS SERVIÇOS:

11.1. Forma de Execução dos Serviços:

11.1.1. Caberá à CONTRATADA fornecer ao CORE-SP acesso à Internet — rede mundial de computadores — conforme condições estabelecidas neste Edital;

11.1.2. O modelo de prestação do suporte técnico será por solicitação, ou seja, a CONTRATADA receberá do CORE-SP solicitação para o fornecimento de suporte técnico conforme severidades especificadas;

11.1.3. Caberá a CONTRATADA apresentar soluções definitivas para os problemas apresentados dentro dos prazos e condições estabelecidas;

11.1.4. Nesse modelo não se caracteriza a subordinação direta e nem a pessoalidade, visto que:

a. não se requer a exclusividade, pois não há óbice ao compartilhamento de qualquer profissional com outros contratos que porventura a CONTRATADA possua;

b. não haverá controle de frequência ou de número de horas de presença nas dependências do CORE-SP

11.1.5. Não haverá qualquer relação de subordinação jurídica entre os profissionais da equipe da CONTRATADA do CORE-SP;

11.1.6. A prestação de serviço não é baseada em horas de serviço ou posto de trabalho;

11.1.7. Os serviços de acesso à Internet com circuito de comunicação de dados, roteadores e suporte técnico deverão estar em plena operação e disponíveis ao CORE-SP no prazo de, no máximo, 60 (sessenta)

dias, contados a partir da emissão da ordem de serviço.

12.0. DAS OBRIGAÇÕES DA CONTRATADA:

12.1. A CONTRATADA deverá:

12.1.1. Fornecer serviço de acesso à Internet, dedicado e exclusivo entre a Rede de Dados do **CORE-SP** e a rede mundial de computadores — Internet, conforme condições estabelecidas neste Edital e seus anexos;

12.1.2. Disponibilizar Central de Atendimento para a abertura e fechamento de chamados de suporte técnico, conforme períodos e condições estabelecidas no Edital e seus Anexos;

12.1.3. Prestar as informações e os esclarecimentos que venham a ser solicitados pelos técnicos da CONTRATANTE referente a qualquer problema detectado ou no andamento de atividades das manutenções previstas;

12.1.4. Arcar com todos os encargos sociais trabalhistas, tributos de qualquer espécie que venham a ser devidos em decorrência da execução do serviço contratado, bem como custos relativos ao deslocamento e estada de seus profissionais, caso exista;

12.1.5. Utilizar as melhores práticas, capacidade técnica, materiais, equipamentos, recursos humanos e supervisão técnica e administrativa, para garantir a qualidade do serviço e o atendimento às especificações contidas no Contrato, Edital e seus Anexos;

12.1.6. Responsabilizar-se integralmente pela sua equipe técnica, primando pela qualidade, desempenho, eficiência e produtividade, visando a execução dos trabalhos durante todo o Contrato, dentro dos prazos estipulados, sob pena de ser considerada infração passível de aplicação de penalidades previstas, caso os prazos e condições não sejam cumpridas;

12.1.7. Substituir, sempre que exigido pelo Fiscal do Contrato, qualquer um dos seus empregados, cuja qualificação, atuação, permanência eu comportamento forem julgados prejudiciais, inconvenientes ou insatisfatórios à disciplina do órgão ou ao interesse do serviço público,

decorrente da execução do serviço;

12.1.8. Prestar suporte a todas as funcionalidades presentes e necessárias para que o serviço seja efetivamente prestado;

12.1.9. Fornecer serviço com suporte a aplicações TCP/IP, obedecendo às recomendações do IETF (*Internet Engineering Task Force*);

12.1.10. Fornecer os endereços IP de seus POPS do CORE-SP para a aferição do serviço;

12.1.11. Prever e implementar em seus equipamentos toda a configuração relacionada ao protocolo de roteamento BGP, incluindo configuração de vizinhança e circuito;

12.1.12. Permitir visitas da equipe técnica da CONTRATANTE a suas dependências, para fins de auditoria das condições estabelecidas no Contrato, Edital e seus Anexos;

12.1.13. Instalar os materiais e equipamentos necessários à prestação do serviço, inclusive os roteadores especificados, assumindo todos os custos dessa instalação;

12.1.14. Fornecer dispositivos e roteadores, de sua propriedade, para provimento do serviço de acesso à Internet, em conformidade com as exigências técnicas constantes do item 3.4 deste anexo;

12.1.15. Os roteadores permanecerão dedicados ao serviço durante o transcorrer da prestação de serviço, podendo somente ser desativados ao término do Contrato ou por solicitação do CORE-SP;

12.1.16. Eventuais substituições dos roteadores estarão sujeitas a autorização do CORE-SP, após comprovada a conformidade do novo dispositivo com as especificações definidas no Edital e seus anexos;

12.1.17. Os roteadores deverão ser substituídos por outros de maior capacidade sempre que sua utilização descumprir o definido no nível de qualidade do serviço;

12.1.18. A administração dos roteadores será de responsabilidade da

CONTRATADA;

12.1.19. O CORE-SP poderá, em função de suas necessidades e a seu juízo, demandar a execução de ações coordenadas entre os provedores de acesso à Internet visando a adequada prestação do serviço e o seu aperfeiçoamento;

12.1.20. A critério da CONTRATANTE, o serviço de DNS (*Domain Name System*) primário será provido por equipamento de propriedade da CONTRATADA ou da CONTRATANTE;

12.1.21. O serviço de DNS secundário será provido de maneira segura (DNSSec - *Domain Name System Security Extensions*) por equipamentos próprios da CONTRATADA e instalados fora das dependências do CORE-SP

13.0. DO SUPORTE TÉCNICO E DOS NÍVEIS DE SERVIÇOS EXIGIDOS:

13.1. O serviço de suporte técnico será realizado por telefone (0800) e por sistema WEB e, ainda, *on-site* nas dependências do CORE-SP, sempre que a natureza do serviço exigir a presença de técnico especializado.

13.2. O serviço de suporte técnico será prestado de forma ininterrupta, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, inclusive em feriados, por profissionais especializados e deverá cobrir todo e qualquer defeito apresentado no serviço de acesso à Internet e no equipamento, peça e componente, incluindo esclarecimentos técnicos para ajustes, reparos, instalações, configurações e correções necessárias.

13.3. A CONTRATADA deverá prover manutenções preventivas, corretivas, evolutivas e, ainda, a substituição de peça e/ou componente para os equipamentos.

13.4. Entende-se por manutenção preventiva a série de procedimentos destinados a prevenir indisponibilidades e/ou falhas do serviço de comunicação e dos equipamentos.

13.5. A forma e o prazo para execução serão estabelecidos pela equipe técnica da CONTRATANTE quando da abertura do chamado de suporte técnico e será considerado como um chamado de severidade BAIXA.

13.6. Entende-se por manutenção corretiva a série de procedimentos destinados a recolocar o serviço de comunicação e/ou equipamentos em seu pleno estado de funcionamento, removendo definitivamente os defeitos apresentados.

13.7. Entende-se por manutenção evolutiva o fornecimento de novas versões e/ou releases corretivas e/ou evolutivas de softwares lançadas durante a vigência do Contrato, mesmo em caso de mudança de designação do nome do software.

14.0. Níveis de Serviço Exigidos (NSE)

14.1. A CONTRATADA responderá pela reparação dos danos causados por defeitos relativos ao serviço prestado. Por isso deverá prezar pela qualidade e eficiência, garantindo que o serviço e também as soluções definitivas fornecidas não causem problemas adicionais àqueles apresentados pelo CORE-SP quando da abertura dos chamados de suporte técnico.

14.2. Caberá à CONTRATADA apresentar novas soluções dentro dos prazos e condições estabelecidas no NSE, sem prejuízo de aplicação de penalidades previstas, caso sejam detectados erros ou impropriedades na solução apresentada.

14.3. Os Níveis de Serviço Exigidos (NSE) serão contados a partir da abertura dos chamados de suporte técnico e serão classificados conforme as severidades especificadas a seguir.

14.3.1. Severidade ALTA: esse nível de severidade é aplicado quando há a indisponibilidade do uso do serviço e/ou equipamentos.

Prazo de Solução Definitiva	
Dias Úteis	**Sábados, Domingos e Feriados**
4 (quatro) horas	6 (seis) horas

14.3.2. Severidade MÉDIA: esse nível de severidade é aplicado quando há falha, simultânea ou não, do uso do serviço e/ou equipamentos, estando ainda disponíveis, porém apresentando problemas.

Prazo de Solução Definitiva	
Dias Úteis	**Sábados, Domingos e Feriados**
8 (oito) horas	10 (dez) horas

14.3.3. Severidade BAIXA: esse nível de severidade é aplicado para a instalação, configuração, manutenções preventivas, esclarecimentos técnicos relativos ao uso e aprimoramento do serviço e/ou dos equipamentos. Não haverá abertura de chamados de suporte técnico com esta severidade em sábados, domingos e feriados.

Prazo de Solução Definitiva	
Dias Úteis	**Sábados, Domingos e Feriados**
10 (dez) dias	---

14.4. Faculta-se à CONTRATADA substituir temporariamente o equipamento, peça e componente defeituoso por outros de mesmas características técnicas ou superior, quando então, a partir de seu pleno estado de funcionamento, ficará suspensa a contagem do prazo de solução definitiva.

14.5. O prazo máximo para a substituição temporária descrita no item anterior será de 30 (trinta) dias, sendo que neste prazo o equipamento, peça e componente deverá ser devolvido ao CORE-SP em pleno estado de funcionamento ou ser substituído definitivamente.

14.6. A CONTRATADA deverá substituir, no prazo máximo de 30 (trinta) dias, qualquer equipamento, peça e componente que venha a se enquadrar em um dos seguintes casos:

a. ocorrência de 4 (quatro) ou mais chamados técnicos de manutenção corretiva dentro de um período contínuo qualquer de 30 (trinta) dias;

b. soma dos tempos de paralisação que ultrapasse as 20 (vinte) horas, dentro de um período contínuo qualquer de 30 (trinta) dias;

c. problemas recorrentes em um período contínuo de 90 (noventa) dias

contados a partir da abertura do primeiro chamado.

14.7. No caso de inviabilidade da solução definitiva do problema apresentado no equipamento, peça e componente, independentemente do enquadramento nos casos previstos no item anterior, faculta-se à CONTRATADA promover a sua substituição em caráter definitivo.

14.8. A substituição será admitida a critério do CORE-SP, após prévia avaliação técnica quanto às condições de uso e compatibilidade do equipamento, peça e componente ofertado, em relação àquele que está sendo substituído.

14.9. Os equipamentos, peças e/ou componentes substitutos deverão ser homologados pelo fabricante dos equipamentos.

14.10. A substituição de equipamento, peça e/ou componente deverá ocorrer sem custo adicional para o CORE-SP.

14.11. Caso seja necessário enviar equipamento, peça e componente para centro de assistência técnica fora das dependências do CORE-SP, a CONTRATADA deverá desinstalar, embalar, transportar e reinstalar, bem como deverá arcar com todos os custos necessários, sendo considerada fiel depositária do equipamento, peça e componente.

14.12. O envio para centros de assistência técnica em outra localidade não exime a CONTRATADA do cumprimento dos prazos estabelecidos nos níveis de serviço exigidos.

14.13. O CORE-SP reserva-se o direito de efetuar conexões dos equipamentos ou componentes a outros, bem como adicionar peças ou componentes, compatíveis tecnicamente com equipamentos, sem que isso constitua motivo para a CONTRATADA se desobrigar do serviço de suporte técnico, desde que tal fato não implique danos materiais ou técnicos aos equipamentos.

14.14. A equipe técnica da CONTRATANTE detém competência e terá total autonomia para executar ações de administração, gerenciamento e configuração dos equipamentos, podendo promover alterações e

reconfigurações sempre que julgar necessário, sem que isso constitua motivo para a CONTRATADA se desobrigar do serviço de suporte técnico.

14.15. O fornecimento do acesso à Internet deverá obedecer aos seguintes critérios:

a) Latência máxima: 50 ms (cinquenta milissegundos) até o roteador de borda (PE);

b) perda de pacotes máxima: 2% (dois por cento);

c) disponibilidade mínima: 99,44% (noventa e nove vírgula quarenta e quatro por cento);

d) a apuração e/ou contabilização das grandezas acima definidas, para efeito de aferição de resultados, dar-se-á mensalmente.

15.0. No que se refere aos roteadores:

a) taxa máxima de utilização de CPU e Memória: 70% (setenta por cento);

b) as taxas máximas referentes ao roteador só serão levadas em consideração quando se mantiverem constantes em valores maiores ou iguais aos especificados por um período mínimo de 5 (cinco) minutos ou ocorrerem repetidas vezes por períodos menores;

c) a operação do roteador com taxas superiores às especificadas na alínea “a” implicará sua substituição por outro de maior capacidade.

16.0. A Latência, definida como o tempo em que um pacote IP leva para ir de um ponto a outro da rede e retornar à origem, será aferida nos seguintes termos para os itens:

a) a cada 5 (cinco) minutos serão coletadas amostras de Latência dos Pontos de Presença (POP), sendo feito o cálculo da média aritmética das amostras coletadas;

b) ao final de cada mês, será verificado o número de observações cujo tempo de latência ultrapassou 50 ms (cinquenta milissegundos);

c) a quantidade de observações relativas à alínea “b” não poderá ser superior a 20% (vinte por cento) do total de amostras.

17.0 A perda de pacotes, definida como o índice que mede a taxa de sucesso na transmissão de pacotes IP entre dois pontos da rede, será aferida de forma análoga à utilizada para medição da Latência.

a) a cada 5 (cinco) minutos serão coletadas amostras da perda de pacotes dos Pontos de Presença (POP), sendo feito o cálculo da média aritmética das amostras coletadas;

b) ao final de cada mês será verificada a quantidade de pacotes perdidos dentro desse período de apuração;

c) a quantidade de pacotes perdidos não poderá ser superior à 2% (dois por cento) do total de pacotes.

18.0. O serviço de acesso à Internet deverá estar disponível 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, inclusive feriados.

18.1. Após a instalação inicial da rede, solicitações de instalação, retirada ou alteração do acesso à Internet dar-se-ão por solicitação formal da equipe técnica da CONTRATANTE, e deverão ser executadas em um prazo máximo de 5 (cinco) dias e contados a partir da solicitação.

18.2. A disponibilidade do serviço de acesso à Internet corresponde ao percentual de tempo, durante o período mensal de operação, em que o serviço esteve em condições normais de funcionamento. Tal percentual não poderá ser inferior a 99,44% (noventa e nove vírgula quarenta e quatro por cento).

18.3. A disponibilidade mensal, denominada Taxa Útil Operacional (TUO), é definida como o tempo em que o acesso à Internet estiver operacional para transmissão e recepção de pacotes IP e será medida pelo monitoramento das interfaces dos roteadores instalados nas dependências do CORE-SP, sendo seu cálculo, em termos percentuais, efetuado a partir da expressão aritmética apresentada a seguir, sendo considerada apenas a primeira casa decimal do resultado, sem arredondamento:

$$TUO(\%) = \frac{THC - TPP - \mathrm{TPI} - \mathrm{THP}}{\mathrm{THC} - \mathrm{TPP} - \mathrm{TPI}} * 100$$

Onde,

TUO (%) = Taxa Útil Operacional;

THC (h) = Total de Horas contratadas para prestação do serviço, por mês;

TPP (h) = Total de horas Paradas Programadas pela CONTRATADA e aprovadas pelo CORE-SP por mês;

TPI (h) = Total de Paradas Internas (sem responsabilidade da CONTRATADA);

THP (h) = Total de Horas Paradas por mês (ambiente de acesso total ou parcialmente indisponível).

18.4. A apuração da TUO para fins de aplicação de penalidades previstas somente será realizada a partir da data de entrada do serviço em operação.

18.5. A TUO será apurada mensalmente nos dias de calendário correspondentes aos das datas de entrada do serviço em operação.

18.6. As coletas destinadas às medições dos parâmetros de latência, perda de pacotes e disponibilidade serão efetuadas pela equipe técnica da CONTRATADA. Os resultados obtidos, consolidados em relatório mensal, deverão ser submetidos à equipe técnica da CONTRATANTE.

18.7. A CONTRATADA tornará disponíveis informações sobre desempenho e falhas (disponibilidade) do acesso à Internet de forma interativa (“on-line”), a partir do momento da entrada do serviço em operação.

18.8. As informações tornadas disponíveis na forma interativa serão amparadas por mecanismos de segurança que mantenham a confidencialidade, com acesso restrito aos usuários autorizados pelo CORE-SP

18.9. O acesso à Internet que a CONTRATADA possui com o “backbone” Internet internacional deverá ter um percentual médio de utilização de, no máximo, 80% (oitenta por cento).

O serviço contratado será considerado indisponível a partir do momento em que eventuais problemas forem registrados pelo CORE-SP e até seu retorno às condições plenas de funcionamento.

18.10. Quando da ocorrência de falhas que tornem o serviço indisponível por mais de 5 (cinco) minutos, a CONTRATADA deverá entregar ao CORE-SP, no prazo máximo de 3 (três) dias uteis, relatório técnico com a descrição detalhada da ocorrência, suas causas e as ações corretivas realizadas para tornar o serviço novamente disponível.

18.11. A CONTRATADA deverá manter registro dos eventos, que porventura tenham provocado interrupções no acesso à Internet dentro do período do faturamento (30 dias), de modo a justificar à CORE-SP não consideração de tempos de inoperância, causados por falta de energia elétrica nas dependências da CONTRATANTE, por ações ou solicitações do C ou ainda por manutenções programadas.

18.12. Será considerado, como prazo de solução definitiva, o tempo decorrido entre a abertura do chamado efetuada pela equipe técnica da CONTRATANTE à CONTRATADA e a efetiva recolocação do serviço em pleno estado de funcionamento.

18.13. A contagem do prazo de solução definitiva de cada chamado será a partir da abertura do chamado na Central de Atendimento disponibilizada pela CONTRATADA, até o momento da comunicação da solução definitiva do problema e aceite pela equipe técnica da CONTRATANTE.

18.14. Os chamados de severidade ALTA deverão ser atendidos on-site e não poderão ser interrompidos até o completo restabelecimento do serviço, mesmo que se estendam para períodos noturnos, sábados, domingos e feriados. Nesse caso, não poderão acarretar custos adicionais à CORE-SP

18.15. A interrupção do suporte técnico de um chamado desse tipo de severidade por parte da CONTRATADA e que não tenha sido previamente autorizado pela CONTRATANTE, poderá ensejar em aplicação de penalidades previstas.

18.16. Os chamados classificados com severidade MÉDIA, quando não solucionados no prazo definido, deverão ser automaticamente escalados para a severidade ALTA, sendo que o prazo de solução definitiva do problema, bem como penalidades previstas, serão automaticamente ajustados para o novo nível.

18.17. A interrupção do suporte técnico de um chamado desse tipo de severidade por parte da CONTRATADA e que não tenha sido previamente autorizado pela CONTRATANTE, poderá ensejar em aplicação de penalidades previstas.

18.17.1. Depois de concluído o suporte técnico, a CONTRATADA comunicará o fato à equipe técnica da CONTRATANTE e solicitará autorização para o fechamento do chamado. Caso a CONTRATANTE não confirme a solução definitiva do problema, o chamado permanecerá aberto até que seja efetivamente solucionado pela CONTRATADA. Nesse caso, a CONTRATANTE fornecerá as pendências relativas ao chamado aberto.

18.17.2. A CONTRATANTE encaminhará à CONTRATADA, quando da reunião de alinhamento de expectativas, relação nominal da equipe técnica autorizada a abrir e fechar chamados de suporte técnico.

18.18. Por necessidade excepcional de serviço, ao CORE-SP também poderá solicitar a escalação de chamado para níveis superiores de severidade. Nesse caso, a escalação deverá ser justificada e os prazos dos chamados passarão a contar do início novamente.

18.19. Sempre que houver quebra dos Níveis de Serviço Exigidos - NSE ao CORE-SP emitirá ofício de notificação à CONTRATADA, que terá prazo máximo de 5 (cinco) dias e contados a partir do recebimento do ofício para apresentar as justificativas para as falhas verificadas.

18.19.1. Caso não haja manifestação dentro desse prazo ou caso ao CORE-SP entenda serem improcedentes as justificativas apresentadas, será iniciado processo de aplicação de penalidades previstas, conforme e nível de serviço transgredido.

São Paulo, 01 de maio de 2021.

Edson Yassudi Miyashiro
Assessor de Suporte Técnico