Governo do Estado do Rio de Janeiro

Centro de Tecnologia da Informação e Comunicação do Estado do Rio de Janeiro

Vice Presidência de Tecnologia

# ANEXO IV

# ORDEM DE SERVIÇO

| MODELO DE ORDEM DE SERVIÇO - OS | | | |
|---|---|---|---|
| **ORGÃO:** | | **CNPJ:** | |
| **IDENTIFICAÇÃO DA ORDEM DE SERVICO** | | | |
| **Ordem de Serviço n°:** | | **Data de Emissão** | |
| **Classificação da OS:** | | **Requisitante do Serviço:** | |
| **Nome do Projeto:** | | **Sigla:** | |
| **Contratada:** | | **N° do Contrato:** | |

| ESPECIFICAÇÃO DO(S) SERVIÇO(S) | | | | | |
|---|---|---|---|---|---|
| **ID** | **Serviço** | **Qtde** | **Métrica Prevista** | **Valor Unitário** | **Valor Total do Item** |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| **Valor Total da Ordem de Serviço** | | | | | |

| INSTRUÇÕES COMPLEMENTARES |
|---|
| |

| CRONOGRAMA | | |
|---|---|---|
| **ID** | **Tarefa / Fase** | **Cronograma Previsto** |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

| DOCUMENTOS A ENTREGAS | | |
|---|---|---|
| **ID** | **Documento** | **Observações** |
| | | |
| | | |

| | | |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |

| DATAS E PRAZOS | | |
|---|---|---|
| **Data prevista para início dos serviços** | **Data prevista para entrega dos serviços** | **Prazo Total da Ordem de Serviço** |
| | | |

| APROVAÇÃO E CIÊNCIA | | |
|---|---|---|
| **CONTRATANTE** | **CONTRATADA** | **DATA RECEBIMENTO: / / .** |
| Assinatura do Gestor do Contrato<br>Nome<br>Cargo<br>Siape | Assinatura do Preposto da Contratada<br>Nome<br>Cargo<br>CPF | |
| **Observações:** | | |

Rio de Janeiro, 23 novembro de 2020

Documento assinado eletronicamente por **Daniel Luzente de Lima**, **Gerente**, em 05/01/2021, às 12:14, conforme horário oficial de Brasília, com fundamento nos art. 21º e 22º do Decreto nº 46.730, de 9 de agosto de 2019.

Documento assinado eletronicamente por **Elio Thomé de Souza Filho**, **Analista de Sistemas**, em 05/01/2021, às 12:17, conforme horário oficial de Brasília, com fundamento nos art. 21º e 22º do Decreto nº 46.730, de 9 de agosto de 2019.

A autenticidade deste documento pode ser conferida no site http://sei.fazenda.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **12098552** e o código CRC **BA579B6F**.

**Referência:** Processo nº E-04/171/221/2018 SEI nº 10650739

Rua da Conceição, 69, 24º Andar / 25º Andar - Bairro Centro, Rio de Janeiro/RJ, CEP 20051-011
Telefone:

Governo do Estado do Rio de Janeiro

Centro de Tecnologia da Informação e Comunicação do Estado do Rio de Janeiro

Vice Presidência de Tecnologia

# ANEXO V

## MODELO DE ATESTADO (OU DECLARAÇÃO) DE CAPACIDADE TÉCNICA

Atestamos (ou declaramos) que a empresa , inscrita no CNPJ (MF) nº , inscrição estadual nº , estabelecida no (a) _____, executa (ou executou) serviços de _____para este órgão (ou para esta empresa).

Atestamos (ou declaramos), ainda, que os compromissos assumidos pela empresa foram cumpridos satisfatoriamente, nada constando em nossos arquivos que o desabone comercial ou tecnicamente.

Local e data

Rio de Janeiro, 23 novembro de 2020

Documento assinado eletronicamente por **Daniel Luzente de Lima**, **Gerente**, em 05/01/2021, às 12:14, conforme horário oficial de Brasília, com fundamento nos art. 21º e 22º do Decreto nº 46.730, de 9 de agosto de 2019.

Documento assinado eletronicamente por **Elio Thomé de Souza Filho**, **Analista de Sistemas**, em 05/01/2021, às 12:17, conforme horário oficial de Brasília, com fundamento nos art. 21º e 22º do Decreto nº 46.730, de 9 de agosto de 2019.

A autenticidade deste documento pode ser conferida no site http://sei.fazenda.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **12098629** e o código CRC **096EAAE3**.

**Referência:** Processo nº E-04/171/221/2018 SEI nº 10651135

Rua da Conceição, 69, 24º Andar / 25º Andar - Bairro Centro, Rio de Janeiro/RJ, CEP 20051-011
Telefone:

Governo do Estado do Rio de Janeiro

Centro de Tecnologia da Informação e Comunicação do Estado do Rio de Janeiro

Vice Presidência de Tecnologia

# ANEXO VI

## LOCAL DE PRESTAÇÃO DOS SERVIÇOS

## REDE IP INTERNET ASSIMÉTRICA

## LOTE III – ENLACES REDE IP INTERNET ASSIMÉTRICA

| ENDEREÇO | CEP | LAT, LON | VELOC | ÓRGÃO |
|---|---|---|---|---|
| RUA BENEDITO HONORATO 147 - Ref: DENTRO DO CIEP - CENTRO - PINHEIRAL | 27197000 | | 10 Mbps | FAETEC |
| RUA VINTE DE ABRIL 14 - Ref: ETE TEATRO MARTINS PENA - CENTRO - RIO DE JANEIRO | 20231020 | | 10 Mbps | FAETEC |
| RUA JORN ANTONIO FREITAS 75 - Ref: FAETEC JUSCELINO KUBITSCHEK - JARDIM AMERICA - RIO DE JANEIRO | 21240535 | | 10 Mbps | FAETEC |
| AV GETULIO DE MOURA 1282 - Ref: FAETEC MESQUITA - JUSCELINO - MESQUITA | 26550070 | | 10 Mbps | FAETEC |
| RUA J AC R EDGARD WERNECK 1615 - Ref: FAETEC CIDADE DE DEUS - PECHINCHA - RIO DE JANEIRO | 22763011 | | 10 Mbps | FAETEC |
| VIA SERGIO BRAGA 0 - Ref: FAETEC DE BARRA MANSA - BARBARA - BARRA MANSA | 27265602 | -22.541795, -44.147679 | 10 Mbps | FAETEC |
| RUA CEL JOAO VALERIO 485 - Ref: FAETEC DE MAGE - CENTRO - MAGE | 25900097 | | 10 Mbps | FAETEC |
| EST DO BOITATA 0 - Ref: FAETEC DUQUE DE CAXIAS - CHACARA ARCAMPO - CAMPOS ELYSEOS | 25251130 | -22.6547245, -43.2798656 | 10 Mbps | FAETEC |
| AV ANTONIO GOMES 1260 - Ref: FAETEC ITABORAI - CALUNDU - ITABORAI | 24806682 | | 10 Mbps | FAETEC |
| VIA SERGIO BRAGA 0 - Ref: FAETERJ DE BARRA MANSA - BARBARA - BARRA MANSA | 27265602 | -22.541955, -44.147247 | 10 Mbps | FAETEC |
| ROD PREF RENATO DE ALVIM PADILHA 0 - Ref: RJ 186 KM 2 5 - NOVA DIVINEIA - S ANT PADUA | 28470000 | -21.531330, -42.141983 | 10 Mbps | FAETEC |
| RUA BR BARCELOS 0 - Ref: CIEP PROFESSOR GLADYS TEIXEIRA - CENTRO - S JOAO BARRA | 28200000 | -21.6368446, -41.0484428 | 15 Mbps | FAETEC |
| RUA JOAO VICENTE 1775 - Ref: EEEF VISCONDE DE MAUA - MARECHAL HERMES - RIO DE JANEIRO | 21610210 | | 15 Mbps | FAETEC |
| RUA CAP NUNES 0 - Ref: ETE HELBER VIGNOLI MUNIZ - JARDIM - SAQUAREMA | 28990310 | -22.894230, -42.477852 | 15 Mbps | FAETEC |
| RUA JOAO VICENTE 2151 - Ref: ETE TRANSPORTE ENG SILVA FREIRE - DEODORO - | 21610211 | | 15 Mbps | FAETEC |

| | | | | |
|---|---|---|---|---|
| RIO DE JANEIRO | | | | |
| RUA JOAO VICENTE 1775 - Ref: ETE VISCONDE DE MAUA - MARECHAL HERMES - RIO DE JANEIRO | 21610210 | | 15 Mbps | FAETEC |
| RUA JOAO VICENTE 1775 - Ref: ETE VISCONDE DE MAUA PREDIO MEC - MARECHAL HERMES - RIO DE JANEIRO | 21610210 | | 15 Mbps | FAETEC |
| RUA XAVIER CURADO 0 - Ref: FAETEC MARECHAL HERMES - MARECHAL HERMES - RIO DE JANEIRO | 21610330 | -22.859427, -43.375635 | 15 Mbps | FAETEC |
| RUA PAULO SERGIO NADER PEREIRA 0 - Ref: FAETEC - MENDES - CENTRO - MENDES | 26700000 | -22.526338, -43.730195 | 15 Mbps | FAETEC |
| RUA ROBERTO SILVEIRA 0 - Ref: FAETEC PIRAI - CENTRO - PIRAI | 27175000 | -22.622832, -43.912316 | 15 Mbps | FAETEC |
| RUA JOAO PEDRO SILVEIRA 0 - Ref: FAETEC AREAL - CENTRO - AREAL | 25845000 | -22.233985, -43.064304 | 15 Mbps | FAETEC |
| RUA JOSE ALVES PIMENTA 1520 - Ref: FAETEC BARRA DO PIRAI UNIDADE MATADOURO - MATADOURO - BARRA DO PIRAI | 27115010 | | 15 Mbps | FAETEC |
| RUA JOSE BENTO DE OLIVEIRA 1005 - Ref: FAETEC BARRA DO PIRAI UNIDADE PARQUE SSO JOAQUIM - QUIMICA - BARRA DO PIRAI | 27130270 | | 15 Mbps | FAETEC |
| RUA ABIGAIL PEREIRA 0 - Ref: FAETEC BATAN - REALENGO - RIO DE JANEIRO | 21730500 | -22.860565, -43.424525 | 15 Mbps | FAETEC |
| AV RIBEIRO DANTAS 0 - Ref: FAETEC DE BANGU - BANGU - RIO DE JANEIRO | 21870170 | -22.872162, -43.458510 | 15 Mbps | FAETEC |
| AV DEP LUIS FERNANDO LINHARES 454 - Ref: FAETEC DE MIRACEMA - CENTRO - MIRACEMA | 28460000 | | 15 Mbps | FAETEC |
| EST AUSTIN 0 - Ref: FAETEC DE NOVA IGUACU - COMENDADOR SOARES - NOVA IGUACU | 26280295 | -22.734919, -43.499935 | 15 Mbps | FAETEC |
| EST MACHADO FAGUNDES 326 - Ref: FAETEC DE PETROPOLIS - CASCATINHA - PETROPOLIS | 25716001 | | 15 Mbps | FAETEC |
| RUA NOSSA SENHORA APARECIDA 0 - Ref: FAETEC DE VALENCA - NS APARECIDA - VALENCA | 27600000 | -22.255821, -43.716143 | 15 Mbps | FAETEC |
| RUA ALUISIO DIAS MOREIRA 320 - Ref: FAETEC ITAPERUNA - PRES COSTA E SILVA - ITAPERUNA | 28300000 | | 15 Mbps | FAETEC |
| RUA BRAULIO CORDEIRO 915 - Ref: FAETEC JACARE - JACARE - RIO DE JANEIRO | 20975090 | | 15 Mbps | FAETEC |
| PCA PREF JOAQUIM JOSE FERREIRA 187 - Ref: FAETEC LEVY GASPARIAN - CENTRO - COM L GASPARIAN | 25870000 | | 15 Mbps | FAETEC |
| RUA GUARANY 0 - Ref: FAETEC MAGE UNIDADE PIABETA - PIABETA - PIABETA | 25931782 | -22.613783, -43.171490 | 15 Mbps | FAETEC |
| RUA FR AFONSO 0 - Ref: FAETEC MANGARATIBA - PRAIA SACO - MANGARATIBA | 23860000 | -22.9161789, -44.0389554 | 15 Mbps | FAETEC |
| RUA XAVIER CURADO 0 - Ref: FAETEC MARECHAL HERMES CVT - MARECHAL HERMES - RIO DE JANEIRO | 21610330 | -22.860622, -43.375711 | 15 Mbps | FAETEC |
| EST GEN OLIMPIO DA FONSECA 0 - Ref: FAETEC NILOPOLIS UNIDADE PAIOL DE POLVORA - OLINDA - NILOPOLIS | 26545470 | -22.813269, -43.394595 | 15 Mbps | FAETEC |

| | | | | |
|---|---|---|---|---|
| RUA XAVIER CURADO 0 - Ref: FAETEC OSCAR TENORIO - MARECHAL HERMES - RIO DE JANEIRO | 21610330 | -22.862006, -43.377087 | 15 Mbps | FAETEC |
| RUA EDNA 0 - Ref: FAETEC QUEIMADOS - QUEIMADOS - QUEIMADOS | 26325210 | -22.7189334, -43.5522550 | 15 Mbps | FAETEC |
| RUA MIL E QUINZE LTO VOLTA GRANDE 0 - Ref: FAETERJ AMAURY CESAR VIEIRA - SANTO AGOSTINHO - VOLTA REDONDA | 27210240 | -22.487767, -44.070365 | 15 Mbps | FAETEC |
| RUA ARISTIDES FIGUEIREDO 147 - Ref: FAETERJ BOM JESUS DE ITABAPOANA - CENTRO - B J ITABAPOANA | 28360000 | -22.872162, -43.458510 | 15 Mbps | FAETEC |
| AV WILSON BATISTA 0 - Ref: FAETERJ AGRICOLA ANTONIO SARLO - PARQUE ALDEIA - CAMP GOYTACAZES | 28060560 | -21.720947, -41.343977 | 15 Mbps | FAETEC |
| RUA DEZ DE MAIO 512 - Ref: FAETERJ ITAPERUNA - CENTRO - ITAPERUNA | 28300000 | | 15 Mbps | FAETEC |
| RUA LUIS DE LIMA 272 - Ref: ETE JOAO LUIZ DO NASCIMENTO - CENTRO - NOVA IGUACU | 26221080 | | 5 Mbps | FAETEC |
| LGO DO BODEGAO 46 - Ref: ETE SANTA CRUZ - SANTA CRUZ - RIO DE JANEIRO | 23550050 | | 5 Mbps | FAETEC |
| RUA VSC DE NITEROI 1072 - Ref: FAETEC MANGUEIRA - MANGUEIRA - RIO DE JANEIRO | 20943001 | | 5 Mbps | FAETEC |
| AV DR RANDOLFO PENNA 840 - Ref: FAETEC PARAIBA DO SUL - JATOBA - PARAIBA DO SUL | 25850000 | | 5 Mbps | FAETEC |
| RUA BR DE ITAPAGIPE 311 - Ref: FAETEC TIJUCA - TIJUCA - RIO DE JANEIRO | 20261105 | | 5 Mbps | FAETEC |
| AV TEN ENEAS TORNO 70 - Ref: FAETEC TRES RIOS - NOVA NITEROI - TRES RIOS | 25802330 | | 5 Mbps | FAETEC |
| RUA LUIS FERNANDES CARRIELO 39 - Ref: FAETEC BOM JARDIM - JD ORNELAS - BOM JARDIM | 28660000 | | 5 Mbps | FAETEC |
| AV JOSE BENTO RIBEIRO DANTAS 0 - Ref: FAETEC BUZIOS - BAIA FORMOSA - ARMACAO BUZIOS | 28950000 | -22.752216, -41.963699 | 5 Mbps | FAETEC |
| LGO DO BODEGAO 46 - Ref: FAETEC SANTA CRUZ - SANTA CRUZ - RIO DE JANEIRO | 23550050 | | 5 Mbps | FAETEC |
| RUA AUGUSTO RUSH 0 - Ref: FAETEC SAO GONCALO UNIDADE COLUBANDE - COLUBANDE - SAO GONCALO | 24451650 | -22.833937, -43.007067 | 5 Mbps | FAETEC |
| RUA ITAPERA 500 - Ref: FAETEC VIA BRASIL - IRAJA - RIO DE JANEIRO | 21230500 | | 5 Mbps | FAETEC |
| AV TEN ENEAS TORNO 70 - Ref: FAETERJ TRES RIOS - NOVA NITEROI - TRES RIOS | 25802330 | | 5 Mbps | FAETEC |
| AV BARTOLOMEU DE GUSMAO 850 - Ref: FAETERJ ADOLPHO BLOCH - SAO CRISTOVAO - RIO DE JANEIRO | 20941160 | | 5 Mbps | FAETEC |
| AV MARIA TERESA 0 - CAMPO GRANDE - RIO DE JANEIRO | 23050160 | -22.9056647, -43.5659961 | 15 Mbps | PCERJ |
| RUA GEN DIONISIO 0 - JD 25 AGOSTO - DUQUE DE CAXIAS | 25075095 | -22.792997, -43.302258 | 15 Mbps | PCERJ |
| RUA BR MIRACEMA 0 - CENTRO - CAMP GOYTACAZES | 28035302 | -21.7540787, -41.3272999 | 15 Mbps | PCERJ |
| RUA DR COUTINHO 6 - CENTRO - ANGRA DOS REIS | 23900620 | | 15 Mbps | PCERJ |
| | | | | |

| | | | | |
|---|---|---|---|---|
| AV ACTURA 7 - CAMPOS ELISEOS - CAMPOS ELYSEOS | 25225210 | | 15 Mbps | PCERJ |
| RUA PEDRO I 28 - CENTRO - RIO DE JANEIRO | 20060050 | | 15 Mbps | PCERJ |
| RUA PEDRO I 28 - CENTRO - RIO DE JANEIRO | 20060050 | | 15 Mbps | PCERJ |
| RUA PROF CLEMENTINO FRAGA 77 - CENTRO - RIO DE JANEIRO | 20230250 | | 15 Mbps | PCERJ |
| RUA BAMBINA 140 - BOTAFOGO - RIO DE JANEIRO | 22251050 | | 15 Mbps | PCERJ |
| RUA FR CANECA 162 - CENTRO - RIO DE JANEIRO | 20211040 | | 15 Mbps | PCERJ |
| ROD GEN BRUNO MARTINS 0 - ALCALIS - ARRAIAL DO CABO | 28930000 | -22.9673373, -42.0268099 | 15 Mbps | PCERJ |
| RUA ZENI ESTEVES 0 - CENTRO - MIGUEL PEREIRA | 26900000 | -22.4577356, -43.4806903 | 15 Mbps | PCERJ |
| EST DO PIAI 0 - GUARATIBA - RIO DE JANEIRO | 23028050 | -22.983616, -43.661711 | 15 Mbps | PCERJ |
| RUA STA FILOMENA 1 - PCA DA BANDEIRA - RIO DE JANEIRO | 20270110 | -22.9139729, -43.2147925 | 15 Mbps | PCERJ |
| RUA DA RELACAO 42 - CENTRO - RIO DE JANEIRO | 20231110 | | 15 Mbps | PCERJ |
| RUA DA RELACAO 42 - CENTRO - RIO DE JANEIRO | 20231110 | | 15 Mbps | PCERJ |
| AV CASTRO ALVES 120 - PORTAO VERMELHO - TRES RIOS | 25808020 | | 15 Mbps | PCERJ |
| AV AFRANIO DE MELO FRANCO 175 - LEBLON - RIO DE JANEIRO | 22430060 | | 15 Mbps | PCERJ |
| RUA GEN ESPIRITO SANTO CARDOSO 208 - TIJUCA - RIO DE JANEIRO | 20530500 | | 15 Mbps | PCERJ |
| AV GOMES FREIRE 491 - CENTRO - RIO DE JANEIRO | 20231014 | | 15 Mbps | PCERJ |
| EST CORREIO IMPERIAL 1073 - PITEIRA - QUISSAMA | 28735000 | | 15 Mbps | PCERJ |
| AV BRAZ DE PINA 1105 - PENHA CIRCULAR - RIO DE JANEIRO | 21210673 | | 15 Mbps | PCERJ |
| AV MARIA TERESA 0 - CAMPO GRANDE - RIO DE JANEIRO | 23050160 | -22.863307, -43.544774 | 15 Mbps | PCERJ |
| RUA TIARAJU 0 - CAMPO GRANDE - RIO DE JANEIRO | 23050040 | -22.904259, -43.566475 | 15 Mbps | PCERJ |
| RUA MAL BENTO MANOEL 0 - JD 25 AGOSTO - DUQUE DE CAXIAS | 25075270 | -22.792964, -43.302278 | 15 Mbps | PCERJ |
| RUA PARQUE 0 - PR FERRADURA - ARMACAO BUZIOS | 28950000 | -22.774539, -41.927267 | 15 Mbps | PCERJ |
| RUA PETER SHUTZWENCE 0 - FANCHEM - QUEIMADOS | 26383450 | -22.706453, -43.565111 | 15 Mbps | PCERJ |
| RUA ANA FRANK 0 - PENHA CIRCULAR - RIO DE JANEIRO | 21210040 | -22.845485, -43.304350 | 15 Mbps | PCERJ |
| EST DO PIAI 0 - GUARATIBA - RIO DE JANEIRO | 23028050 | -22.983625, -43.661707 | 15 Mbps | PCERJ |
| ROD GEN BRUNO MARTINS 0 - ALCALIS - ARRAIAL DO CABO | 28930000 | 22.937571, -42.189030 | 15 Mbps | PCERJ |
| AV DR ARRUDA NEGREIROS 0 - CENTRO - S JOAO MERITI | 25520001 | -22.805603, -43.376042 | 15 Mbps | PCERJ |
| RUA ZENI ESTEVES 0 - CENTRO - MIGUEL PEREIRA | 26900000 | -22.481719, -43.505091 | 15 Mbps | PCERJ |
| AV MAL FONTENELLE 0 - CAMPO DOS AFONSOS - RIO DE JANEIRO | 21740900 | -22.884274, -43.404175 | 15 Mbps | PCERJ |

| | | | | |
|---|---|---|---|---|
| RUA LEMOS CUNHA 0 - ICARAI - NITEROI | 24230136 | -22.908194, -43.103273 | 15 Mbps | PCERJ |
| RUA BR MIRACEMA 0 - CENTRO - CAMP GOYTACAZES | 28035302 | -21.756606, -41.328418 | 15 Mbps | PCERJ |
| RUA GEN IVAN RAPOSO 0 - BARRA DA TIJUCA - RIO DE JANEIRO | 22621040 | -23.0102881, -43.3136040 | 15 Mbps | PCERJ |
| RUA LIBERDADE 0 - PASSAGEM - CABO FRIO | 28906140 | -22.878970, -42.018896 | 15 Mbps | PCERJ |
| AV TEIXEIRA E SOUZA 0 - CENTRO - CABO FRIO | 28909971 | -22.889950, -42.034069 | 15 Mbps | PCERJ |
| RUA GEN DIONISIO 0 - JD 25 AGOSTO - DUQUE DE CAXIAS | 25075095 | -22.792980, -43.302267 | 15 Mbps | PCERJ |
| RUA STA FILOMENA 1 - PCA DA BANDEIRA - RIO DE JANEIRO | 20270110 | | 15 Mbps | PCERJ |
| RUA PRES CASTELO BRANCO 2 - CENTRO - NITEROI | 24030260 | | 15 Mbps | PCERJ |
| RUA DR COUTINHO 6 - CENTRO - ANGRA DOS REIS | 23900620 | | 15 Mbps | PCERJ |
| AV ACTURA 7 - CAMPOS ELISEOS - CAMPOS ELYSEOS | 25225210 | | 15 Mbps | PCERJ |
| RUA GEN BELFORD 14 - ROCHA - RIO DE JANEIRO | 20961000 | | 15 Mbps | PCERJ |
| PCA GETULIO VARGAS 20 - CENTRO - MAGE | 25900112 | | 15 Mbps | PCERJ |
| RUA PEDRO I 28 - CENTRO - RIO DE JANEIRO | 20060050 | | 15 Mbps | PCERJ |
| RUA PEDRO I 28 - CENTRO - RIO DE JANEIRO | 20060050 | | 15 Mbps | PCERJ |
| RUA DESIDERIO DE OLIVEIRA 33 - CENTRO - NITEROI | 24030310 | | 15 Mbps | PCERJ |
| RUA DESIDERIO DE OLIVEIRA 33 - CENTRO - NITEROI | 24030310 | | 15 Mbps | PCERJ |
| AV FLORIPES ROCHA 38 - CENTRO - BELFORD ROXO | 26113340 | | 15 Mbps | PCERJ |
| RUA DA RELACAO 42 - CENTRO - RIO DE JANEIRO | 20231110 | | 15 Mbps | PCERJ |
| RUA DA RELACAO 42 - CENTRO - RIO DE JANEIRO | 20231110 | | 15 Mbps | PCERJ |
| RUA DA RELACAO 42 - CENTRO - RIO DE JANEIRO | 20231110 | | 15 Mbps | PCERJ |
| RUA DA RELACAO 42 - CENTRO - RIO DE JANEIRO | 20231110 | | 15 Mbps | PCERJ |
| RUA DA RELACAO 42 - CENTRO - RIO DE JANEIRO | 20231110 | | 15 Mbps | PCERJ |
| RUA DA RELACAO 42 - CENTRO - RIO DE JANEIRO | 20231110 | | 15 Mbps | PCERJ |
| RUA DA RELACAO 42 - CENTRO - RIO DE JANEIRO | 20231110 | | 15 Mbps | PCERJ |
| RUA PROF CLEMENTINO FRAGA 77 - CENTRO - RIO DE JANEIRO | 20230250 | | 15 Mbps | PCERJ |
| RUA JORGE RUDGE 104 - VILA ISABEL - RIO DE JANEIRO | 20550220 | | 15 Mbps | PCERJ |
| AV CASTRO ALVES 120 - PORTAO VERMELHO - TRES RIOS | 25808020 | | 15 Mbps | PCERJ |
| RUA BAMBINA 140 - BOTAFOGO - RIO DE JANEIRO | 22251050 | | 15 Mbps | PCERJ |
| RUA DO LAVRADIO 155 - CENTRO - RIO DE JANEIRO | 20230070 | | 15 Mbps | PCERJ |
| RUA FR CANECA 162 - CENTRO - RIO DE | 20211040 | | 15 Mbps | PCERJ |

| | | | | |
|---|---|---|---|---|
| JANEIRO | | | | |
| RUA FR CANECA 162 - CENTRO - RIO DE JANEIRO | 20211040 | | 15 Mbps | PCERJ |
| AV AFRANIO DE MELO FRANCO 175 - LEBLON - RIO DE JANEIRO | 22430060 | | 15 Mbps | PCERJ |
| RUA GEN ESPIRITO SANTO CARDOSO 208 - TIJUCA - RIO DE JANEIRO | 20530500 | | 15 Mbps | PCERJ |
| AV DQ DE CAXIAS 334 - DEODORO - RIO DE JANEIRO | 21615220 | | 15 Mbps | PCERJ |
| RUA HAROLDO LOBO 400 - PORTUGUESA - RIO DE JANEIRO | 21931580 | | 15 Mbps | PCERJ |
| AV GOMES FREIRE 491 - CENTRO - RIO DE JANEIRO | 20231014 | | 15 Mbps | PCERJ |
| RUA FR CANECA 505 - ESTACIO - RIO DE JANEIRO | 20211020 | | 15 Mbps | PCERJ |
| RUA FR CANECA 505 - ESTACIO - RIO DE JANEIRO | 20211020 | | 15 Mbps | PCERJ |
| RUA FR CANECA 505 - ESTACIO - RIO DE JANEIRO | 20211020 | | 15 Mbps | PCERJ |
| EST CORREIO IMPERIAL 1073 - PITEIRA - QUISSAMA | 28735000 | | 15 Mbps | PCERJ |
| AV BRAZ DE PINA 1105 - PENHA CIRCULAR - RIO DE JANEIRO | 21210673 | | 15 Mbps | PCERJ |
| AV N SRA DE COPACABANA 1260 - COPACABANA - RIO DE JANEIRO | 22070012 | | 15 Mbps | PCERJ |
| RUA PARQUE 0 - Ref: 127 DELEGACIA POLICIAL - PR FERRADURA - ARMACAO BUZIOS | 28950000 | -22.762783, -41.889467 | 50 Mbps | PCERJ |
| RUA HAROLDO LOBO 400 - Ref: 37 DP CONTATO NO LOCAL CIRO TEL 985967326. - PORTUGUESA - RIO DE JANEIRO | 21931580 | | 50 Mbps | PCERJ |
| PCA GETULIO VARGAS 20 - Ref: 65 DELEGACIA LEGAL - MAGE - CENTRO - MAGE | 25900112 | | 50 Mbps | PCERJ |
| RUA DESIDERIO DE OLIVEIRA 33 - Ref: DELEGACIA DE HOMICIDIOS NITEROI SAO GONCALO PROV II - CENTRO - NITEROI | 24030310 | | 50 Mbps | PCERJ |
| RUA BERTA LUTZ 80 - Ref: DELEGACIA ROCINHA - GAVEA - RIO DE JANEIRO | 22450290 | | 50 Mbps | PCERJ |
| RUA CDOR LAJE 44 - Ref: DPO DO 17 BPM EM PAQUETA - PAQUETA - RIO DE JANEIRO | 20396010 | | 50 Mbps | PCERJ |
| RUA FR CANECA 162 - Ref: IPPGF - LABORATORIO GENETICA - CENTRO - RIO DE JANEIRO | 20211040 | | 50 Mbps | PCERJ |
| AV FLORIPES ROCHA 38 - Ref: PCERJ - DELEGACIA DE HOMICIDIOS - BAIXADA FLUMINENSE - CENTRO - BELFORD ROXO | 26113340 | | 50 Mbps | PCERJ |
| AV TEIXEIRA E SOUZA 0 - Ref: PROXIMO N 1966 - CENTRO - CABO FRIO | 28909971 | -22.889968, -42.034059 | 50 Mbps | PCERJ |
| RUA LIBERDADE 0 - Ref: UNIDADE PRPTC - CABO FRIO - PASSAGEM - CABO FRIO | 28906140 | -22.8786864, -42.0095107 | 50 Mbps | PCERJ |
| RUA DA RELACAO 42 - CENTRO - RIO DE JANEIRO | 20231110 | | 50 Mbps | PCERJ |
| RUA DA RELACAO 42 - CENTRO - RIO DE JANEIRO | 20231110 | | 50 Mbps | PCERJ |
| RUA DA RELACAO 42 - CENTRO - RIO DE | 20231110 | | 50 Mbps | PCERJ |

| | | | | |
|---|---|---|---|---|
| JANEIRO | | | | |
| RUA DA RELACAO 42 - CENTRO - RIO DE JANEIRO | 20231110 | | 50 Mbps | PCERJ |
| RUA DA RELACAO 42 - CENTRO - RIO DE JANEIRO | 20231110 | | 50 Mbps | PCERJ |
| RUA BERTA LUTZ 80 - GAVEA - RIO DE JANEIRO | 22450290 | | 50 Mbps | PCERJ |
| RUA DA RELACAO 42 - CENTRO - RIO DE JANEIRO | 20231110 | | 50 Mbps | PCERJ |
| RUA DA RELACAO 42 - CENTRO - RIO DE JANEIRO | 20231110 | | 50 Mbps | PCERJ |
| RUA DA RELACAO 42 - CENTRO - RIO DE JANEIRO | 20231110 | | 50 Mbps | PCERJ |
| RUA DA RELACAO 42 - CENTRO - RIO DE JANEIRO | 20231110 | | 50 Mbps | PCERJ |
| RUA DA RELACAO 42 - CENTRO - RIO DE JANEIRO | 20231110 | | 50 Mbps | PCERJ |
| RUA DA RELACAO 42 - CENTRO - RIO DE JANEIRO | 20231110 | | 50 Mbps | PCERJ |
| RUA DA RELACAO 42 - CENTRO - RIO DE JANEIRO | 20231110 | | 50 Mbps | PCERJ |
| RUA DA RELACAO 42 - CENTRO - RIO DE JANEIRO | 20231110 | | 50 Mbps | PCERJ |
| RUA DA RELACAO 42 - CENTRO - RIO DE JANEIRO | 20231110 | | 50 Mbps | PCERJ |
| RUA BR DE MESQUITA 669 - ANDARAI - RIO DE JANEIRO | 20540155 | | 10 Mbps | PMERJ |
| RUA BR DE MESQUITA 669 - ANDARAI - RIO DE JANEIRO | 20540155 | | 10 Mbps | PMERJ |
| AV MAL FONTENELLE 2906 - VILA MILITAR - RIO DE JANEIRO | 21750001 | | 10 Mbps | PMERJ |
| RUA EVARISTO DA VEIGA 78 - CENTRO - RIO DE JANEIRO | 20031040 | | 10 Mbps | PMERJ |
| AV NOSSA SENHORA DE FATIMA 0 - VL SAO JOAO - VILAR DOS TELES | 25561171 | -22.916593, -43.188285 | 5 Mbps | PMERJ |
| RUA LUCIDIO LAGO 181 - MEIER - RIO DE JANEIRO | 20780020 | | 5 Mbps | PMERJ |
| AV MAL FONTENELLE 2906 - VILA MILITAR - RIO DE JANEIRO | 21750001 | | 5 Mbps | PMERJ |
| RUA INGLATERRA 0 - JARDIM CAICARA - CABO FRIO | 28910360 | -22.882900, -42.034554 | 5 Mbps | PMERJ |
| RUA JOSE ESPINOLA ELIAS 0 - SANTO AMARO - RESENDE | 27513130 | -22.482147, -44.449151 | 5 Mbps | PMERJ |
| ROD AMARAL PEIXOTO 1 - TRIBOBO - NITEROI | 24750491 | | 5 Mbps | PMERJ |
| AV SALVADOR DE SA 2 - CIDADE NOVA - RIO DE JANEIRO | 20211260 | | 5 Mbps | PMERJ |
| AV SALVADOR DE SA 2 - CIDADE NOVA - RIO DE JANEIRO | 20211260 | | 5 Mbps | PMERJ |
| AV SALVADOR DE SA 2 - CIDADE NOVA - RIO DE JANEIRO | 20211260 | | 5 Mbps | PMERJ |
| RUA EVARISTO DA VEIGA 78 - CENTRO - RIO DE JANEIRO | 20031040 | | 5 Mbps | PMERJ |
| RUA SALVADOR MENDONCA 208 - CENTRO - ITABORAI | 24800161 | | 5 Mbps | PMERJ |

| | | | | |
|---|---|---|---|---|
| RUA GUANDU 680 - PIMENTEIRAS - TERESOPOLIS | 25963620 | | 5 Mbps | PMERJ |
| AV MAL FONTENELLE 2906 - VILA MILITAR - RIO DE JANEIRO | 21750001 | | 5 Mbps | PMERJ |
| AV MAL FONTENELLE 2906 - VILA MILITAR - RIO DE JANEIRO | 21750001 | | 5 Mbps | PMERJ |
| RUA CAMPO BELO 0 - LARANJEIRAS - RIO DE JANEIRO | 22221110 | -22.929333, -43.189774 | 5 Mbps | PMERJ |
| RUA ASIA 0 - VILA MARGARIDA - ITAGUAI | 23821130 | -22.872228, -43.789155 | 5 Mbps | PMERJ |
| RUA DR ALFREDO BACKER 367 - MUTONDO - NITEROI | 24452001 | | 5 Mbps | PMERJ |
| RUA OLIVEIRA BOTELHO 1677 - NEVES - NITEROI | 24425005 | | 5 Mbps | PMERJ |
| AV MAL FONTENELLE 2906 - VILA MILITAR - RIO DE JANEIRO | 21750001 | | 5 Mbps | PMERJ |
| RUA REGINA 0 - CENTRO - MESQUITA | 26210350 | -22.756487, -43.447476 | 5 Mbps | PMERJ |
| RUA MACKENZIE 0 - BALDEADOR - NITEROI | 24140020 | -22.879823, -43.077042 | 5 Mbps | PMERJ |
| AV FELICIANO SODRE 0 - CENTRO - NITEROI | 24030014 | -22.883034, -43.117060 | 5 Mbps | PMERJ |
| RUA EVARISTO DA VEIGA 78 - CENTRO - RIO DE JANEIRO | 20031040 | | 5 Mbps | PMERJ |
| RUA EVARISTO DA VEIGA 78 - CENTRO - RIO DE JANEIRO | 20031040 | | 5 Mbps | PMERJ |
| AV OSWALDO CRUZ 175 - FLAMENGO - RIO DE JANEIRO | 22250060 | | 5 Mbps | PMERJ |
| ROD RJ 186 2000 - GLORIA - S ANT PADUA | 28470000 | | 5 Mbps | PMERJ |
| AV MAL FONTENELLE 2906 - VILA MILITAR - RIO DE JANEIRO | 21750001 | | 5 Mbps | PMERJ |
| AV MAL FONTENELLE 2906 - VILA MILITAR - RIO DE JANEIRO | 21750001 | | 5 Mbps | PMERJ |
| AV MAL FONTENELLE 2906 - VILA MILITAR - RIO DE JANEIRO | 21750001 | | 5 Mbps | PMERJ |
| AV MAL FONTENELLE 2906 - VILA MILITAR - RIO DE JANEIRO | 21750001 | | 5 Mbps | PMERJ |
| RUA TUNIS 0 - BANGU - RIO DE JANEIRO | 21850365 | -22.856658, -43.485099 | 5 Mbps | PMERJ |
| AV JOAQUIM DA COSTA LIMA 0 - SAO BERNARDO - BELFORD ROXO | 26165225 | -22.7588169, -43.4011319 | 5 Mbps | PMERJ |
| AV AMARAL PEIXOTO 0 - MIRAMAR - MACAE | 27943400 | -22.354631, -41.770075 | 5 Mbps | PMERJ |
| RUA CANDEIAS 0 - CAMPO GRANDE - RIO DE JANEIRO | 23055030 | -22.906922, -43.574169 | 5 Mbps | PMERJ |
| RUA VSC DE NITEROI 1 - MANGUEIRA - RIO DE JANEIRO | 20943000 | | 5 Mbps | PMERJ |
| AV SALVADOR DE SA 2 - CIDADE NOVA - RIO DE JANEIRO | 20211260 | | 5 Mbps | PMERJ |
| AV SALVADOR DE SA 2 - CIDADE NOVA - RIO DE JANEIRO | 20211260 | | 5 Mbps | PMERJ |
| RUA ESTACIO DE SA 20 - ESTACIO - RIO DE JANEIRO | 20211270 | | 5 Mbps | PMERJ |
| RUA EVARISTO DA VEIGA 78 - CENTRO - RIO DE JANEIRO | 20031040 | | 5 Mbps | PMERJ |
| RUA TACARATU 94 - HONORIO GURGEL - RIO DE JANEIRO | 21555010 | | 5 Mbps | PMERJ |
| AV FELICIANO SODRE 190 - CENTRO - NITEROI | 24030011 | | 5 Mbps | PMERJ |
| RUA MARTINS TORRES 245 - SANTA ROSA - NITEROI | 24240705 | | 5 Mbps | PMERJ |

| | | | | |
|---|---|---|---|---|
| RUA PEDRO CORREIA 273 - VL MERITI - DUQUE DE CAXIAS | 25020160 | | 5 Mbps | PMERJ |
| EST PAU FERRO 435 - PECHINCHA - RIO DE JANEIRO | 22743050 | | 5 Mbps | PMERJ |
| RUA CARDOSO JUNIOR 479 - LARANJEIRAS - RIO DE JANEIRO | 22245000 | | 5 Mbps | PMERJ |
| EST DO RIO JEQUIA 518 - ZUMBI - RIO DE JANEIRO | 21930185 | | 5 Mbps | PMERJ |
| RUA PARANAPANEMA 769 - OLARIA - RIO DE JANEIRO | 21073185 | | 5 Mbps | PMERJ |
| AL S BOAVENTURA 773 - FONSECA - NITEROI | 24130001 | | 5 Mbps | PMERJ |
| EST DO GUANDU DO SENA 1954 - BANGU - RIO DE JANEIRO | 21854002 | | 5 Mbps | PMERJ |
| AV MAL FONTENELLE 2906 - VILA MILITAR - RIO DE JANEIRO | 21750001 | | 5 Mbps | PMERJ |
| RUA PAULO TEIXEIRA DOS SANTOS 0 - CENTRO - MAGE | 25900082 | -22.654776, -43.038197 | 5 Mbps | PMERJ |
| AV JANSEN DE MELO 0 - CENTRO - NITEROI | 24030221 | -22.885268, -43.115714 | 5 Mbps | PMERJ |
| AV NOSSA SENHORA DE FATIMA 0 - VL SAO JOAO - VILAR DOS TELES | 25561171 | -22.8096595, -43.4366753 | 5 Mbps | PMERJ |
| RUA ALVARO RAMOS 155 - BOTAFOGO - RIO DE JANEIRO | 22280110 | | 5 Mbps | PMERJ |
| EST DO GUANDU DO SENA 1954 - BANGU - RIO DE JANEIRO | 21854002 | | 5 Mbps | PMERJ |
| ROD AMARAL PEIXOTO 9500 - VARZEA DAS MOCAS - NITEROI | 24330286 | | 5 Mbps | PMERJ |
| AV FELICIANO SODRE 0 - CENTRO - NITEROI | 24030014 | -22.882968, -43.117636 | 5 Mbps | PMERJ |
| AV FELICIANO SODRE 0 - CENTRO - NITEROI | 24030014 | -22.882968, -43.117636 | 5 Mbps | PMERJ |
| RUA ESTACIO DE SA 20 - ESTACIO - RIO DE JANEIRO | 20211270 | | 5 Mbps | PMERJ |
| RUA PROF CLEMENTINO FRAGA 49 - CENTRO - RIO DE JANEIRO | 20230250 | | 5 Mbps | PMERJ |
| RUA EVARISTO DA VEIGA 78 - CENTRO - RIO DE JANEIRO | 20031040 | | 5 Mbps | PMERJ |
| RUA MQ DE POMBAL 128 - CENTRO - RIO DE JANEIRO | 20230240 | | 5 Mbps | PMERJ |
| RUA PEDRO CORREIA 273 - VL MERITI - DUQUE DE CAXIAS | 25020160 | | 5 Mbps | PMERJ |
| AV FELICIANO SODRE 275 - CENTRO - NITEROI | 24030012 | | 5 Mbps | PMERJ |
| RUA PARANAPANEMA 769 - OLARIA - RIO DE JANEIRO | 21073185 | | 5 Mbps | PMERJ |
| RUA PARANAPANEMA 965 - OLARIA - RIO DE JANEIRO | 21073185 | | 5 Mbps | PMERJ |
| RUA STA FE 26 - MEIER - RIO DE JANEIRO | 20775065 | | 5 Mbps | PMERJ |
| RUA TEN ALDIR SOARES ADRIANO 45 - CENTRO - MESQUITA | 26551180 | | 5 Mbps | PMERJ |
| RUA CAP CESAR DE ANDRADE 119 - Ref: 23 BPM - LEBLON - RIO DE JANEIRO | 22431010 | | 5 Mbps | PMERJ |
| RUA CEL LUIS FERRAZ 307 - Ref: 29 BPM ITAPERUNA - CENTRO - ITAPERUNA | 28300000 | | 5 Mbps | PMERJ |
| RUA MOCAMBIQUE 18 - Ref: 3 DPJM - NOVA IGUACU - POSSE - NOVA IGUACU | 26030620 | | 5 Mbps | PMERJ |
| EST PADUA PIRAPETINGA 0 - Ref: 36. BPM - SANTA AFRA - SANTA AFRA - S ANT PADUA | 28470000 | -21.553543, -42.178222 | 5 Mbps | PMERJ |

| | | | | |
|---|---|---|---|---|
| AV PASTOR MARTIN LUTHER KING JR 8848 - Ref: 41 BPM - CEASA - CAIXOTARIA - ENTRADA SUL - COLEGIO - RIO DE JANEIRO | 21530013 | | 5 Mbps | PMERJ |
| RUA JOSE ALVES PIMENTA 923 - Ref: 5 DPJM - MATADOURO - BARRA DO PIRAI | 27115010 | | 5 Mbps | PMERJ |
| RUA TEN CEL CARDOSO 200 - Ref: 8 BPM - CENTRO - CAMP GOYTACAZES | 28010802 | | 5 Mbps | PMERJ |
| RUA PARATINGA 0 - Ref: 9. BPM - VISTA ALEGRE - VISTA ALEGRE - RIO DE JANEIRO | 21230772 | -22.854666, -43.353395 | 5 Mbps | PMERJ |
| AV ITAOCA 0 - Ref: ANTIGA COCA COLA - BONSUCESSO - RIO DE JANEIRO | 21061902 | -22.867521, -43.268267 | 5 Mbps | PMERJ |
| AV SALVADOR DE SA 2 - Ref: AO LADO DO BPCHQ - GRUPAMENTO TATICO DE MOTOCICLISTA - CIDADE NOVA - RIO DE JANEIRO | 20211260 | | 5 Mbps | PMERJ |
| RUA FIGUEIREDO MAGALHAES 550 - Ref: AO LADO DO METRO DE COPACAPANA - 19 BATALHAO DE POL - COPACABANA - RIO DE JANEIRO | 22031012 | | 5 Mbps | PMERJ |
| AV ITAOCA 0 - Ref: C EST. DO TIMBO 1 CPA - BONSUCESSO - RIO DE JANEIRO | 21061902 | -22.867507, -43.268282 | 5 Mbps | PMERJ |
| AV MAL FONTENELLE 2906 - Ref: CCRIM - CENTRO DE CRIMINALISTICA - VILA MILITAR - RIO DE JANEIRO | 21750001 | | 5 Mbps | PMERJ |
| RUA ARINDO DA SILVA ALVES 126 - Ref: CCRIM - CENTRO DE CRIMINALISTICA - PADRE MIGUEL - RIO DE JANEIRO | 21720320 | | 5 Mbps | PMERJ |
| RUA PARANHOS 820 - Ref: CENTRO FISIATRIA REABILITACAO PMERJ - OLARIA - RIO DE JANEIRO | 21073460 | | 5 Mbps | PMERJ |
| AV MAL FONTENELLE 2906 - Ref: CIEAT-CENTRO DE INSTRUCAO ESPECIAL EM ARMAMENTO/TIRO - VILA MILITAR - RIO DE JANEIRO | 21750001 | | 5 Mbps | PMERJ |
| AL S BOAVENTURA 1134 - Ref: COLEGIO DA POLICIA MILITAR - FONSECA - NITEROI | 24120344 | | 5 Mbps | PMERJ |
| RUA FRANCISCO EUGENIO 228 - Ref: DAS - DIRETORIA DE ASSISTENCIA SOCIAL - SAO CRISTOVAO - RIO DE JANEIRO | 20941120 | | 5 Mbps | PMERJ |
| AV MAL FONTENELLE 2906 - Ref: DEI - DIRETORIA DE ENSINO E INSTRUCAO - VILA MILITAR - RIO DE JANEIRO | 21750001 | | 5 Mbps | PMERJ |
| RUA BAHIA 638 - Ref: DPO DE MURIQUI - CENTRO - VILA MURIQUI | 23870000 | | 5 Mbps | PMERJ |
| EST CAETANO MONTEIRO 0 - Ref: ESQUINA COM FRANCISCO DA CRUZ NUNES - 12 BPM - LARGO DA BATALHA - NITEROI | 24320570 | -22.885344, -43.115726 | 5 Mbps | PMERJ |
| RUA MACKENZIE 0 - Ref: FONSECA - BALDEADOR - NITEROI | 24140020 | -22.879823, -43.077042 | 5 Mbps | PMERJ |
| EST CANTAGALO 500 - Ref: GPAE/RECEPCAO - COPACABANA - RIO DE JANEIRO | 22071060 | | 5 Mbps | PMERJ |
| RUA OLIVEIRA BOTELHO 1677 - Ref: NEVES - NEVES - NITEROI | 24425005 | | 5 Mbps | PMERJ |
| AV N SRA DO AMPARO 0 - Ref: NITEROI - NITEROI - VOLTA REDONDA | 27283370 | | 5 Mbps | PMERJ |

| | | | | |
|---|---|---|---|---|
| PCA DA BANDEIRA 0 - Ref: POLICIA MILITAR - VILA NOVA - NOVA FRIBURGO | 28630040 | -22.2937210, -42.5380994 | 5 Mbps | PMERJ |
| RUA BR DE MESQUITA 625 - Ref: POLICIA MILITAR - ANDARAI - RIO DE JANEIRO | 20540155 | | 5 Mbps | PMERJ |
| AV MAL FONTENELLE 2906 - Ref: PREDIO ANEXO - VILA MILITAR - RIO DE JANEIRO | 21750001 | | 5 Mbps | PMERJ |
| AV MAL FONTENELLE 2906 - Ref: PROERD SULACAP - VILA MILITAR - RIO DE JANEIRO | 21750001 | | 5 Mbps | PMERJ |
| RUA CARLOS SEIXAS 0 - Ref: UPP CAJU - SEDE /// RUA 3 - CAJU - RIO DE JANEIRO | 20931007 | -22.879697, -43.230314 | 5 Mbps | PMERJ |
| AV N SRA DO AMPARO 0 - Ref: VOLDAC - NITEROI - VOLTA REDONDA | 27283370 | -22.465570, -44.102741 | 5 Mbps | PMERJ |
| RUA MARIA SOARES SENDAS 111 - VENDA VELHA - VILAR DOS TELES | 25575825 | | 15 Mbps | PRODERJ |
| RUA NELSON ALFRADICK 0 CENTRO - SILVA JARDIM | 28820000 | -22.653939, -42.387590 | 10 Mbps | SEAPPA |
| RUA INT FRANKLIN RABELO 0 NATIVIDADE - NATIVIDADE | 28380000 | -21.039315, -41.982959 | 10 Mbps | SEAPPA |
| RUA NILO PECANHA 20 CENTRO - CASSIMIRO ABREU | 28860000 | | 10 Mbps | SEAPPA |
| RUA VINHOSA 133 VINHOSA - ITAPERUNA | 28300000 | | 10 Mbps | SEAPPA |
| RUA DR LUIS CARNEIRO DE MENDONCA 170 CENTRO - VALENCA | 27600000 | | 10 Mbps | SEAPPA |
| AV DEP LUIS FERNANDO LINHARES 263 CENTRO - MIRACEMA | 28460000 | | 10 Mbps | SEAPPA |
| RUA FR FIDELIS 0 - Ref: AN2 - RESTAURANTE POPULAR CENTRO - DUQUE DE CAXIAS | 25011060 | -22.793116, -43.310214 | 10 Mbps | SEAPPA |
| AV JOAO BATISTA PORTUGAL 279 - Ref: CENTRO CENTRO - RIO CLARO | 27460000 | | 10 Mbps | SEAPPA |
| AV SAQUAREMA 5122 - Ref: EMATER - BACAXA CENTRO - SAQUAREMA | 28990786 | | 10 Mbps | SEAPPA |
| RUA CEL ALFREDO 0 - Ref: EMP. ASST. TECNICA CENTRO - TRAJANO MORAIS | 28750000 | -22.063752, -42.062800 | 10 Mbps | SEAPPA |
| AV ALBERTO BRAUNE 224 - Ref: SL 300 - EMATER CENTRO - NOVA FRIBURGO | 28613000 | | 10 Mbps | SEAPPA |
| RUA MANUEL DIZ MARTINEZ 0 CENTRO - CACH MACACU | 28680000 | -22.465730, -42.656246 | 5 Mbps | SEAPPA |
| PCA DR NILO PECANHA 0 CENTRO - CAMP GOYTACAZES | 28010045 | -21.764767, -41.337535 | 5 Mbps | SEAPPA |
| RUA GETULIO VARGAS 0 CANTAGALO - CORDEIRO | 28540000 | -22.028853, -42.355807 | 5 Mbps | SEAPPA |
| AV PARANHOS 0 CENTRO - MACUCO | 28545000 | -21.9844505, -42.2531991 | 5 Mbps | SEAPPA |
| RUA ISMAR GOMES DE AZEVEDO 13 CENTRO - CABO FRIO | 28907100 | | 5 Mbps | SEAPPA |
| RUA EVARISTO SILVA RIBEIRO 65 CENTRO - CONC MACABU | 28740000 | | 5 Mbps | SEAPPA |
| AV PARANHOS 365 CENTRO - SAO FIDELIS | 28400000 | | 5 Mbps | SEAPPA |
| RUA MORAIS SANTOS 1032 CENTRO - BARRA DO PIRAI | 27113000 | | 5 Mbps | SEAPPA |
| RUA MOREIRA DOS SANTOS 1042 CENTRO - BARRA DO PIRAI | 27130430 | | 5 Mbps | SEAPPA |
| AV VINTE E DOIS DE MAIO 7557 PARQUE INDUSTRIAL - ITABORAI | 24800109 | | 5 Mbps | SEAPPA |
| AV SIMAO DA MOTTA 0 CENTRO - MAGE | 25900001 | -22.659676, -43.036268 | 5 Mbps | SEAPPA |

| | | | | |
|---|---|---|---|---|
| RUA UIRAPURUS 0 FLAMENGO - MARICA | 24903640 | -22.9122516, -42.8076973 | 5 Mbps | SEAPPA |
| RUA DOMINGOS MOTA 85 MADRUGA - VASSOURAS | 27700000 | | 5 Mbps | SEAPPA |
| RUA OTAVIO TARQUINO 774 CENTRO - NOVA IGUACU | 26215342 | | 5 Mbps | SEAPPA |
| ROD BR 356 0 CENTRO - ITALVA | 28250000 | -21.419735, -41.692070 | 5 Mbps | SEAPPA |
| RUA FLAVIO MACHADO ABDALLA 0 CENTRO - STA M MADALENA | 28770000 | -21.951938, -42.008463 | 5 Mbps | SEAPPA |
| PCA CRUZEIRO 0 MANGUEIRINHA - RIO BONITO | 28800000 | -22.718386, -42.643836 | 5 Mbps | SEAPPA |
| ROD RJ 116 0 CENTRO - VALAO DO BARRO | 28555000 | -21.8241684, -42.0870524 | 5 Mbps | SEAPPA |
| RUA DAVI VIEIRA NEY 0 CENTRO - SAO JOSE DE UBA | 28455000 | -21.359023, -41.942151 | 5 Mbps | SEAPPA |
| RUA PROJETADA 9 PORTO REAL - QUATIS | 27570000 | | 5 Mbps | SEAPPA |
| RUA GONCALVES VIEIRA 143 CENTRO - PORCIUNCULA | 28390000 | | 5 Mbps | SEAPPA |
| RUA CEL FRANCISCO LIMONGI 171 CENTRO - SJV PRETO | 25780000 | | 5 Mbps | SEAPPA |
| AV CIRCULAR OCIDENTAL 375 NOVA NITEROI - TRES RIOS | 25802336 | | 5 Mbps | SEAPPA |
| RUA JOSE ALENCAR 930 CENTRO - SUMIDOURO | 28637000 | | 5 Mbps | SEAPPA |
| RUA MOREIRA DOS SANTOS 1034 CENTRO - BARRA DO PIRAI | 27130430 | | 5 Mbps | SEAPPA |
| RUA DR BERNARDO VASCONCELOS 791 - Ref: AO LADO DO HOSPITAL REGIONAL CENTRO - ARARUAMA | 28970000 | | 5 Mbps | SEAPPA |
| RUA JOSE TUPINI 27 - Ref: EMATER CENTRO - VARRE SAI | 28375000 | | 5 Mbps | SEAPPA |
| AV PRES VARGAS 180 - Ref: EMATER PARQUE PECUARIA - CAMP GOYTACAZES | 28053100 | | 5 Mbps | SEAPPA |
| AV STA TERESA 94 - Ref: EMP. ASS. TECNICA CENTRO - RIO DAS FLORES | 27660000 | | 5 Mbps | SEAPPA |
| AV PRES GETULIO VARGAS 38 - Ref: EMP. ASSIT. TECNICA CENTRO - DUAS BARRAS | 28650000 | | 5 Mbps | SEAPPA |
| AV SEBASTIAO LUTERBACK SOBRINHO 70 - Ref: EMP. ASSIT. TECNICA CENTRO - CARMO | 28640000 | | 5 Mbps | SEAPPA |
| AV EMB PASCHOAL CARLOS MAGNO 650 - Ref: EMP. ASSIT. TECNICA ARCOZELO - PATY DO ALFERES | 26950000 | | 5 Mbps | SEAPPA |
| AV MIN FERNANDO COSTA 0 - Ref: KM 7 TO - PREDIO DA PESAGRO RJ UNIVER RURAL - SEROPEDICA | 23894358 | -22.758479, -43.684385 | 5 Mbps | SEAPPA |
| EST ROGERIO DE MOURA ESTEVAO 0 - Ref: KM 7,3 PRQ EXPOSICOES ALBUQUERQUE - TERESOPOLIS | 25976440 | -22.386050, -42.901686 | 5 Mbps | SEAPPA |
| ROD RIO SANTOS 0 - Ref: KM97,5 JAPUIBA - ANGRA DOS REIS | 23942325 | -22.9442395, -44.3169994 | 5 Mbps | SEAPPA |
| RUA SEIS AC BEIRA RIO 0 - Ref: LT17 - RUA DA FEIRINHA PORTO PARATI - PARATI | 23970000 | -23.219854, -44.711625 | 5 Mbps | SEAPPA |
| RUA GETULIO VARGAS 0 - Ref: PDFRENT - CANTAGALO - CORDEIRO | 28540000 | -22.028853, -42.355807 | 5 Mbps | SEAPPA |
| PCA TOLEDO PIZZA 0 - Ref: PREFEITURA MUNICIPAL DE ITAOCARA - EM CIMA DA | 28570000 | -21.666353, -42.079424 | 5 Mbps | SEAPPA |

| | | | | |
|---|---|---|---|---|
| RODOVI CENTRO - ITAOCARA | | | | |
| PCA MQ SAO JOAO MARCOS 6 - Ref: SJ - EMP. ASSIT. TECNICA CENTRO - PARAIBA DO SUL | 25850000 | | 5 Mbps | SEAPPA |
| PCA OSCAR JOSE FERNANDES 4 - Ref: SL2 - EMP. ASS. TECNICA CENTRO - SAPUCAIA | 25880000 | | 5 Mbps | SEAPPA |
| ALAMENDA SÃO BOA VENTURA, 770- FONSECA, NITERÓI - | 24120191 | | 15 Mbps | SEAPPA |
| AV. ALMIRANTE JÚLIO CÉSAR DE NORONHA, 317 - SÃO BENTO – ANGRA DOS REIS – RJ | 23900-000 | | 5 Mbps | SEAPPA |
| RUA DR. BATISTA, S/Nº - PARQUE DE EXPOSIÇÕES – FAZENDINHA – ARARUAMA – RJ | 28970000 | | 5 Mbps | SEAPPA |
| RUA MOREIRA SANTOS, 1032 SALA 101 – CENTRO – BARRA DO PIRAÍ – RJ | 27130000 | | 5 Mbps | SEAPPA |
| AVENIDA JOÃO CHIESSE FILHO N° 312 - PARQUE DA CIDADE - BAIRRO BOA VISTA | 27320410 | | 5 Mbps | SEAPPA |
| RUA FRANCISCO BORGES SOBRINHO, 151 - CENTRO - BOM JESUS DO ITABAPOANA - RJ | 28360000 | | 5 Mbps | SEAPPA |
| RJ 116 KM 33,5 TABOADO – SINDICATO RURAL – CACHOEIRAS DE MACACU -RJ | 28680000 | | 5 Mbps | SEAPPA |
| RUA VISCONDE DE INHAÚMA, Nº 102 – PARQUE TAMANDARÉ – CAMPOS DOS GOYTACAZES – RJ | 28030160 | | 5 Mbps | SEAPPA |
| ESTRADA SERRA MAR, RJ 142, KM 01 - QUIOSQUE DE INF. TUR. - BOX 05 E 06 - BAIRRO INDUSTRIAL - CASIMIRO DE ABREU - RJ | 28860000 | | 5 Mbps | SEAPPA |
| RUA PRESIDENTE GETÚLIO VARGAS, Nº 197 - POSTO ZOOTÉCNICO - CENTRO – CORDEIRO – RJ. | 28540000 | | 5 Mbps | SEAPPA |
| RUA CORONEL PITA DE CASTRO, Nº 247 – CENTRO - ITAOCARA – RJ | 28570000 | | 5 Mbps | SEAPPA |
| AVENIDA DEPUTADO RUBENS TINOCO FERRAZ, 21 – CIDADE NOVA – ITAPERUNA | 28300000 | | 5 Mbps | SEAPPA |
| RUA FRANCISCO PORTELA, Nº 489 – CENTRO – MACAÉ – RJ. | 27910200 | | 5 Mbps | SEAPPA |
| RUA INTENDENTE FRANKLIN RABELLO, S/Nº - CENTRO – SINDICATO – NATIVIDADE – RJ | 28380000 | | 5 Mbps | SEAPPA |
| RUA EUCLIDES SOLON PONTES, N° 30 - CENTRO - NOVA FRIBURGO - RJ | 28625020 | | 5 Mbps | SEAPPA |
| AVENIDA GUADALARRARA Nº 125 – CENTRO - PIRAÍ – RJ | 27175000 | | 5 Mbps | SEAPPA |
| ESTRADA UNIÃO INDÚSTRIA, 11.590 – BLOCO B/SALA 103 - ITAIPAVA - PETRÓPOLIS - RJ | 25770220 | | 5 Mbps | SEAPPA |
| AV CEL. BRASIL, N° 33 - CAMPOS ELISIOS - RESENDE - RJ | 27542150 | | 5 Mbps | SEAPPA |
| AVENIDA BRASIL, 19001 - IRAJÁ - RIO DE JANEIRO - RJ | 21539900 | | 5 Mbps | SEAPPA |
| RUA VEREADOR DILSON BATISTA SOARES, 108 - ARRANCHADOURO SANTA MARIA MADALENA – RJ | 28770000 | | 5 Mbps | SEAPPA |
| RUA FLORISMUNDO DECNOP, Nº 255 – SANTO ANTÔNIO DE PÁDUA – RJ | 28470000 | | 5 Mbps | SEAPPA |
| RUA JOAQUIM DA MOTA SOBRINHO N.º 230- | | | 5 Mbps | SEAPPA |

| | | | | |
|---|---|---|---|---|
| ALTO-CENTRO-SÃO FRANCISCO DE ITABAPOANA – RJ | | | | |
| AVENIDA PARANHOS, 365 – SÃO FIDÉLIS – RJ | 28400000 | | 5 Mbps | SEAPPA |
| RUA DEMERVAL GARCIA DE FREITAS S/N° - CENTRO - TANGUÁ - RJ. | 24890000 | | 5 Mbps | SEAPPA |
| RUA RITA CERQUEIRA, 61 - CENTRO - TRÊS RIOS - RJ | 25804210 | | 5 Mbps | SEAPPA |
| RUA OSIRES DE PAIVA SOUZA Nº 1012 - BENFICA - VALENÇA - RIO DE JANEIRO - RJ | | | 5 Mbps | SEAPPA |
| RUA FERNANDO PEDROSA FERNANDES, N.º 20, SALA 16 – TERM. ROD. HÉLIO DE ANDRADE PINTO – VASSOURAS – RJ | 27700000 | | 5 Mbps | SEAPPA |
| ALAMENDA SÃO BOA VENTURA, 770-FONSECA, NITERÓI - | 24120191 | | 5 Mbps | SEAPPA |
| AV FELICIANO SODRE 0 - Ref: SEDRAP - CENTRO - NITEROI | 24030014 | -22.8834728, -43.1175983 | 5 Mbps | SEDRAP |
| EST DAS FURNAS 1467 - Ref: ESCOLA ARTHUR ANTONIO SENDAS - ALTO DA BOA VISTA - RIO DE JANEIRO | 20531572 | | 10 Mbps | SEEDUC |
| RUA CRISTOVAO PADILHA CAMPOS 36 - CENTRO - CARABUCU | 28372000 | | 15 Mbps | SEEDUC |
| RUA SEN ALFREDO NEVES 76 - GOIABAL - CACH MACACU | 28680000 | | 15 Mbps | SEEDUC |
| RUA JOSE RODRIGUES POVOAS 561 - GAMBOA - CABO FRIO | 28924180 | | 15 Mbps | SEEDUC |
| RUA JOSE BENTO DE OLIVEIRA 1005 - QUIMICA - BARRA DO PIRAI | 27130270 | | 15 Mbps | SEEDUC |
| RUA VER SEBASTIAO DE CARVALHO 1789 - AREAL - BARRA DO PIRAI | 27150160 | | 15 Mbps | SEEDUC |
| RUA JOAO FRANCISCO ALMEIDA 439 - Ref: CE ALBERTO TORRES - CENTRO - S JOAO BARRA | 28200000 | | 15 Mbps | SEEDUC |
| RUA GETULIO VARGAS 100 - Ref: CE ALFREDO GOMES - CENTRO - CONSERVATORIA | 27655000 | | 15 Mbps | SEEDUC |
| RUA ALLAN KARDEC 254 - Ref: CE ALMIRANTE RODRIGUES SILVA - FATIMA - VALENCA | 27600000 | | 15 Mbps | SEEDUC |
| PCA PREF JOAQUIM JOSE FERREIRA 0 - Ref: CE CORONEL ANTONIO PECANHA - CENTRO - COM L GASPARIAN | 25870000 | -22.118331, -43.212040 | 15 Mbps | SEEDUC |
| PCA PE GOMES LEAL 303 - Ref: CE CORONEL BENJAMIN GUIMARAES - CENTRO - VALENCA | 27600000 | | 15 Mbps | SEEDUC |
| RUA ALFREDO MAURICIO SILVA 0 - Ref: CE CORONEL JOAO LIMONGI - CENTRO - SJV PRETO | 25780000 | -22.150126, -42.923602 | 15 Mbps | SEEDUC |
| AV DEP LUIS FERNANDO LINHARES 214 - Ref: CE DEODATO LINHARES - CENTRO - MIRACEMA | 28460000 | | 15 Mbps | SEEDUC |
| RUA BONIFACIO PORTELA 22 - Ref: CE DOUTOR ANTONIO FERNANDES - CENTRO - MIGUEL PEREIRA | 26900000 | | 15 Mbps | SEEDUC |
| AV SANTA CRUZ 2 - Ref: CE DOUTOR JOAO NERY - HUMBERTO ANTUNES - MENDES | 26700000 | | 15 Mbps | SEEDUC |
| AV DORALICE RANGEL FELIZARDO 0 - Ref: CE DOUTOR OLIMPIO SATURNINO DE BRITO - DEGREDO - DEGREDO | 28200000 | -21.636731, -41.048416 | 15 Mbps | SEEDUC |
| | | | | |

| | | | | |
|---|---|---|---|---|
| RUA VALDEMAR CRISTIANO 497 - Ref: CE DOUTOR OSWALDO TERRA - VL FERROVIAR - VALENCA | 27600000 | | 15 Mbps | SEEDUC |
| RUA HERMINIA SANTOS SILVA 0 - Ref: CE EMILIA ROSCHEMANT - CENTRO - RIOGRANDINA | 28634330 | -22.190911, -42.507290 | 15 Mbps | SEEDUC |
| RUA JOSE ALBERONE 115 - Ref: CE EUCLIDES FELICIANO TARDIN - CENTRO - B J ITABAPOANA | 28360000 | | 15 Mbps | SEEDUC |
| RUA MANUEL PORTUGAL 191 - Ref: CE FAGUNDES VARELA - CENTRO - RIO CLARO | 27460000 | | 15 Mbps | SEEDUC |
| AV AMARAL PEIXOTO 234 - Ref: CE JANUARIO DE TOLEDO PIZZA - CENTRO - VALAO DO BARRO | 28555000 | | 15 Mbps | SEEDUC |
| RUA FIRMINO FARIA 2 - Ref: CE JOAO DE ABREU JUNIOR - CENTRO - BOA SORTE | 28525000 | | 15 Mbps | SEEDUC |
| PCA ROGER MALHARDES 7 - Ref: CE JOAO KOPKE - CENTRO - ENG P FRONTIN | 26650000 | | 15 Mbps | SEEDUC |
| RUA STA LUZIA 75 - Ref: CE JOSE CARDOSO DE MORAES - CENTRO - IPITUNA | 28557000 | | 15 Mbps | SEEDUC |
| AV NILO PECANHA 82 - Ref: CE JOSE FONSECA - CENTRO - VALENCA | 27600000 | | 15 Mbps | SEEDUC |
| RUA DR NILO PECANHA 166 - Ref: CE MINISTRO RAUL FERNANDES - CENTRO - VASSOURAS | 27700000 | | 15 Mbps | SEEDUC |
| AV MAL CASTELO BRANCO 903 - Ref: CE MONSENHOR FRANCISCO - CENTRO - PARAIBA DO SUL | 25850000 | | 15 Mbps | SEEDUC |
| RUA PROF SOUZA 124 - Ref: CE OLIVEIRA VIANA - BACAXA - SAQUAREMA | 28994750 | | 15 Mbps | SEEDUC |
| RUA SAO SEBASTIAO 173 - Ref: CE OSCAR BATISTA - CENTRO - S JOAO PARAISO | 28450000 | | 15 Mbps | SEEDUC |
| EST REAL DE MAUA 2015 - Ref: CE OSWALDO CRUZ - IPIRANGA - MAGE | 25927112 | | 15 Mbps | SEEDUC |
| RUA TANGUARA 247 - Ref: CE PADRE SEBASTIAO DA SILVA PEREIRA - CENTRO - VALENCA | 27600000 | | 15 Mbps | SEEDUC |
| RUA LUIZ FELICIANO CARDOSO 0 - Ref: CE PRAIA DO SIQUEIRA - PRAIA SIQUEIRA - CABO FRIO | 28912090 | -22.874006, -42.051921 | 15 Mbps | SEEDUC |
| AV OPERARIOS 205 - Ref: CE PRESIDENTE RODRIGUES ALVES - CENTRO - PARACAMBI | 26600000 | | 15 Mbps | SEEDUC |
| RUA GUARANY 0 - Ref: CE PROFESSOR ALFREDO BALTHAZAR DA SILVEIRA - PIABETA - PIABETA | 25931782 | -22.613653, -43.171760 | 15 Mbps | SEEDUC |
| RUA MARIO MESQUITA 147 - Ref: CE PROFESSOR AURELIO DUARTE - CENTRO - CARMO | 28640000 | | 15 Mbps | SEEDUC |
| RUA RIO JANEIRO 0 - Ref: CE PROFESSOR CORDELINO TEIXEIRA PAULO - JRD PERO - CAMINHO BUZIOS | 28920100 | -22.839857, -42.012869 | 15 Mbps | SEEDUC |
| RUA BRASIL 153 - Ref: CE PROFESSORA ALDA BERNARDO DOS SANTOS TAVARES - CENTRO - PIABETA | 25931778 | | 15 Mbps | SEEDUC |
| AV N SRA DA CONCEICAO 118 - Ref: CE | 24830080 | | 15 Mbps | SEEDUC |

| | | | | |
|---|---|---|---|---|
| PROFESSORA MARIA INOCENCIA FERREIRA - PORTO DAS CAIXAS - PORTO CAXIAS | | | | |
| RUA CARLOS CONDACK 0 - Ref: CE SALUSTIANO JOSE RIBEIRO SERAFIM - SAO GERALDO - NOVA FRIBURGO | 28630487 | -22.241712, -42.551017 | 15 Mbps | SEEDUC |
| PCA VSC RIO PRETO 401 - Ref: CE THEODORICO FONSECA - CENTRO - VALENCA | 27600000 | | 15 Mbps | SEEDUC |
| RUA DR MACEDO 334 - Ref: CE VISCONDE DE ITABORAI - CENTRO - ITABORAI | 24800213 | | 15 Mbps | SEEDUC |
| RUA CDOR ARAUJO LEITE 265 - Ref: CEJA DOUTOR OSWALDO DA CUNHA FONSECA - CENTRO - VALENCA | 27600000 | | 15 Mbps | SEEDUC |
| AV MAL PAULO TORRES 551 - Ref: CIEP 297 PADRE SALESIO SCHIMID - CENTRO - VASSOURAS | 27700000 | | 15 Mbps | SEEDUC |
| AV AMERICO DA COSTA CARDOSO 0 - Ref: CIEP 308 PASCOAL CARLOS MAGNO - NOVA CIDADE - ITABORAI | 24804033 | -22.754867, -42.847885 | 15 Mbps | SEEDUC |
| RUA PORTO ALEGRE 0 - Ref: CIEP 331 LYSIA BERNARDES - AQUARIUS - TAMOIOS | 28925742 | -22.607585, -42.004491 | 15 Mbps | SEEDUC |
| AV GOV GEREMIAS MATTOS FONTES 0 - Ref: EE MARCILIO DIAS - CENTRO - NOVA FRIBURGO | 28613140 | -22.288748, -42.533776 | 15 Mbps | SEEDUC |
| RUA AMARAL 30 - Ref: ESCOLA SEEDUC - ANDARAI - RIO DE JANEIRO | 20541155 | | 15 Mbps | SEEDUC |
| RUA MATOSO MAIA 250 - Ref: IE DE MIRACEMA - CENTRO - MIRACEMA | 28460000 | | 15 Mbps | SEEDUC |
| RUA JOSE ALVES PIMENTA 1250 - Ref: UN 287 ANGELINA TEIXEIRA NETTO SYM - MATADOURO - BARRA DO PIRAI | 27115010 | | 15 Mbps | SEEDUC |
| TV JOSE PINTO MACEDO 10 - Ref: UN DE ARRAIAL DO CABO - PRAINHA - ARRAIAL DO CABO | 28930000 | | 15 Mbps | SEEDUC |
| RUA DR BERNARDO VASCONCELOS 425 - Ref: UN EDMUNDO SILVA - CENTRO - ARARUAMA | 28970000 | | 15 Mbps | SEEDUC |
| AV PRES GETULIO VARGAS 2 - Ref: UN MARIANO PROCOPIO - CENTRO - AREAL | 25845000 | | 15 Mbps | SEEDUC |
| AV LUCIO MEIRA 311 - Ref: MESMA INSTALACAO TRL 1936803 - VARZEA - TERESOPOLIS | 25953002 | | 5 Mbps | SEEDUC |
| RUA DOZE OUTUBRO 0 - Ref: SEEDUC - BELA VISTA - S PEDRO ALDEIA | 28941188 | | 5 Mbps | SEEDUC |
| RUA JOSE ALENCAR LEITE 89 - Ref: SEEDUC - SAPAL - S ANT PADUA | 28470000 | | 5 Mbps | SEEDUC |
| RUA DUZENTOS E VINTE E DOIS 122 - Ref: SEEDUC - CONFORTO - VOLTA REDONDA | 27265050 | | 5 Mbps | SEEDUC |
| AV LUCIO TOME FETEIRA 0 - Ref: SEEDUC - VILA LAGE - NITEROI | 24415000 | -22.844007, -43.084946 | 5 Mbps | SEEDUC |
| RUA FRANKLIN JOSE SANTOS 0 - Ref: SEEDUC. - CENTRO - CASSIMIRO ABREU | 28860000 | | 5 Mbps | SEEDUC |
| PCA CRISTIANO OTONI 0 - CENTRO - RIO DE JANEIRO | 20221250 | -22.9037938, -43.1905740 | 5 Mbps | SESEG |
| PCA CRISTIANO OTONI 0 - CENTRO - RIO DE JANEIRO | 20221250 | -22.9037938, -43.1905740 | 5 Mbps | SESEG |
| | | | | |

| | | | | |
|---|---|---|---|---|
| AVENIDA ERASMO BRAGA, 118, ANDAR 11, CENTRO. RIO DE JANEIRO - RJ | 20020000 | | 50 Mbps | Rádio Roquete Pinto |
| MUNICÍPIO DO ESTADO DO RJ | | | 35 Mbps | Rádio Roquete Pinto |
| MUNICÍPIO DO ESTADO DO RJ | | | 35 Mbps | Rádio Roquete Pinto |
| MUNICÍPIO DO ESTADO DO RJ | | | 35 Mbps | Rádio Roquete Pinto |
| MUNICÍPIO DO ESTADO DO RJ | | | 35 Mbps | Rádio Roquete Pinto |
| MUNICÍPIO DO ESTADO DO RJ | | | 35 Mbps | Rádio Roquete Pinto |
| MUNICÍPIO DO ESTADO DO RJ | | | 35 Mbps | Rádio Roquete Pinto |
| MUNICÍPIO DO ESTADO DO RJ | | | 35 Mbps | Rádio Roquete Pinto |
| MUNICÍPIO DO ESTADO DO RJ | | | 35 Mbps | Rádio Roquete Pinto |
| MUNICÍPIO DO ESTADO DO RJ | | | 35 Mbps | Rádio Roquete Pinto |
| MUNICÍPIO DO ESTADO DO RJ | | | 35 Mbps | Rádio Roquete Pinto |
| MUNICÍPIO DO ESTADO DO RJ | | | 35 Mbps | Rádio Roquete Pinto |
| MUNICÍPIO DO ESTADO DO RJ | | | 35 Mbps | Rádio Roquete Pinto |
| MUNICÍPIO DO ESTADO DO RJ | | | 15 Mbps | Rádio Roquete Pinto |
| MUNICÍPIO DO ESTADO DO RJ | | | 15 Mbps | Rádio Roquete Pinto |
| MUNICÍPIO DO ESTADO DO RJ | | | 15 Mbps | Rádio Roquete Pinto |
| MUNICÍPIO DO ESTADO DO RJ | | | 15 Mbps | Rádio Roquete Pinto |
| MUNICÍPIO DO ESTADO DO RJ | | | 15 Mbps | Rádio Roquete Pinto |
| MUNICÍPIO DO ESTADO DO RJ | | | 15 Mbps | Rádio |

| | | | | |
|---|---|---|---|---|
| | | | | Roquete Pinto |
| MUNICÍPIO DO ESTADO DO RJ | | | 15 Mbps | Rádio Roquete Pinto |
| MUNICÍPIO DO ESTADO DO RJ | | | 15 Mbps | Rádio Roquete Pinto |
| MUNICÍPIO DO ESTADO DO RJ | | | 15 Mbps | Rádio Roquete Pinto |
| MUNICÍPIO DO ESTADO DO RJ | | | 15 Mbps | Rádio Roquete Pinto |
| MUNICÍPIO DO ESTADO DO RJ | | | 15 Mbps | Rádio Roquete Pinto |
| MUNICÍPIO DO ESTADO DO RJ | | | 15 Mbps | Rádio Roquete Pinto |
| RUA GENERAL ALMERIO DE MOURA, Nº 320 - BAIRRO SÃO CRISTÓVÃO | 20621060 | | 5 Mbps | SES |
| AV. EUTERPE FRIBURGUENSE, Nº 93 - CENTRO - NOVA FRIBURGO | 28605130 | | 5 Mbps | SES |
| RUA GALDINO LESSA Nº 78 (CASA LARANJA) - CENTRO - ITAPERUNA | 28300000 | | 5 Mbps | SES |
| AV. PRESIDENTE KENEDY, 333, 2º ANDAR- BRASILÃNDIA - SÃO GONÇALO | 24440490 | | 5 Mbps | SES |
| AV. LÚCIO MEIRA, 375, PRÉDIO ANEXO (FUNDOS), 2º ANDAR - VÁRZEA - CENTRO - TERESÓPOLIS | 25953002 | | 5 Mbps | SES |
| RUA DA MAÇONARIA, Nº 320 - CENTRO - TRÊS RIOS - ONDE ESTAVA LOCALIZADO O HEMONÚCLEO | 25805025 | | 5 Mbps | SES |
| RUA FLORISBELA ROSA PENHA - S/Nº - BRAGA - CABO FRIO - ANEXO AO HOSPITAL DA MULHER | 28900000 | | 5 Mbps | SES |
| AVENIDA EUTERPE FRIBURGUENSE, 93 - CENTRO - NOVA FRIBURGO | 28605130 | | 5 Mbps | SES |
| AV. GENERAL OSVALDO CORDEIRO DE FARIAS, Nº 466 - MARECHAL HERMES | 21610480 | | 5 Mbps | SES |
| RUA DO RESENDE, 148/156 - BAIRRO DE FÁTIMA - CENTRO - RJ | 20231092 | | 5 Mbps | SES |
| AV. SÃO PEDRO, 300 - CENTRO - SÃO PEDRO DA ALDEIA - SALA 204 | 28940000 | | 5 Mbps | SES |
| AV. SÃO PEDRO, 300 - CENTRO - SÃO PEDRO DA ALDEIA - SALA 204 | 28940000 | | 5 Mbps | SES |
| RUA CORONEL ROMOALDO MONTEIRO DE BARROS, 11 - ALTOS - CIDADE NOVA - ITAPERUNA | 28300000 | | 5 Mbps | SES |
| RUA DON WALMOR. 234 - SALA 505 - CENTRO - NOVA IGUAÇU - RJ | | | 5 Mbps | SES |
| RUA CELSO CARRILHO, 458.PONTO DE REFERÊNCIA: RUA ATRÁS DO HOSPITAL DO CARMO RJ | 28640000 | | 5 Mbps | SES |

| | | | | |
|---|---|---|---|---|
| RUA JÚLIO DO CARMO Nº 175 - CIDADE NOVA - RJ | 20211160 | | 5 Mbps | SES |
| AV. MARECHAL FLORIANO Nº 586 - JARDIM 25 DE AGOSTO - DUQUE DE CAXIAS - RJ | 25075025 | | 5 Mbps | SES |
| AV. GOVERNADOR ROBERTO SILVEIRA - Nº 210 - CENTRO - NOVA IGUAÇU - RJ | 26210210 | | 5 Mbps | SES |
| RUA MÉXICO 128 - SALA 501 - CENTRO - RJ | 20031142 | | 5 Mbps | SES |
| NDVS – TRÊS RIOS – RUA MARECHAL DEODORO DA FONSECA – 315 - CENTRO TRÊS RIOS | 25802220 | | 15 Mbps | SES |
| CECA - ANA NERY – RUA ANA NERY – 1029 – ROCHA | 20960006 | | 25 Mbps | SES |
| RUA AILTON DA COSTA, S/N, BAIRRO 25 DE AGOSTO, DUQUE DE CAXIAS - RJ | 25071-160 | | 50 Mbps | CECIERJ |
| AV. DOS TRABALHADORES, 179. JACUECANGA | | | 50 Mbps | CECIERJ |
| RUA ANTÔNIO DA SILVA BRINCO, N° 976, CAMPO BOM | | | 50 Mbps | CECIERJ |
| RUA MAUÁ, S/N – SÃO BERNARDO | | | 50 Mbps | CECIERJ |
| AV. GOV. ROBERTO SILVEIRA, 578. CENTRO | | | 50 Mbps | CECIERJ |
| AV. MANOEL CALDEIRA DE ALVARENGA.1203. CAMPO GRANDE | | | 50 Mbps | CECIERJ |
| RUA CEL. MANOEL MARCELINO DE PAULA, 108 - CENTRO | | | 50 Mbps | CECIERJ |
| RUA MARECHAL FLORIANO, 555. JARDIM 25 DE AGOSTO | | | 50 Mbps | CECIERJ |
| RUA IVETE LINO RIBEIRO, 125 CENTRO | | | 50 Mbps | CECIERJ |
| R NILO PEÇANHA, 471. CENTRO | | | 50 Mbps | CECIERJ |
| AV. ZULAMITH BITTENCOURT, S/N. BAIRRO PRESIDENTE COSTA E SILVA | | | 50 Mbps | CECIERJ |
| ROD. AMAR. PEIXOTO, KM164 – IMBOACICA | | | 50 Mbps | CECIERJ |
| AV. PADRE ANCHIETA, 163. CENTRO | | | 50 Mbps | CECIERJ |
| RUA LUIS EUGÊNIO, 61 - GOV. PORTELA | | | 50 Mbps | CECIERJ |
| AV. DEPUTADO LUIZ FERNANDO LINHARES, S/N. CENTRO | | | 50 Mbps | CECIERJ |
| RUA VIGÁRIO JOÃO BATISTA, 3. CENTRO | | | 50 Mbps | CECIERJ |
| RUA SOARES MIRANDA, 77. FONSECA | | | 50 Mbps | CECIERJ |
| AV. JOSÉ PIRES BARROSO, S/N. OLARIA | | | 50 Mbps | CECIERJ |
| RUA DOUTOR PAULO FRÓES MACHADO, 38. CENTRO. ANTIGO FORUM | | | 50 Mbps | CECIERJ |
| RUA SEBASTIÃO DE LACERDA, S/N. FÁBRICA | | | 50 Mbps | CECIERJ |
| ESTRADA MACHADO FAGUNDES, 326 - CASCATINHA | | | 50 Mbps | CECIERJ |
| R ROBERTO SILVEIRA, 86 – CENTRO | | | 50 Mbps | CECIERJ |
| AV. TEN. CEL. ADALBERTO MENDES, 1920. BAIRRO VILA SANTA ISABEL | | | 50 Mbps | CECIERJ |
| BR 101 (SENTIDO RIO), KM 265, BAIRRO PRAÇA CRUZEIRO | | | 50 Mbps | CECIERJ |
| RUA CEL. EURICO DE LACERDA CASTRO, 12. CENTRO | | | 50 Mbps | CECIERJ |
| RUA BERTHA LUTZ, 85. SÃO CONRADO | | | 50 Mbps | CECIERJ |
| R HONÓRIO DUBOIS, S/N. CENTRO | | | 50 Mbps | CECIERJ |
| RUA ELYSIO DA COSTA SANTOS S/N – DIRLEY PERLINGEIRO DE ABREU | | | 50 Mbps | CECIERJ |
| | | | | |

| | | | | |
|---|---|---|---|---|
| RUA ANTONIO PINHEIRO FILHO, 2 – CENTRO | | | 50 Mbps | CECIERJ |
| RUA VISCONDE DE ITAÚNA, S/N. GRADIM | | | 50 Mbps | CECIERJ |
| RUA A, S/N. NOVA SÃO PEDRO DA ALDEIA | | | 50 Mbps | CECIERJ |
| RUA ANTONIO FERREIRA, 110. RIO DA AREIA, BACAXÁ | | | 50 Mbps | CECIERJ |
| R MARECHAL DEODORO, 117 –CENTRO | | | 50 Mbps | CECIERJ |
| R 539, S/N – JARDIM PARAÍBA | | | 50 Mbps | CECIERJ |
| CORONEL CARVALHO, 230, ANEXO AO COLÉGIO DOUTOR ARTUR VARGAS, ALA E. CENTRO - ANGRA DOS REIS - RJ | 23900-135 | | 50 Mbps | CECIERJ |
| RUA OSCAR CLARK, S/Nº - PARQUE MATARUNA, ARARUAMA - RJ | 28970-000 | | 50 Mbps | CECIERJ |
| TRAVESSA JOÃO JOSÉ DE ANDRADE, 23 - PRAINHA, ARRAIAL DO CABO - RJ | 28930-000 | | 50 Mbps | CECIERJ |
| RUA SILVA CARDOSO, 349, BANGU, RIO DE JANEIRO - RJ | 21810-031 | | 50 Mbps | CECIERJ |
| RUA ROBERT LANG, 162 V. BARBARÁ, BARRA MANSA - RJ | 27330-360 | | 50 Mbps | CECIERJ |
| RUA MANOEL VIEIRA DE AGUIAR, S/Nº - SÃO MIGUEL, BOM JARDIM - RJ | 28660-000 | | 50 Mbps | CECIERJ |
| AVENIDA GOVERNADOR ROBERTO SILVEIRA, 578 - ANEXO, SANTA RITA, BOM JESUS DO ITABAPOANA - RJ | 28360-000 | | 50 Mbps | CECIERJ |
| AV. ANTONIO PERAZZO, 294 - 1 ANDAR - CENTRO (INDEPENDENTE DO REGULAR), CAMBUCI - RJ | 28430-000 | | 50 Mbps | CECIERJ |
| PÇA DA REPÚBLICA, 8, CENTRO, CAMPOS DOS GOYTACAZES - RJ | 28010-080 | | 50 Mbps | CECIERJ |
| RUA SENADOR DANTAS, 280, CARMO - RJ | 28640-000 | | 50 Mbps | CECIERJ |
| RUA FRANKLIN JOSÉ DOS SANTOS (ANTIGA RUA GUARUS) S/N°, CENTRO, CASIMIRO DE ABREU - RJ | 28860-000 | | 50 Mbps | CECIERJ |
| RUA BELFORD ROXO, 433, COPACABANA - RIO DE JANEIRO - RJ | 22020-010 | | 50 Mbps | CECIERJ |
| RUA RUA ADIR PINTO VAHIA DE ABREU, 216, CORDEIRO - RJ | 28540-000 | | 50 Mbps | CECIERJ |
| AV. GETÚLIO VARGAS, 104, CENTRO, DUAS BARRAS - RJ | 28650-000 | | 50 Mbps | CECIERJ |
| RUA BENTO DO AMARAL, S/Nº, CENTRO, DUQUE DE CAXIAS - RJ | 25020-020 | | 50 Mbps | CECIERJ |
| ESTRADA RJ 127, S/Nº, RAMALHO, ENGENHEIRO PAULO DE FRONTIN - RJ | 26650-000 | | 50 Mbps | CECIERJ |
| RUA SARGENTO JOÃO LOPES, 315 – ANEXO – JARDIM CARIOCA – RJ | 21931-420 | | 50 Mbps | CECIERJ |
| RUA EDNA SALLES, S/N°, VILA GABRIELA, ITABORAÍ, RJ | 24856-004 | | 50 Mbps | CECIERJ |
| R. ELVIRA CIUFO SICARINO, S/Nº VILA MARGARIDA - CENTRO, ITAGUAÍ - RJ | 23821-135 | | 50 Mbps | CECIERJ |
| RUA MARIA DE SOUZA MONTEIRO, 91 - SOBRADINHO, ITAOCARA - RJ | 28570-000 | | 50 Mbps | CECIERJ |
| RUA EXPEDICIONÁRIO CABO GAMA, 233, CIDADE NOVA, ITAPERUNA - RJ | 28300-000 | | 50 Mbps | CECIERJ |
| AVENIDA AGENOR CALDAS, Nº 442, IMBETIBA, MACAÉ - RJ | 27913-300 | | 50 Mbps | CECIERJ |

| | | | | |
|---|---|---|---|---|
| AV. MINISTRO EDGARD ROMERO, 491 - MADUREIRA, RIO DE JANEIRO - RJ | 21360-201 | | 50 Mbps | CECIERJ |
| RUA PREFEITO ULLMAN, 326, CENTRO, MAGÉ | 25900-046 | | 50 Mbps | CECIERJ |
| R GUARANI, S/N - PIABETÁ. (EM FRENTE AO SHOP 15) - LOJA. ENTRAR POR TRÁS DA ESCOLA, MAGÉ - RJ | 25915-000 | | 50 Mbps | CECIERJ |
| AV. ROBERTO SILVEIRA, 259 - CENTRO - MARICÁ - RJ | 24900-000 | | 50 Mbps | CECIERJ |
| RUA PAULO, S/Nº - MESQUITA - RJ | 26551-240 | | 50 Mbps | CECIERJ |
| RUA MATOSO MAIA, 316, MIRACEMA - RJ | 28460-000 | | 50 Mbps | CECIERJ |
| RUA MAURO ALVES RIBEIRO, NO 243 - ANEXO AO C. E. FLÁVIO RIBEIRO DE REZENDE, NATIVIDADE - RJ | 28380-000 | | 50 Mbps | CECIERJ |
| AV. ERNANI DO AMARAL PEIXOTO, 707, CENTRO, NITERÓI - RJ | 24030-170 | | 50 Mbps | CECIERJ |
| PRAÇA DEMERVAL BARBOSA MOREIRA, 15 - FUNDOS, NOVA FRIBURGO - RJ | 28610-160 | | 50 Mbps | CECIERJ |
| ESTRADA SANTA EUGÊNIA S/N, PACIÊNCIA, RIO DE JANEIRO - RJ - 23585-430 - CIEP - BRIZOLÃO 311 DEPUTADO BOCAYUVA CUNHA | | | 50 Mbps | CECIERJ |
| R. MARECHAL DEODORO, S/N - CENTRO - PARATY/RJ | 23970-000 | | 50 Mbps | CECIERJ |
| AV. BRASIL, 10.592 - PENHA, RIO DE JANEIRO - RJ | 21012-350 | | 50 Mbps | CECIERJ |
| AV. IPIRANGA, 494, CENTRO, PETRÓPOLIS - RJ | 25610-150 | | 50 Mbps | CECIERJ |
| RUA DEP. LUIZ FERNANDES LINHARES, 795, ANEXO, PORCIÚNCULA - RJ | 28390-000 | | 50 Mbps | CECIERJ |
| AV. DOZE DE JUNHO 1.265, QUISSAMÃ - RJ | 28735-000 | | 50 Mbps | CECIERJ |
| AV TENENTE CEL ADALBERTO MENDES 1920, SANTA ISABEL, RESENDE - RJ | 27522-240 | | 50 Mbps | CECIERJ |
| RUA LENI PEREIRA MELO 55, BALNEÁRIO REMANSO, RIO DAS OSTRAS - RJ | 28893-099 | | 50 Mbps | CECIERJ |
| RUA JOSÉ DE ALENCAR LEITE, 89 - FUNDOS, SANTO ANTÔNIO DE PÁDUA - RJ | 28470-000 | | 50 Mbps | CECIERJ |
| PÇ. ARGENTINA, 20 – FUNDOS – SÃO CRISTÓVÃO – RJ, RIO DE JANEIRO - RJ | 20920-050 | | 50 Mbps | CECIERJ |
| AV. GOV. ROBERTO SILVEIRA, 237, BARÃO DE MACAÚBA, São Fidélis - RJ | 28400-000 | | 50 Mbps | CECIERJ |
| AVENIDA LUCIO TOME FETEIRA S/N°, VILA LAGE, SÃO GONÇALO - RJ | 24415-000 | | 50 Mbps | CECIERJ |
| RUA DOZE DE OUTUBRO, S/N - BAIRRO ESTAÇÃO - SÃO PEDRO DA ALDEIA - RJ | 28941-192 | | 50 Mbps | CECIERJ |
| AV. PAULINO FERNANDES SILVA, 252 - JAMAPARÁ, SAPUCAIA - RJ | 25887-000 | | 50 Mbps | CECIERJ |
| ANTIGA RODOVIA RIO SAO PAULO KM 40, S/N, BAIRRO DOM BOSCO. SEROPÉDICA - RJ | 23890-000 | | 50 Mbps | CECIERJ |
| RUA DA CONCEIÇÃO, 45 - CENTRO, SUMIDOURO - RJ | 28637-000 | | 50 Mbps | CECIERJ |
| AVENIDA LUCIO MEIRA 311 - FUNDOS, VARZEA, TERESÓPOLIS - RJ | 25953-001 | | 50 Mbps | CECIERJ |
| R. IGLESIAS LOPES, 870 CANTAGALO, TRÊS RIOS -RJ | 25806-040 | | 50 Mbps | CECIERJ |
| AV. PASTEUR, 368, URCA, RIO DE JANEIRO - RJ | 22290-240 | | 50 Mbps | CECIERJ |
| RUA COMEN. ARAÚJO LEITE, 265 - CENTRO, | 27600-000 | | 50 Mbps | CECIERJ |

| | | | | |
|---|---|---|---|---|
| VALENÇA - RJ | | | | |
| AVENIDA MARECHAL PAULO TORRES 551, CENTRO, VASSOURAS - RJ | 27700-000 | | 50 Mbps | CECIERJ |
| AV. BOULEVARD VINTE E OITO DE SETEMBRO, Nº 109- ANEXO – VILA ISABEL, RIO DE JANEIRO - RJ | 20551-030 | | 50 Mbps | CECIERJ |
| RUA DUZENTOS E VINTE DOIS, 122, CONFORTO, VOLTA REDONDA - RJ | 27265-050 | | 50 Mbps | CECIERJ |
| RUA ALBERTO TORRES, Nº 15, CENTRO, MENDES – RJ | | | 5 Mbps | CODERTE |
| PRAÇA JUIZ MACHADO JÚNIOR, Nº 10, CENTRO, VASSOURAS – RJ | | | 5 Mbps | CODERTE |
| AVENIDA CONDESSA DO RIO NOVO, S/Nº, CENTRO, TRÊS RIOS – RJ | | | 5 Mbps | CODERTE |
| AVENIDA ZULAMITH BITTENCOURT, Nº 639, CIDADE NOVA, ITAPERUNA – RJ | | | 5 Mbps | CODERTE |
| AVENIDA JÚLIA KUBITSCHEK, S/Nº, CENTRO, CABO FRIO – RJ | | | 5 Mbps | CODERTE |
| RUA FRANCISCO PORTELA, S/Nº, CENTRO, MACAÉ – RJ | | | 5 Mbps | CODERTE |
| RUA SETE DE SETEMBRO, 170 | | | 5 Mbps | LOTERJ |
| PRAÇA FLORIANO S/N - CENTRO | | | 15 Mbps | FTM |
| AVENIDA ALMIRANTE BARROSO 14/16 - 5º ANDAR - CENTRO | | | 15 Mbps | FTM |
| AV. MINISTRO MAVIGNER 376 - INHAÚMA | | | 15 Mbps | FTM |
| AV RODRIGUES ALVES 303 A 331 - SANTO CRISTO | | | 15 Mbps | FTM |
| PRAÇA FLORIANO S/N - CENTRO | | | 15 Mbps | FTM |
| AVENIDA ALMIRANTE BARROSO 14/16 - 5º ANDAR - CENTRO | | | 15 Mbps | FTM |
| AV. MINISTRO MAVIGNER 376 - INHAÚMA | | | 15 Mbps | FTM |
| AV RODRIGUES ALVES 303 A 331 - SANTO CRISTO | | | 15 Mbps | FTM |
| PRAÇA FLORIANO S/N - CENTRO | | | 15 Mbps | FTM |
| AVENIDA ALMIRANTE BARROSO 14/16 - 5º ANDAR - CENTRO | | | 15 Mbps | FTM |
| AV. MINISTRO MAVIGNER 376 - INHAÚMA | | | 15 Mbps | FTM |
| AV RODRIGUES ALVES 303 A 331 - SANTO CRISTO | | | 15 Mbps | FTM |
| AVENIDA ALMIRANTE BARROSO 14/16 - 5º ANDAR - CENTRO | | | 15 Mbps | FTM |
| AV. MINISTRO MAVIGNER 376 - INHAÚMA | | | 15 Mbps | FTM |
| AV RODRIGUES ALVES 303 A 331 - SANTO CRISTO | | | 15 Mbps | FTM |
| ROD PINHEIRO MACHADO 0 - Ref: PRODERJ - LARANJEIRAS - RIO DE JANEIRO | 22231090 | -22.9370318, -43.1837417 | 50 Mbps | SUBSEC MILITAR |
| ILHA DE BROCOIÓ - PAQUETÁ, RIO DE JANEIRO - RJ | | | 25 Mbps | SUBSEC MILITAR |
| ROD PINHEIRO MACHADO 0 - Ref: PRODERJ - LARANJEIRAS - RIO DE JANEIRO | 22231090 | -22.9370318, -43.1837417 | 25 Mbps | SUBSEC MILITAR |
| RUA URUGUAIANA 118 - CENTRO - RIO DE JANEIRO | 20050092 | | 25 Mbps | SETUR |
| RUA URUGUAIANA 118 - CENTRO - RIO DE JANEIRO | 20050092 | | 25 Mbps | SETUR |

| | | | | |
|---|---|---|---|---|
| RUA BUENOS AIRES 309, CENTRO, RIO DE JANEIRO, RJ | | | 25 Mbps | SETUR |
| RUA BUENOS AIRES 309, CENTRO, RIO DE JANEIRO, RJ | | | 25 Mbps | SETUR |
| TERMINAL RODOVIÁRIO DE NOVA IGUAÇU - CEP | 26220-060; | | 5 Mbps | DETRO |
| AV. DOS TRABALHADORES, 333 – TERMINAL RODOVIÁRIO DE VOLTA REDONDA - CEP | 27255-125; | | 5 Mbps | DETRO |
| AV. JULIA KUBITSCHEK, TERMINAL RODOVIÁRIO DE CABO FRIO - PARQUE RIVIERA - CEP | 28907-270; | | 5 Mbps | DETRO |
| AV. DR. NILO PEÇANHA, 614, LJ. 20 – PARQUE RODOVIÁRIO, CAMPOS - CEP | 28030-035; | | 5 Mbps | DETRO |
| TERMINAL ROD. JOÃO PAULO II – AV. PRESIDENTE DUTRA, 646 – CIDADE NOVA, ITAPERUNA - CEP | 28300-000; | | 5 Mbps | DETRO |
| PRAÇA DR. FELICIANO COSTA, 01 – DUAS PEDRAS, NOVA FRIBURGO - CEP | 28633-010; | | 5 Mbps | DETRO |
| RUA DR. WALDIR BARBOSA MOREIRA, 170 – RODOVIÁRIA, TERESÓPOLIS - CEP | 25955-010; | | 5 Mbps | DETRO |
| AV. VINTE E DOIS DE MAIO, S/N - VENDA DAS PEDRAS, ITABORAÍ – RJ - CEP | 24804-781 | | 5 Mbps | DETRO |
| AV. FRANCISCO BICALHO, 1 TERMINAL RODOVIÁRIO NOVO RIO – SANTO CRISTO - CEP | 20220-310; | | 10 Mbps | DETRO |
| PRAÇA FONSECA RAMOS, TERMINAL RODOVIÁRIO ROBERTO SILVEIRA – CENTRO, NITERÓI - CEP | 24030-020 | | 10 Mbps | DETRO |
| COMPLEXO ESPORTIVO CAIO MARTINS, SITUADO NA RUA PRESIDENTE BACKER, S/Nº, PORTÃO 18, ICARAÍ, NITERÓI – RJ | | | 10 Mbps | SUDERJ |
| COMPLEXO ESPORTIVO DA ROCINHA, SITUADO NA RUA BERTA LUTZ, Nº 82, SÃO CONRADO, RIO DE JANEIRO – RJ | | | 10 Mbps | SUDERJ |
| COMPLEXO ESPORTIVO DO SAMPAIO, SITUADO NA RUA ANTUNES GARCIA, S/Nº, ESQUINA COM AVENIDA MARECHAL RONDON, SAMPAIO, RIO DE JANEIRO – RJ | | | 10 Mbps | SUDERJ |
| ESTÁDIO DE ATLETISMO CÉLIO DE BARROS, RUA PROFESSOR EURICO RABELO S/Nº, MARACANÃ, RIO DE JANEIRO RJ | | | 10 Mbps | SUDERJ |
| PARQUE AQUÁTICO JULIO DELAMARE, AV. MARACANÃ S/Nº, MARACANÃ, RIO DE JANEIRO RJ | | | 10 Mbps | SUDERJ |
| CENTRO DE REFERENCIA DA JUVENTUDE ALEMÃO ESTRADA DO ITARARÉ, Nº 690 – ALEMÃO – RIO DE JANEIRO | | | 10 Mbps | SUDERJ |
| CENTRO DE REFERENCIA DA JUVENTUDE CANTAGALO RUA ALBERTO DE CAMPOS, Nº 12- A – IPANEMA – RIO DE JANEIRO | | | 10 Mbps | SUDERJ |
| CENTRO DE REFERENCIA DA JUVENTUDE CIDADE DE DEUS AVENIDA JOSÉ DE ARIMATÉIA, Nº 80 – CIDADE DE DEUS – RIO DE JANEIRO | | | 10 Mbps | SUDERJ |
| CENTRO DE REFERENCIA DA JUVENTUDE | | | 10 Mbps | SUDERJ |

| | | | | |
|---|---|---|---|---|
| FUMACÊ RUA JOSÉ SALI, Nº 5 – FUMACÊ – RIO DE JANEIRO | | | | |
| CENTRO DE REFERENCIA DA JUVENTUDE MANGUINHOS AVENIDA DOM HELDER CÂMARA, Nº 1.184 – MANGUINHOS – RIO DE JANEIRO | | | 10 Mbps | SUDERJ |
| CENTRO DE REFERENCIA DA JUVENTUDE VILA PACIÊNCIA, RUA SÃO GOMÁRIO, S/Nº – VILA PACIÊNCIA – RIO DE JANEIRO | | | 10 Mbps | SUDERJ |

Rio de Janeiro, 23 novembro de 2020

Documento assinado eletronicamente por **Daniel Luzente de Lima**, **Gerente**, em 05/01/2021, às 12:14, conforme horário oficial de Brasília, com fundamento nos art. 21º e 22º do Decreto nº 46.730, de 9 de agosto de 2019.

Documento assinado eletronicamente por **Elio Thomé de Souza Filho**, **Analista de Sistemas**, em 05/01/2021, às 12:17, conforme horário oficial de Brasília, com fundamento nos art. 21º e 22º do Decreto nº 46.730, de 9 de agosto de 2019.

A autenticidade deste documento pode ser conferida no site http://sei.fazenda.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **12098702** e o código CRC **91404FDF**.

**Referência:** Processo nº E-04/171/221/2018 SEI nº 10651634

Rua da Conceição, 69, 24º Andar / 25º Andar - Bairro Centro, Rio de Janeiro/RJ, CEP 20051-011
Telefone:

Governo do Estado do Rio de Janeiro

Centro de Tecnologia da Informação e Comunicação do Estado do Rio de Janeiro

Vice Presidência de Tecnologia

# ENCARTE TÉCNICO I

# REDE IP GOVERNO

## 1. INTRODUÇÃO

Este documento complementa o Termo de Referência no que se refere à Rede IP Governo, que será uma rede corporativa WAN IP MPLS ou uma Rede SD-WAN, ou ainda uma rede hibrida MPLS/SD-WAN a ser contratada através do PRODERJ para interligação da Rede IP Governo com as Secretarias e Órgãos estaduais.

1.1. Este Encarte Técnico complementa o Termo de Referência, constituindo a documentação necessária e obrigatória à contratação da atualização da Rede IP Governo;

1.2. O objeto desta contratação visa viabilizar a interligação das redes locais das Secretarias e Órgãos Estaduais em todos os Municípios do Estado do Rio de Janeiro, e a Representação do Governo em Brasília, de forma a prover transmissão de dados, voz e imagem entre essas redes geograficamente dispersas, com utilização da tecnologia VPN IP MPLS ou SD-WAN. Ambas as tecnologias permitem a configuração de parâmetros de QoS (Qualidade do Serviço), priorização de tipos pré-definidos de tráfego e segurança na transferência de informações, de forma que os serviços e sistemas disponibilizados no Datacenter da Rede IP Governo, mantido e gerenciado pelo PRODERJ, (correio eletrônico, sistemas, Portal do Governo do Estado, videoconferência, dentre outros) estejam acessíveis em tempo real e integral pelas unidades regionais. No caso do fornecimento de uma Rede SD-WAN, sendo o MPLS uma das tecnologias de transporte utilizada, a solução deverá atender os requisitos exigidos para a Rede SD-WAN.

1.3. A contratação contempla também a instalação, configuração de equipamentos e enlaces de comunicação, e o gerenciamento proativo contra falhas e incidentes de segurança cibernética;

1.4. Nesse documento, utiliza-se o termo **sítio** como referência as unidades descentralizadas e a sede do Datacenter da Rede IP Governo, a serem contempladas na rede VPN IP MPLS ou SD-WAN.

## 2. CONCEITOS

### 2.1. Rede MPLS:

2.1.1. No contexto das redes de computadores e telecomunicações, o protocolo MPLS é definido pelo IETF (Internet Engineering Task Force) e consiste em uma tecnologia de chaveamento de pacotes que proporciona o encaminhamento e a comutação eficientes de fluxos de tráfego através da rede, apresentando-se como uma solução para interligar com maior eficiência redes de tecnologias distintas;

2.1.2. O protocolo MPLS disponibiliza os serviços de:

- QoS (Quality of Service): priorização de aplicações críticas, dando um tratamento diferenciado para o tráfego entre os diferentes pontos da VPN. O QoS cria as condições necessárias para o melhor uso dos recursos da rede, permitindo também o tráfego de voz e vídeo;
- VPN para uma rede baseada em IPV4/IPV6: criação de Redes Virtuais Privadas garantindo um isolamento completo do tráfego com a criação de tabelas de "labels" (usadas para roteamento) exclusivas de cada VPN.

2.1.3. A tecnologia MPLS foi concebida para satisfazer as necessidades de infraestrutura de comunicação segura e economicamente viável entre escritórios de uma mesma instituição em diferentes localidades, e entre os recursos pode-se citar:

- Acesso corporativo a servidores de aplicações centralizadas como sistemas corporativos, e-mail e intranet;
- Formação de redes para compartilhamento de arquivos;
- Integração de sistemas de telefonia;
- Formação de sistemas de videoconferência;
- Gerenciamento de banda;

- Acesso remoto aos sistemas corporativos.

2.1.4. Entre as vantagens de uma Rede IP MPLS podemos citar:

- Melhor desempenho no encaminhamento de pacotes;
- Criação de caminhos (Label Switching Paths) entre os roteadores;
- Possibilidade de associar requisitos de QoS, baseados nos rótulos carregados pelos pacotes.

*Fonte Wikipedia (http://pt.wikipedia.org/wiki/MPLS)*

2.2. **Rede SD-WAN:**

2.2.1. Entende-se como tecnologia SD-WAN (Software-Defined WAN) a rede de área ampla definida por software que centraliza a gerência da rede WAN em uma console única, eliminando a necessidade de intervenções manuais em roteadores em localidades remotas, proporcionando visibilidade do tráfego, seleção de caminho dinâmico baseado em políticas de QoS, aplicação ou desempenho e utilização de túneis VPN para comunicação entre os sites remotos;

2.2.2. Total independência da tecnologia de transporte, permitindo a utilização de tecnologias como:

- MPLS;
- Rede Wireless, 3G/4G;
- Internet;
- Satélite;
- Links Ponto a Ponto

*Fonte Wikipedia (*https://en.wikipedia.org/wiki/SD-WAN)

3. **CONTEXTUALIZAÇÃO**

3.1. O PRODERJ – Centro de Tecnologia da Informação e Comunicação do Estado do Rio de Janeiro – autarquia vinculada à Secretaria de Estado da Casa Civil e Governança – é o órgão gestor de Tecnologia da Informação e Comunicação (TIC) do Governo do Estado, desempenhando o importante papel de propor diretrizes e orientações técnicas voltadas para o estabelecimento da política de TIC no âmbito da administração pública estadual;

3.2. Com o intuito de ampliar, garantir segurança e melhorar a qualidade dos serviços de comunicação de dados, o Governo do Estado do Rio de janeiro, através do PRODERJ deseja contratar serviços de Rede WAN para a interligação do Backbone da Rede IP Governo aos demais sítios das Secretarias e Órgãos Estaduais localizados nos municípios do Estado do Rio de Janeiro;

3.3. O objetivo da contratação é a disponibilização de uma rede que seja adequada para o tráfego dos dados das aplicações, e para o tráfego de voz e imagem. A rede deverá ser flexível e escalável, permitindo a acomodação instantânea do tráfego das unidades durante o período de vigência do contrato;

3.4. O Backbone da Rede IP Governo será o ponto central de internet dos sítios abrangidos pela rede VPN IP MPLS ou pela rede SD-WAN.

3.5. Justificativa para a necessidade da contratação:

3.5.1. O Governo do Estado do Rio de Janeiro necessita de uma rede de comunicação de alta velocidade com capacidade de prover dados, voz, vídeo e imagens para atender às necessidades do exercício da sua missão institucional proporcionando elevado padrão de qualidade, atendendo as necessidades de comunicação e acesso a novas tecnologias que possam suprir as demandas de infraestrutura tecnológica;

3.5.2. Conforme contextualizado nos itens acima, a Diretoria de Infraestrutura Tecnológica visualizou um modelo seguro, moderno e eficiente para interconexão entre as unidades descentralizadas e a sede. Trata-se da implantação de uma rede VPN IP MPLS ou de uma rede SD-WAN que deverá ser capaz de viabilizar a conexão com a Internet, feita a partir de um ponto Central, localizado no Backbone da Rede, onde as Secretarias e Órgãos Estaduais participantes serão os pontos de conexão dessa infraestrutura ao Backbone da Rede IP Governo;

3.5.3. Ademais, esclarece-se que com a evolução tecnológica, e aumento da demanda de serviços, com o passar do tempo, uma determinada velocidade de link pode não ser mais suficiente para suprir as necessidades da sede ou unidades. Sendo assim, as tabelas de velocidade de todos os serviços contratados preveem a possibilidade de mudança de patamares dos serviços contratados;

3.5.4. A necessidade da comunicação entre Órgãos do Governo do Estado do RJ, formando a topologia da rede corporativa (Rede IP Governo), o que permite disponibilizar sistemas e serviços para os componentes da Rede IP Governo, garantindo maior segurança por meio da redução nos riscos de vazamentos de informação, além de redução de custos com melhor uso da tecnologia.

3.5.5. A topologia da Rede IP Governo deve permitir que os dados trafegados sejam auditáveis, que haja detecção de incidentes e gargalos e capacidade de otimização de funcionamento. Esses requisitos contribuem para a atividade de resposta aos incidentes na Rede IP Governo;

3.5.6. Os pontos de atendimento da Rede IP Governo se distribuem por todo o território geográfico do Estado do Rio de Janeiro e, devido às diferenças na infraestrutura disponível ao longo dessa mesma área geográfica, a qualidade de serviço oferecida não será a mesma;

3.5.7. Os dados gerados pelo tráfego de conectividade, bem como dos incidentes de rede e de segurança da informação precisam ser armazenados de forma estruturada, e disponibilizados em forma de painéis de controle (dashboards), gráficos e relatórios, garantindo a formação de um histórico que permita análise quantitativa e qualitativa de um único circuito de dados ou de forma global de toda a rede corporativa.

3.5.8. Cada órgão do Estado deve ter a possibilidade de requisitar, ao longo do tempo, os enlaces que forem necessários para atender às suas demandas.

3.5.9. Há uma grande concentração geográfica de órgãos na região mais próxima à capital, aumentando o nível de serviço a ser prestados nos órgãos localizados nessa região, em comparação com órgãos que se encontram fora dela;

3.5.10. O PRODERJ tem como uma de suas missões institucionais, prevista em lei (4480/2004 – Art. 2o VI) "- planejar e coordenar a implantação de uma solução de rede multisserviço que suporte tráfego integrado de voz, dados e imagens, para as diversas demandas de comunicações, inclusive telefonia, no âmbito do governo estadual, com capilaridade e capacidade adequadas para evitar a duplicação de esforços na criação de sub-redes paralelas distintas";

3.5.11. Necessidade na redução de custos do custo da rede, aproveitando a evolução tecnológica das soluções computacionais e de telecomunicações e o fomento à participação do máximo de empresas que tenham reais condições de prestar os serviços sem perda na qualidade dos níveis mínimos exigidos.

## 4. ESPECIFICAÇÕES BÁSICAS DA REDE IP MPLS E SD-WAN

4.1. As Redes IP MPLS e/ou SD-WAN deverão permitir a criação de múltiplas redes virtuais (VRFs) ou túneis criptográficos/VPN; ;

4.2. O provedor que atenderá a demanda de formação da Rede IP Governo (Lote I) poderá subcontratar os meios de acesso à última milha, sem que isso implique em transferência de responsabilidade, que será exclusiva da CONTRATADA vencedora do certame;

4.3. Os Órgãos e Secretarias de governo poderão constituir cada um sua própria VRF, contudo a interligação destas redes com o Backbone da Rede IP Governo deverá seguir as orientações e estrutura estipulada pelo PRODERJ descritas neste documento, tendo como premissas a segurança e padronização da Rede IP Governo;

4.4. Os meios de acessos para conexão dos sites à rede, última milha, deverão dar-se preferencialmente através de fibra ótica e par metálico. Será permitida a utilização de enlaces de rede em tecnologias alternativas desde que obedecendo aos critérios de desempenho estabelecidos neste projeto, principalmente o especificado no item 22 e todos os seus subitens;

4.5. Os roteadores CPE (Customer Premises Equipment) deverão ser fornecidos pela CONTRATADA de acordo com os requisitos previstos neste documento e adequados as especificações e velocidades dos circuitos a serem contratados;

4.6. O hardware dos roteadores fornecidos (CPEs e Centrais) poderá ser único para suportar o funcionamento tanto na Rede IP MPLS como na Rede SD-WAN;

4.7. A infraestrutura de rede da CONTRATADA deverá ser redimensionada e ser capaz de suportar serviços adicionais que possam ser solicitados pelo PRODERJ, como expansão ou redução de banda mínima de acesso garantida, ou alteração do endereço de um novo sítio, ou mesmo adição de um novo sítio não contemplado na relação de sítios. Em todos os casos, a CONTRATADA deve manter os níveis de serviços de desempenho especificados;

4.8. O limite de atuação da CONTRATADA deverá ser a porta de rede local do roteador CPE;

4.9. A assessoria de TIC de cada Secretaria ou Órgão será responsável pelo fornecimento de cabo(s) de rede local certificado(s) no padrão RJ-45 para interligação do(s) roteador CPE com o switch (es) /firewall(s) de sua propriedade, os quais serão responsáveis pelo encaminhamento de pacotes e conexões aos ativos finais de comunicação;

4.10. A rede oferecida deve ser logicamente independente e isolada de qualquer outra rede, em especial do ambiente público da internet;

4.11. A rede deverá ser flexível e escalável, permitindo acomodação instantânea do tráfego dos sítios em todo momento durante o período de vigência do contrato, permitindo a adaptação tempestiva a eventuais aumentos ou diminuição de demanda por tráfego, ou necessidade de provimento de novos serviços;

4.12. A Rede IP Governo contratada deverá respeitar o plano de endereçamento das Redes Locais atuais, permitindo o roteamento entre as redes conectadas. Os detalhes de endereçamento deverão ser definidos em conjunto com CONTRATADA;

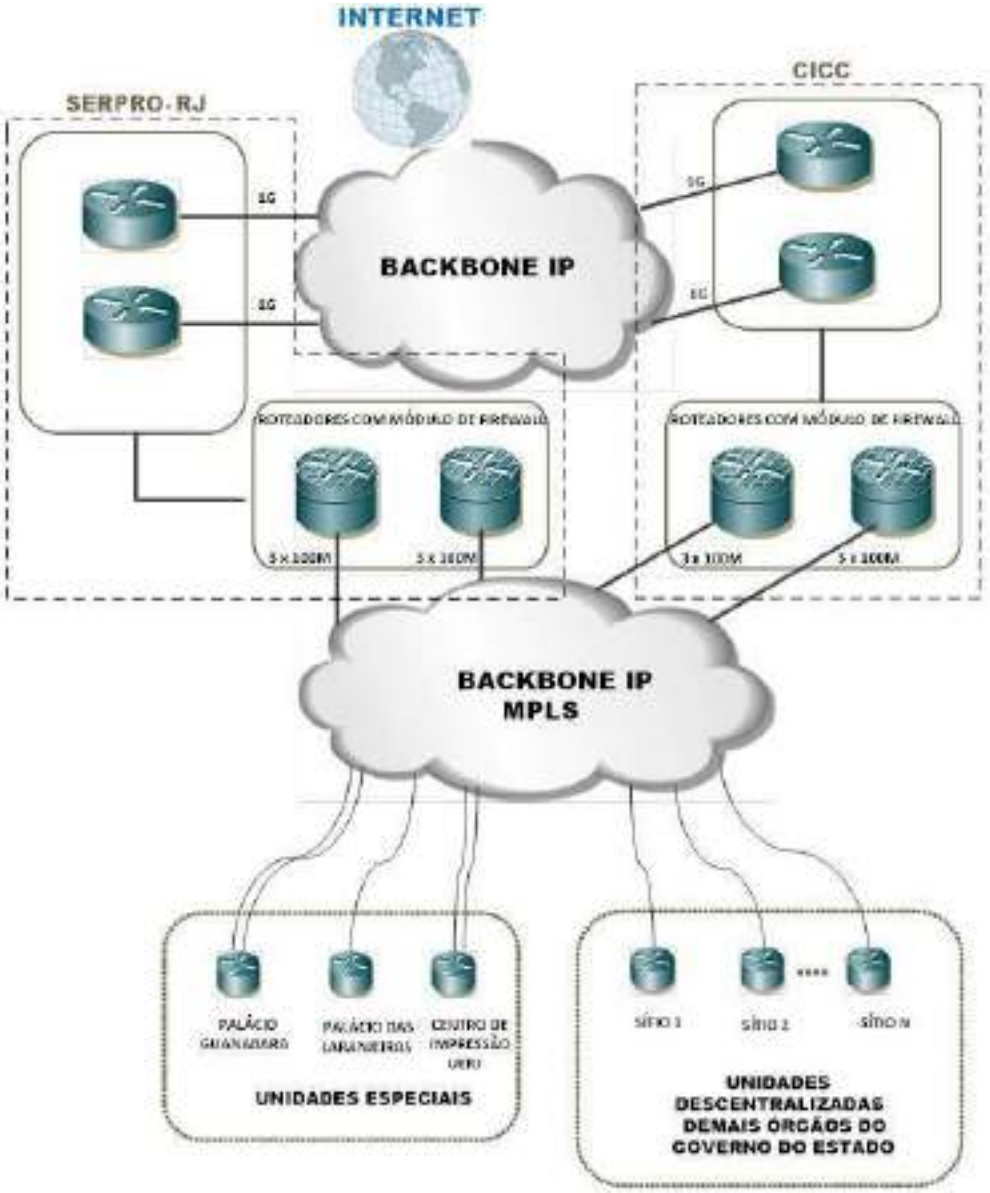
4.13. O uso da tecnologia IP MPLS ou SD-WAN deverá permitir que a rede se beneficie das vantagens da adoção desse padrão, tais como: configuração de recursos de qualidade de serviço (QoS), flexibilidade na definição de topologia lógica,

simplificação de roteamento, menor custo, implantação de parâmetros de segurança da informação, entre outros;

4.14. A Rede IP Governo a ser entregue deverá atender também aos seguintes requisitos:

- Ser de alta qualidade, disponibilidade e atualização tecnológica;
- Possibilitar o suporte à implantação de soluções de contingência e redundância;
- Suportar Qualidade de Serviço fim a fim, permitindo a priorização do tráfego de voz e videoconferência;
- Possuir Backbone IP com de tolerância a falhas em suas conexões, com baixos tempos de convergência em caso de falha de enlaces ou equipamentos;
- Possuir solução de segurança, embarcada no CPE ou em appliances próprios, desde que atendam aos requisitos do Termo de Referência e este Encarte Técnico;
- Seguir as melhores práticas de projeto e suporte e operação de redes.

4.15. A solução deverá ser ofertada prevendo o atendimento de várias VRFs independentes utilizando a tecnologia IP MPLS, sendo que o Core da Rede deverá atender as condições de contingência entre sites distintos, considerando como exemplo a topologia da rede conforme figura abaixo:




4.16. A topologia definida no item 4.14 será implementada sob demanda da CONTRATANTE, podendo ter suas características de velocidades, localidades e componentes físicos e lógicos alterados a qualquer tempo.

4.17. A latência máxima entre o roteador de acesso e o Backbone da CONTRATADA deve ser de 100ms.

## 5. DOS LOCAIS DE IMPLANTAÇÃO

5.1. Os endereços de instalação dos circuitos constantes foram levantados no momento da elaboração do Estudo Técnico, e pode haver alterações até a finalização do procedimento licitatório. Durante a implantação de cada circuito, a CONTRATADA deverá validar os endereços junto aos Órgãos e Secretarias do Governo com a anuência do PRODERJ;

5.2. Durante o decorrer da vigência do contrato de prestação poderá eventualmente haver mudança de endereços dos sites relacionados;

5.3. A CONTRATADA deverá se comprometer com o atendimento eventual de futuros sítios (unidades descentralizadas) e unidades especiais localizados no Estado do Rio de Janeiro durante a vigência do contrato, nas mesmas condições técnicas e de preço oferecidos para o objeto do edital, bem como expansão ou redução de bandas de comunicação, respeitados os limites legais e técnicos, bem como os prazos estipulados;

5.4. A CONTRATANTE poderá solicitar a desativação do serviço prestado de qualquer sítio ou, bem como mudança de local de prestação dos serviços ou mesmo adição de um novo sítio não contemplado na relação de sítios indicados, sem que isso enseje qualquer tipo de ônus a mesma. A CONTRATANTE deverá comunicar essas alterações em tempo hábil antes do início da prestação do serviço;

5.5. Eventuais mudanças de local de prestação dos serviços poderão ser solicitadas, durante a vigência do contrato. Entende-se por mudanças de local de prestação dos serviços a mudança de endereços de instalação dos equipamentos e acessos dentro da mesma localidade;

5.6. Os circuitos com velocidades acima de 100 Mbps serão utilizados apenas nos endereços já constantes no Anexo I e, para novas instalações, em localidades dentro da Região Metropolitana do Estado do RJ.

## 6. PROJETO EXECUTIVO DA REDE VPN IP MPLS OU SD-WAN

6.1. O Projeto Executivo deverá contemplar os seguintes itens:

- Definição de topologias físicas e lógicas da rede;
- Cronograma da implantação dos serviços;
- Os Esquemas de redundância para os enlaces necessários;
- O Plano de Roteamento;
- Os parâmetros de qualidade de serviço;
- Dimensionamento de enlaces e interfaces de comunicação;
- Plano de endereçamento compatível com a atual rede corporativa do Governo do Estado do Rio de Janeiro, associando endereços IPs privados de modo a torná-los únicos dentro da nuvem VPN IP MPLS ou SD-WAN;
- Cronograma de execução de obras civis de reponsabilidade da CONTRATADA, caso seja necessário;
- Definição do QoS e dos perfis de banda por Classe de Serviço.

## 7. DOS REQUISITOS DE INFRAESTRUTURA

7.1. Os equipamentos fornecidos pela contratada deverão ser capazes de operar com a alimentação elétrica de 110V ou 220V e frequência de 60Hz;

7.2. A CONTRATADA será responsável por fornecer, dimensionar, disponibilizar, instalar, configurar, monitorar, operar, gerenciar e manter os Equipamentos/recursos que forem necessários (roteadores, firewalls, UTMs, modems, estações de gerenciamento, meios de transmissão, cabeamento WAN, acessórios necessários, dentre outros) para o provimento dos serviços. Os Equipamentos serão de propriedade da CONTRATADA, que deverá ser responsável pelo suporte técnico dos mesmos;

7.3. A infraestrutura interna da rede da CONTRATADA (backbones, POPs, Equipamentos internos, dentre outros) deverá ser atendida por solução de alimentação e proteção elétrica de modo a manter todos os Equipamentos em operação por tempo indeterminado no caso de falta de energia;

7.4. A CONTRATADA será responsável pela interligação da rede entre o Distribuidor Geral (DG) de telefonia do prédio em cada um dos sítios e o local físico onde será instalado o roteador CPE para os acessos por rede cabeada;

7.5. Para o caso de atendimento do sítio por meio de rede não-cabeada, por exemplo, enlace de rádio frequência terrestre ou satélite, quando a implantação implique a necessidade de execução de obras civis, estas ficarão a cargo da CONTRATANTE, e deverão constar do cronograma que faz parte do Projeto Executivo. Nestes casos, a CONTRATADA apresentará relatório de visita contendo as adequações e providências necessárias para a conclusão da instalação dos circuitos.

## 8. REQUISITOS GERAIS DOS CPES

Os roteadores e equipamentos CPE, de propriedade da CONTRATADA, a serem disponibilizados em cada um dos endereços deverão satisfazer os seguintes requisitos:

8.1. Atenderem totalmente aos recursos solicitados, apresentando total compatibilidade e interoperabilidade, evitando-se problemas futuros na Rede do Governo;

8.2. Serem fornecidos com todos os componentes, módulos e acessórios necessários ao seu funcionamento atendendo aos requisitos deste documento;

8.3. Todos os roteadores CPE do Backbone PRODERJ, unidades especiais e dos sítios especificados deverão ser dimensionados, fornecidos, instalados, configurados, mantidos, gerenciados e operados de modo a garantir o desempenho e os níveis de serviços contratados;

8.4. Todos os roteadores CPE (Backbone PRODERJ, nas unidades especiais e dos sítios), devem ser dimensionados de forma que tenham capacidade de encaminhamento de pacotes IPV4/IPV6, em pacotes por segundo, compatíveis com as velocidades dos enlaces WAN conectados;

8.5. Todos os roteadores CPE (Backbone PRODERJ, nas unidades especiais e dos sítios), deverão ser dimensionados para operarem com utilização de CPU e memória de no máximo de 75% (setenta e cinco por cento), desde que satisfeita a condição de tráfego igual ou inferior à capacidade da soma dos enlaces WAN calculada a média de no mínimo 5 (cinco) minutos;

8.6. Caso seja identificado, durante a execução do contrato, um roteador com uso de CPU ou memória acima destes limites, este deverá ser substituído ou atualizado, sem ônus adicional para o Governo do Estado;

8.7. Todas as atualizações e correções (patches) de softwares, necessárias para o cumprimento dos requisitos exigidos neste documento técnico, deverão ser monitoradas e realizadas pela CONTRATADA sem ônus adicionais para o Governo do Estado, e comunicadas previamente, quando estas exigirem reinicialização de Equipamentos;

8.8. A CONTRATADA deverá aplicar atualização em prazo máximo de 10 dias após formalização pelo CONTRATANTE, considerando que deverá ser feito agendamento prévio em virtude da necessidade de janela de manutenção;

8.9. A CONTRATADA deverá garantir todos os roteadores atualizados desde o primeiro dia da vigência contratual, procedendo com no mínimo mais quatro atualizações em intervalo de 6 meses;

8.10. A CONTRATADA deverá habilitar nos roteadores CPE (Backbone PRODERJ, nas unidades especiais e dos sítios), o protocolo SNMP, disponibilizando nestes uma comunidade SNMP com acesso de leitura e permitir a solicitação de configuração de traps específicos pelo PRODERJ;

8.11. A configuração lógica dos roteadores CPE, para cada nível de serviço, será definida pela CONTRATADA com a aprovação do PRODERJ, e apresentada no Projeto Executivo;

8.12. Todos os equipamentos fornecidos pela CONTRATADA deverão suportar os protocolos IPV4 e IPV6;

8.13. Os roteadores fornecidos deverão contemplar todas as interfaces necessárias para o fornecimento dos circuitos por parte da CONTRATADA e com as especificações adequadas;

8.14. Todos os roteadores deverão possuir no mínimo uma interface LAN de 1G padrão Ethernet para a conexão da Rede Local dos endereços, sendo que devem satisfazer também as necessidades específicas em termos de desempenho e interfaces, como por exemplo: no caso da necessidade de balanceamento de dois circuitos em um mesmo roteador;

8.15. Para o caso do CPE conter solução de segurança embarcada, a mesma deverá atender a todos os requisitos especificados no Termo de Referência e este Encarte Técnico. Caso a solução de segurança embarcada não atenda aos requisitos, a CONTRATADA deverá prover solução de segurança apartada do CPE.

## 9. ESPECIFICAÇÃO DOS EQUIPAMENTOS CONCENTRADORES DO DATACENTER DO PRODERJ

### 9.1. ROTEADORES DATA CENTER PRODERJ

Os roteadores atualmente existentes poderão ser mantidos por um período de até 3 meses, quando então, deverão ser substituídos por equipamentos que contemplem as especificações detalhadas abaixo, e que estejam em conformidade com os requisitos especificados no **item 8 e todos os seus subitens**, em função da necessidade de atualização tecnológica da Rede IP Governo.

Deverão ser fornecidos pela CONTRATADA, sob demanda do PRODERJ, 2 (Dois) roteadores para serem os concentradores do Datacenter do PRODERJ em endereço a ser definido no momento da contratação, considerando aqueles que constam no item 2.8 do Termo de Referência (SERPRO ou CICC).

Estes equipamentos serão utilizados exclusivamente para o Núcleo da Rede IP Governo, situados nos Datacenters do PRODERJ.

9.1.1. Características de Hardware:

9.1.1.1. O atendimento deverá ser realizado com chassis único, não sendo permitida a utilização de um conjunto de equipamentos para atendimento da capacidade solicitada;

9.1.1.2. O equipamento deve permitir a instalação em gabinetes de 19 polegadas;

9.1.1.3. Deve possuir altura máxima de 2 (duas) unidades rack (2RU) / 88.9mm;

9.1.1.4. O equipamento deverá suportar fontes de alimentação AC ou DC;

9.1.1.5. O equipamento deve possuir no mínimo 2 (duas) fontes de energia internas, para Corrente Alternada (AC – Alternating Current), com chaveamento automático e capacidade de operação em 100V à 240V (50/60Hz), conforme abaixo:

- As fontes de energia devem permitir utilização de circuitos elétricos distintos;
- As fontes de energia devem ser do tipo substituível (hot-swap), permitindo instalação e/ou substituição sem a necessidade de remoção do equipamento;
- As fontes de energia devem ser suficientes para manter todas as operações do equipamento, mesmo no caso de falha de uma das fontes de energia, independentemente da quantidade de interfaces em uso ou funcionalidades habilitadas;
- As fontes de energia devem vir acompanhadas com cabos de energia com 1,80m (hum metro e oitenta centímetros) de comprimento mínimo;
- Os sistemas de fonte de alimentação devem ser o de maior capacidade oferecido pelo fabricante para o equipamento.

9.1.1.6. Deve possuir memória não-volátil com capacidade suficiente para armazenar, no mínimo, uma nova versão de sistema operacional que tenha o tamanho de 2 (duas) vezes o sistema operacional na versão mais recente, atendendo simultaneamente a todas as funcionalidades exigidas nesta Especificação, em conformidade com as recomendações do Fabricante;

9.1.1.7. Deve possuir configuração de CPU e memória RAM suficiente para a implementação de todas as funcionalidades descritas nesta especificação;

9.1.1.8. Deve possuir uma porta de console para o gerenciamento e configuração do equipamento, no padrão RS-232, com conector RJ-45 ou DB-9 ou uma porta de console com interface USB;

9.1.1.9. Deve operar entre as temperaturas de 0°C e 40ºC;

9.1.1.10. Deve ser destinado ao uso normal em ambiente tropical com umidade relativa na faixa de 10 a 90% (sem condensação);

9.1.1.11. Deve suportar temperatura ambiente de armazenamento entre -10ºC e 60ºC;

9.1.1.12. O sistema operacional / firmware dos equipamentos fornecidos deve, dentro das características solicitadas, ser a versão atual e estável no momento da instalação;

9.1.1.13. O equipamento deve implementar, no momento da entrega, todas as características exigidas nesta Especificação sem a necessidade de inclusão de nenhum componente, módulo ou dispositivo extras;

9.1.1.14. O equipamento deve implementar, no momento da entrega, todas as características exigidas nesta Especificação sem a necessidade de inclusão de nenhum componente, módulo ou dispositivo extras;

9.1.1.15. Deverá possuir modulo específico para criptografia, com capacidade mínima de 25 Gbps;

9.1.1.16. Deve possuir, no mínimo, 1 (uma) portas ethernet 1/100/1000 para gerenciamento;

9.1.1.17. Deve possuir pelo menos 8 (oito) interfaces Gigabit Ethernet com suporte a adaptadores padrão SFP;

9.1.1.18. Deve ser fornecido e configurado com, no mínimo, (4) quatro SFP padrão 1000BaseT (10/100/1000) e (4) quatro SFPs padrão 1000-BaseSX;

9.1.1.19. Deve possuir pelo menos 8 (oito) interfaces 10 Gigabit Ethernet com suporte a adaptadores padrão SFP+;

9.1.1.20. Deve ser fornecido e configurado com, no mínimo, (4) quatro SFP+ padrão 10GBaseSR;

9.1.1.21. Deve permitir a reinicialização de interfaces do equipamento sem afetar o funcionamento do mesmo;

9.1.1.22. Deve possuir LEDs de diagnóstico que forneçam informações de alimentação e atividade do equipamento;

9.1.1.23. Deve possuir LEDs de diagnósticos que forneçam informações e atividades das portas;

9.1.2. Funcionalidades Gerais:

9.1.2.1. Deve permitir a configuração em cada porta de um texto possibilitando ao administrador a inclusão de informações que identifiquem o que está conectado na respectiva porta;

9.1.2.2. Deve possuir suporte à tradução de endereços de rede (Network Address Translation – NAT) em conformidade com a RFC 1631 e RFC 3022;

9.1.2.3. Deve possuir suporte à tradução de endereços de porta (Port Address Translation – PAT);

9.1.2.4. Permitir a atualização remota do sistema operacional e arquivos de configuração utilizados no equipamento via interface Ethernet;

9.1.2.5. Deve implementar a opção local de carga do sistema do equipamento via memória Flash;

9.1.2.6. Permitir que a sua configuração seja feita através de terminal assíncrono;

9.1.2.7. Possuir ferramentas para depuração e gerenciamento em primeiro nível para IPv4 e IPv6, implementando ao menos, testes ICMP, debug, trace e log de eventos;

9.1.2.8. Suportar protocolo de coleta de informações de fluxos que circulam pelo equipamento contemplando no mínimo as seguintes informações: IP de origem/destino, Parâmetro "protocol type" do cabeçalho IP, Marcação de QoS, Portas TCP/UDP de origem/destino, interface de entrada do tráfego;

9.1.2.9. Deve ser possível especificar o uso de tal funcionalidade somente para tráfego de entrada, somente para tráfego de saída e também para ambos os sentidos simultaneamente, em cada uma das interfaces do equipamento;

9.1.2.10. A informação coletada deve ser automaticamente exportável em intervalos pré-definidos através de um protocolo IPFIX padronizado, para no mínimo: Net Flow ou Sflow ou JFlow ou Hflow ou Cflowd;

9.1.2.11. Deve suportar o envio de traps SNMP em função do resultado dos testes ultrapassarem limiares pré-configurados ou no caso de falha.

9.1.2.12. Deve suportar a implementação da funcionalidade de DHCP Relay e DHCP Server;

9.1.2.13. Deve possibilitar a configuração dinâmica de portas por software, permitindo a definição de portas ativas/inativas;

9.1.3. Funcionalidades Gerais - Rede MPLS:

9.1.3.1. Deve suportar o protocolo de tunelamento GRE (Generic Routing Encapsulation) em conformidade com o padrão RFC 2784, contemplando, no mínimo, os seguintes recursos:

- Permitir a associação do túnel GRE a uma tabela virtual de roteamento específica;
- Operação em modo multiponto ("multipoint GRE");
- Possibilidade de configuração de "Keepalive" nos túneis;
- Suporte a QoS – deve ser possível preservar as marcações no cabeçalho do pacote original para os pacotes transportados com encapsulamento GRE.

9.1.3.2. Deve permitir a criação de versões de configuração e suporte a "rollback" da configuração para versões anteriores;

9.1.3.3. Deve ter a capacidade de atualização de software via FTP e via TFTP, em conformidade com as RFCs 783 e 1350;

9.1.3.4. Deve permitir a transferência segura de arquivos para o equipamento através do protocolo SCP (Secure Copy) ou SFTP (Secure FTP);

9.1.3.5. Deve permitir a gravação de log externo (syslog). Deve ser possível definir o endereço IP de origem dos pacotes syslog gerados pelo equipamento;

9.1.3.6. Deve permitir consultas de DNS com resolução de nomes em endereços IPv6;

9.1.3.7. Deve implementar ICMPv6, em conformidade com a RFC 4443;

9.1.3.8. Suportar o espelhamento da totalidade do tráfego de uma porta, de um grupo de portas e de VLANs para um endereço IP. Deve ser possível definir o sentido do tráfego a ser espelhado: somente tráfego de entrada, somente tráfego de saída e ambos simultaneamente;

9.1.3.9. Permitir o espelhamento do tráfego total de uma porta e de um grupo de portas para outra porta localizada no mesmo equipamento;

9.1.3.10. Suportar mecanismo de extensão de Layer 2 sobre redes IP sem a necessidade de extensão do domínio Spanning-Tree entre sites diferentes e com a supressão de broadcast de ARP-requests sobre a rede IP de transporte. Este mecanismo não deverá necessitar de uma rede MPLS de transporte;

9.1.3.11. Deve responder a pacotes para teste da implementação dos níveis de serviço especificados (SLA). Deverão ser suportadas no mínimo as seguintes operações de teste: ICMP echo, estabelecimento de conexão TCP (em porta TCP configurável), UDP echo (em porta UDP configurável);

9.1.3.12. Deve suportar o envio de traps SNMP em função do resultado dos testes ultrapassarem limiares pré-configurados ou no caso de falha.

9.1.3.13. O equipamento deve suportar ao menos 2000 (dois mil) destas operações de testes simultaneamente;

9.1.3.14. Deve possibilitar a implementação de Lan Virtual (VLAN) por porta e compatíveis com o padrão IEEE 802.1Q e IEEE 802.1Q-in-Q;

9.1.3.15. Deve implementar, no mínimo, 4000 (quatro mil) VLANs simultaneamente;

9.1.3.16. Deve implementar o protocolo de controle de agregação de enlace (LACP) conforme o padrão IEEE 802.3ad, permitindo agrupar, no mínimo, 4 (quatro) interfaces do mesmo tipo;

9.1.3.17. Deve permitir o encaminhamento de “jumbo frames” (pacotes de 9016 bytes);

9.1.3.18. Deve implementar o protocolo VRRP (Virtual Router Redundancy Protocol), em conformidade com o padrão RFC 2338;

9.1.3.19. Deve suportar mecanismo de autenticação MD5 entre os peers VRRP;

9.1.3.20. Deve implementar, no mínimo, 100 grupos VRRP;

9.1.4. Roteamento

9.1.4.1. Deve suportar a pilha de protocolos TCP/IP;

9.1.4.2. Deve suportar o protocolo roteável IPv4;

9.1.4.3. Deve suportar o protocolo roteável IPv6;

9.1.4.4. Deve implementar o protocolo de roteamento RIPv2, em conformidade com, no mínimo, os padrões RFC 2453 e 2082;

9.1.4.5. Deve implementar o protocolo de roteamento OSPF, em conformidade com, no mínimo, os padrões RFC 2328, 3101, 3137, 3623, 2370 e 4750;

9.1.4.6. Deve implementar o protocolo de roteamento BGPv4, em conformidade com, no mínimo, os padrões RFC 1997, 2858, 2439, 2842, 2918, 4271, 3065, 4456, e 2385;

9.1.5. Roteamento – Rede MPLS

9.1.5.1. Deve implementar mecanismo de pilha dupla (IPv4 e IPv6), para permitir o funcionamento simultâneo dos protocolos IPv4 e IPv6

9.1.5.2. Deve permitir a configuração de rotas estáticas para IPv4 e IPv6;

9.1.5.3. Deve implementar mecanismo de controle de multicast conforme os protocolos: IGMPv1, IGMPv2 e IGMPv3. Deve implementar roteamento multicast PIM-SM (Protocol Independent Mode-Sparse Mode) e PIM-DM

9.1.5.4. (Protocol Independent Mode-Dense Mode), em conformidade com, no mínimo, os padrões RFC 1112, 1349, 1256, 2236, 3376 e 2362;

9.1.5.5. Deve suportar o protocolo MPLS (Tag Distribution Protocol, Label Distribution Protocol, MPLS Virtual Private Network, MPLS QoS, MPLS Traffic Engineering), em conformidade com, no mínimo, os padrões RFC 4364, 2702, 3031, 3443, 3036, 3037, 3107, 3215 e 3270;

9.1.5.6. Deve implementar roteamento dinâmico RIPng, em conformidade com o padrão RFC 2080;

9.1.5.7. Deve suportar roteamento dinâmico OSPFv3 para IPv6, em conformidade com o padrão RFC 5340;

9.1.5.8. Deve implementar Multiprotocol BGP (MP-BGP) com suporte a IPv6;

9.1.5.9. Deve permitir a virtualização das tabelas de roteamento (camada 3). As tabelas de roteamento virtuais deverão ser completamente segmentadas;

9.1.5.10. Deve suportar a criação de, no mínimo, 4000 tabelas de roteamento virtuais (VRF) p/ IPv4 e IPv6;

9.1.5.11. Deve implementar roteamento baseado em uma condição de origem, inclusive dentro das VRFs.

9.1.5.12. Deve permitir a possibilidade de alterações de roteamento automatizadas baseadas em métricas de desempenho dos enlaces, para no mínimo, perda de pacotes, atraso e jitter;

9.1.6. Segurança:

9.1.6.1. Deve implementar filtragem de pacotes (listas de controle de acesso) para IPv4 e IPv6;

9.1.6.2. Deve implementar listas de controle de acesso (ACLs), para filtragem de pacotes, baseadas em endereço IP de origem e destino, portas TCP e UDP de origem e destino;

9.1.6.3. Deve implementar mecanismos de AAA (Authentication, Authorization e Accounting) com garantia de entrega;

9.1.6.4. Deve implementar mecanismo de autenticação para acesso local ou remoto ao equipamento baseado em um servidor de autenticação e autorização do tipo TACACS+;

9.1.6.5. Deve suportar serviços de Virtual Private Network (VPN) baseados no padrão IPSec (IP Security Protocol), compatível com IPv4 e IPv6;

9.1.6.6. Deve suportar algoritmos de criptografia DES – 56 bits, 3DES – 168 bits, AES – 128 bits, AES – 256 bits para conexões de túneis VPN IPSec;

9.1.6.7. Suportar o tráfego do protocolo GRE sobre IPSec;

9.1.6.8. Deve suportar as funcionalidades de "Stateful Firewall", baseado em zonas de segurança, caso esta funcionalidade seja ativada através de licença de software, não existe a necessidade de fornece-la inicialmente.

9.1.7. Segurança - Rede MPLS:

9.1.7.1. Deve permitir a criação de listas de acesso baseadas em endereços IP para limitar o acesso ao equipamento via Telnet, SSH e SNMP;

9.1.7.2. Deve implementar a criptografia de todos os pacotes enviados ao servidor de controle de acesso e não só os pacotes referentes à senha;

9.1.7.3. Deve permitir controlar e auditar quais comandos os usuários e grupos de usuários podem emitir;

9.1.7.4. Deve suportar serviços de Virtual Private Network (VPN) baseados no padrão IKE (Internet Key Exchange);

9.1.7.5. Deve suportar, no mínimo, 2000 (dois mil) túneis VPN IPSec Site-to-Site;

9.1.7.6. Deve suportar uma taxa de estabelecimento de túneis VPN de no mínimo 30 (trinta) túneis por segundo;

9.1.7.7. Deve suportar a transparência de conexões IPSEC a NAT (NAT-T) através do encapsulamento dos pacotes IPSEC com UDP;

9.1.7.8. Deve reagrupar pacotes de sessão de VPN fragmentados para análise e entrega no destino;

9.1.7.9. Deve permitir a criação de VPNs IPSec baseada em politícas de segurança;

9.1.7.10. Devem ser implementados túneis VPN nos modos de operação “tunnel mode” e “transport mode”. Devem ser suportadas no mínimo as RFCs 1828, 1829, 2401, 2402, 2406, 2407, 2408 e 2409;

9.1.7.11. Deve suportar as funcionalidades de gerenciamento de chaves para VPN;

9.1.7.12. Deve suportar a utilização de clientes baseados em IPSec;

9.1.7.13. Suportar o tráfego Multicast IP sobre IPSec;

9.1.8. Gerenciamento:

1. 9.1.8.1. Deve implementar o protocolo NTPv3 (Network Time Protocol versão 3). Deve ser suportada autenticação entre os peers NTP, conforme definições da RFC 1305;
2. 9.1.8.2. Deve suportar o protocolo SNTP (Simple Network Time Protocol), em conformidade com o padrão RFC 4330 ou 5905;
3. 9.1.8.3. Deve suportar o protocolo de gerenciamento SNMP e MIB-II, em conformidade com os padrões RFCs 1157 e RFC 1213;
4. 9.1.8.4. Deve suportar os protocolo SNMPv2c e SNMPv3, incluindo a geração de traps;
5. 9.1.8.5. Implementar pelo menos os seguintes níveis de segurança para SNMP versão 3:
    - Sem autenticação e sem privacidade (no AuthNoPriv);
    - Com autenticação e sem privacidade (authNoPriv);
    - Com autenticação e com privacidade (authPriv) utilizando algoritmo de criptografia AES.

9.1.8.6. Suportar SNMP sobre IPv6;

9.1.8.7. Implementar MIB privativa que forneça informações relativas ao funcionamento do equipamento;

9.1.8.8. Possuir descrição completa da MIB implementada no equipamento, inclusive a extensão privativa;

9.1.8.9. Possibilitar a obtenção via SNMP de informações de capacidade e desempenho da CPU, memória e portas;

9.1.8.10. Deve permitir a configuração de endereços IPv6 para gerenciamento;

9.1.8.11. Deve proteger a interface de gerência do equipamento através de senha.

9.1.9. Gerenciamento – Rede MPLS:

9.1.9.1. Deve possuir suporte nativo, no mínimo, aos 2 (dois) grupos básicos de RMON, a saber: alarms e events, em conformidade com os padrões RFC 1757 ou 2819;

9.1.9.2. Possibilitar a obtenção da configuração do equipamento através do protocolo SNMP;

9.1.9.3. Deve permitir ser configurável e gerenciável via interface gráfica (GUI), linha de comando (CLI), SNMP, Telnet, SSH, HTTP e HTTPS com, no mínimo, 15 sessões simultâneas e independentes

9.1.9.4. Deve permitir a inserção de um certificado digital PKI para autenticação do protocolo SSH e Túneis IPSEC;

9.1.9.5. O equipamento deve suportar a configuração com um único endereço IP para gerência e administração, para uso dos protocolos: SNMP, NTP, HTTPS, SSH, TELNET, TACACS+ e RADIUS, provendo identificação gerencial única ao equipamento;

9.1.9.6. Deve proteger a interface de gerência do equipamento através de senha.

9.1.10. Desempenho:

9.1.10.1. Deve possuir backplane com capacidade de no mínimo 100 (cem) Gbps;

9.1.11. Desempenho – Rede MPLS:

9.1.11.1. Deve ser fornecido com capacidade licenciada de no mínimo 40 (quarenta) Gbps;

9.1.11.2. Deve garantir esta capacidade com no mínimo as funcionalidades de roteamento e NAT ativas simultaneamente;

9.1.11.3. Deve suportar uma taxa de comutação de pacotes de no mínimo 50 Mpps (cinquenta milhões de pacotes por segundo), considerando-se pacotes de 64 bytes;

9.1.12. Desempenho – Rede SD-WAN:

9.1.12.1. Deve ser fornecido com capacidade suficiente para suportar o tráfego criptografado sem prejuízo aos requisitos técnicos de disponibilidade e desempenho especificados neste documento;

9.1.13. Qualidade de serviço:

9.1.13.1. Deve suportar o padrão IEEE 802.1p para cada porta;

9.1.13.2. Deve possuir a facilidade de priorização de tráfego através do padrão IEEE 802.1p;

9.1.13.3. Deve possuir suporte a uma fila com prioridade estrita (prioridade absoluta em relação às demais classes dentro do limite de banda que lhe foi atribuído) para tratamento do tráfego "real-time" (voz e vídeo);

9.1.13.4. Deve suportar a classificação de pacotes de dados (QoS), baseados em:

- Protocolos da camada de rede (IPv4 e IPv6) do Modelo OSI (Endereços IP origem e destino);
- Protocolos da camada de transporte do Modelo OSI (TCP e UDP);

9.1.13.5. Deve suportar a classificação, marcação e remarcação baseadas em CoS ("Class of Service") para a camada de enlace;

9.1.13.6. Deve suportar a classificação, marcação e remarcação baseados em "DSCP" ("Differentiated Services Code Point");

9.1.13.7. Deve permitir a marcação de tráfego baseado no campo ToS (Type of Service), conforme RFC 2474;

9.1.13.8. Deve suportar funcionalidades de QoS de "Traffic Shaping";

9.1.13.9. Deve suportar funcionalidades de QoS de "Traffic Policing";

9.1.13.10. Deve possuir mecanismos de descarte de pacotes que evitem o congestionamento nas filas do equipamento, tais como RED (Random Early Detection) ou WRED (Weighted Random Early Detection);

9.1.13.11. Deve suportar o padrão IEEE 802.3x (Flow Control);

9.1.14. Qualidade de serviço – Rede MPLS:

9.1.14.1. Deve suportar a classificação de pacotes de dados (QoS), baseados em:

- Endereços MAC de origem e destino;
- VLAN.

9.1.14.2. Deve suportar a classificação, marcação e remarcação baseadas em CoS ("Class of Service") para a camada de enlace;

9.1.14.3. Deve suportar a classificação, marcação e remarcação baseados em "IP precedence";

9.1.14.4. Deve permitir a marcação de tráfego baseado no campo ToS (Type of Service), conforme RFC 2474;

9.1.14.5. Deve prover as funcionalidades de priorização de tráfego nas interfaces através da utilização de First In First Out (FIFO), Priority Queuing (PQ), Custom Queuing (CQ), Weighted Fair Queuing (WFQ), Class-Based Weighted Fair Queueing (CBWFQ) e Low Latency Queueing (LLQ);

9.1.14.6. Deve suportar QoS hierárquico no mínimo e níveis de hierarquia;

9.1.14.7. Suportar no mínimo duas filas Low Latency Queueing (LLQ) por policies;

9.1.14.8. Deve ser possível a especificação de garantia de banda por classe de serviço;

9.1.14.9. Para os pacotes que excederem a especificação, deve ser possível configurar ações, para no mínimo: transmissão do pacote sem modificação, transmissão com remarcação do valor de DSCP e descarte do pacote;

9.1.14.10. O equipamento deve suportar o mapeamento das prioridades nível 2 (802.1p) em prioridades nível 3 (IP Precedence e DSCP) e vice-versa;

9.1.14.11. Deve suportar a priorização do tráfego de rede, com no mínimo 10 (dez) filas por interface (processamento distribuído) ou 200.000 (duzentos mil) filas (processamento centralizado), permitindo uma integração transparente de dados, voz e vídeo;

9.1.14.12. Deve implementar RSVP (Resource Reservation Protocol) em conformidade com no mínimo, os padrões RFC 3209, RFC 2961, RFC 2747 e RFC 2205;

## 9.2. ESPECIFICAÇÃO DA SOLUÇÃO DE FIREWALL/IPS DO DATACENTER PRODERJ

Com o objetivo de permitir o controle das conexões dos distintos Órgãos e Unidades às aplicações sitiadas no PRODERJ, a CONTRATADA deverá prover solução de Firewall/IPS. A solução atual poderá ser mantida por um período de até 3 meses, quando então, deverá ser substituída por uma Solução de Firewall/IPS com as especificações a seguir.

9.2.1. Características Gerais:

9.2.1.1. Deve possuir licenciamento válido, pelo período do contrato todas as funcionalidades: Statefull Inspection Firewall, virtualização/contextos, IPS, NGFW, Aplication Control, AntiMalware, Filtro de URL, Análise de Arquivos, Licença de Cluster Ativo-Ativo ou Ativo-Passivo e qualquer outra funcionalidade de software suportada pelos equipamentos;

9.2.2. Características de Hardware Gerais:

9.2.2.1. Deve possuir pelo menos 4 (quatro) interfaces de 1 Gbps SFP com seus respectivos transceivers;

9.2.2.2. Deve ser fornecido e configurado com, no mínimo, 2 (duas) SFP padrão 1000BaseT (10/100/1000) e 2 (duas) SFPs padrão 1000-BaseSX;

9.2.2.3. Deve possuir pelo menos 4 (quatro) interfaces de 10 Gbps SFP com seus respectivos transceivers;

9.2.2.4. Deve ser fornecido e configurado com, no mínimo, (4) quatro SFP+ padrão 10GBaseSR

9.2.2.5. Deve possuir 1 (uma) interface de rede Gigabit dedicada para gerenciamento;

9.2.2.6. Deve possuir 1 (uma) interface do tipo console ou similar;

9.2.3. Características gerais:

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

9.2.3.2. As funcionalidades de proteção de rede que compõem a plataforma de segurança podem funcionar em múltiplos appliances, desde que obedeçam a todos os requisitos desta especificação;

9.2.3.3. Deverá ser possível acessar o equipamento para aplicar configurações durante momentos onde o trafego é muito alto e a CPU e memória do equipamento estiverem com alto nível de utilização, através de isolamento entre o processamento de gerenciamento e o processamento do tráfego inspecionado;

9.2.3.4. Na data da proposta, o modelo ofertado não podera estar listado em listas de end-of-life e end-of-sale;

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

9.2.3.6. O software deverá ser fornecido em sua versão mais recente ( versão recomendada pelo Fabricante) e atualizada;

9.2.3.7. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS);

9.2.3.8. Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:

- Suporte a 1024 VLAN Tags 802.1q;
- Agregação de links 802.3ad e LACP;
- Roteamento multicast (IGMPv1/v2, PIM-SM, Bidir-PIM);
- DHCP Relay;
- DHCP Server;
- Jumbo Frames;
- Suportar sub-interfaces ethernet lógicas;
- Deve suportar os seguintes tipos de NAT:
    - NAT dinâmico (Many-to-1);
    - NAT dinâmico (Many-to-Many);
    - NAT estático (1-to-1);
    - NAT estático (Many-to-Many);
    - NAT estático bidirecional 1-to-1;
    - Tradução de porta (PAT);
    - NAT de Origem;
    - NAT de Destino;
    - Suportar NAT de Origem e NAT de Destino simultaneamente;

- Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;
- NAT64 e NAT46;

9.2.3.9. Deve permitir monitorar via SNMP falhas de hardware, uso de recursos e estatísticas de uso das interfaces de rede;

9.2.3.10. Enviar log para sistemas de monitoração externos, simultaneamente;

9.2.3.11. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;

9.2.3.12. Proteção anti-spoofing;

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

9.2.3.14. Para IPv6, deve suportar roteamento estático e dinâmico;

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

9.2.3.16. Modo sniffer, para inspeção via porta espelhada do tráfego de dados da rede;

9.2.3.17. Modo camada 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;

9.2.3.18. Modo camada 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas;

9.2.3.19. Suporte a configuração de alta disponibilidade Ativo/Passivo ou Ativo/Ativo:

- Em modo transparente;
- Em layer 3;

9.2.3.20. Caso configurado em alta disponibilidade deve sincronizar:

- Sessões;
- Configurações, incluindo, mas não limitado às políticas de Firewall, NAT, QoS e objetos de rede;

9.2.3.21. O HA (modo de alta disponibilidade) deve possibilitar monitoração de falha de link;

9.2.3.22. A configuração em alta disponibilidade deve possibilitar a instalação de cada membro do cluster, de forma que o sincronismo de sessões e configurações deve ocorrer sobre a camada 3 (IP);

9.2.3.23. As características descritas deverão ser passíveis de comprovação por meio de documentação acessível no site do fabricante na Internet;

9.2.4. Controle por Política de Firewall:

9.2.4.1. Deve suportar controles por zona de segurança;

9.2.4.2. Deve suportar controles de políticas por porta e protocolo;

9.2.4.3. Deve suportar controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;

9.2.4.4. Deve suportar controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;

9.2.4.5. Deve suportar controle de políticas por país (geolocation);

9.2.4.6. Deve suportar controle, inspeção e decriptografia de SSL por política para tráfego de entrada (inbound) e Saída (outbound);

9.2.4.7. Deve suportar offload de certificado em inspeção de conexões SSL de entrada (inbound);

9.2.4.8. Deve decriptografar tráfego inbound e outbound em conexões negociadas com TLS 1.2;

9.2.4.9. Bloqueios dos seguintes tipos de arquivos: bat, cab, dll, exe, bin, zip, tar e mp3;

9.2.4.10. Suporte a objetos e regras IPV6;

9.2.4.11. Suporte a objetos e regras multicast;

9.2.4.12. Deve suportar no mínimo os seguintes tipos de negação de tráfego nas políticas de firewall: drop sem notificação do bloqueio ao usuário, drop com notificação do bloqueio ao usuário, TCP-Reset para o client, TCP-Reset para o server ou para ambos os lados da conexão;

9.2.4.13. Deve implementar filtragem de URL;

9.2.5. Controle de Aplicações:

9.2.5.1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independentemente de porta e protocolo, com as seguintes funcionalidades:

- Deve ser possível a liberação e bloqueio exclusivo de aplicações sem a necessidade de liberação de portas e protocolos;
- Deve reconhecer pelo menos 1.700 (hum mil e setecentas) aplicações diferentes, incluindo, mas não limitado a: tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;
- Deve reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, webex , google-docs;
- Deve inspecionar o payload de pacote de dados com o objetivo de detectar, através de expressões regulares, assinaturas de aplicações conhecidas pelo fabricante, independente de porta e protocolo;
- Para tráfego criptografado SSL, deve decriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
- Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde à especificação do protocolo, incluindo, mas não limitado a Yahoo Instant Messenger usando HTTP. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação, incluindo, mas não limitado a compartilhamento de arquivo dentro do Webex;
- Deve identificar o uso de táticas evasivas via comunicações criptografadas;
- Deve atualizar a base de assinaturas de aplicações automaticamente;
- Deve limitar a banda (download/upload) usada por aplicações (rate limiting) baseado no IP de origem, usuários e grupos do LDAP/AD;
- Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory (AD), com ou sem a necessidade de instalação de agente no Domain Controller nem nas estações dos usuários;
- Deve ser possível adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente à possibilidade de habilitar controle de aplicações em algumas regras;
- Deve suportar, no mínimo, os seguintes métodos de identificação e classificação das aplicações: checagem de assinaturas e decodificação de protocolos;
- Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;
- Deve permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do ambiente do CONTRATANTE;
- A criação de assinaturas personalizadas deve permitir o uso de expressões regulares e contexto (sessões ou transações), usando posição no payload dos pacotes TCP e UDP e usando decoders de, pelo menos, os seguintes protocolos: HTTP, FTP, NBSS, DCE RPC, SMTP, Telnet, SSH, MS-SQL, IMAP, DNS, LDAP, RTSP e SSL;
- O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
- Deve alertar o usuário quando uma aplicação for bloqueada;
- Deve possibilitar que o controle de portas seja aplicado para todas as aplicações;
- Deve possibilitar a diferenciação de tráfegos Peer2Peer (ex.: Bittorrent, emule, neonet), possuindo granularidade de controle/políticas para os mesmos;
- Deve possibilitar a diferenciação de tráfegos de Instant Messaging (ex.: AIM, Hangouts, Facebook Chat), possuindo granularidade de controle/políticas para os mesmos;
- Deve possibilitar a diferenciação e controle de partes das aplicações como, por exemplo, permitir o uso do chat e bloquear a chamada de vídeo.

9.2.6. Prevenção de Ameaças:

9.2.6.1. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS integrado ao appliance de Firewall;

9.2.6.2. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos;

9.2.6.3. Deve sincronizar as assinaturas de IPS quando implementado em alta disponibilidade ativo/ativo ou ativo/passivo;

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

9.2.6.5. Deve permitir ativar, desativar e habilitar apenas em modo de monitoração as assinaturas de prevenção contra invasão;

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

9.2.6.7. Deve suportar granularidade nas políticas de IPS, possibilitando a criação de diferentes politicas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens:

- Deve permitir o bloqueio de vulnerabilidades;
- Deve permitir o bloqueio de exploits conhecidos;
- Deve incluir proteção contra ataques de negação de serviços;
- Deve possuir os seguintes mecanismos de inspeção de IPS:
  - Análise de padrões de estado de conexões;
  - Análise de decodificação de protocolo;
  - Análise para detecção de anomalias de protocolo;
  - IP Defragmentation;
  - Remontagem de pacotes de TCP;
  - Bloqueio de pacotes malformados;
- Deve ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;
- Deve detectar e bloquear a origem de portscans;
- Deve bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões;
- Deve possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;
- Deve possuir assinaturas para bloqueio de ataques de buffer overflow;
- Deve possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;
- Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS e anti-spyware, permitindo a criação de exceções com granularidade nas configurações;
- Deve permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMTP e POP3;
- Deve suportar bloqueio de arquivos por tipo;
- Deve identificar e bloquear comunicação com botnets;
- Deve registrar na console de monitoração as seguintes informações sobre ameaças identificadas:
  - Nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
- Deve suportar a captura de pacotes (PCAP) por assinatura de IPS e controle de aplicação;
- Deve possuir a função de proteção à resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;
- Os eventos devem identificar o país de onde partiu a ameaça;
- Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;
- Deve oferecer proteção contra downloads involuntários usando HTTP de arquivos executáveis, maliciosos;
- De ve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseada em políticas do firewall considerando usuários, grupos de usuários, origem, destino, zonas de segurança, etc., ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por usuários, grupos de usuário, origem, destino e zonas de segurança;

9.2.7. Análise de Malware Moderno:

9.2.7.1. Devido ao malware, hoje em dia, ser muito dinâmico e um antivírus comum reativo não ser capaz de detectá-los com a mesma velocidade que suas variações são criadas, a solução ofertada deverá possuir funcionalidades para análise de malware não conhecido, incluídas na própria ferramenta ou entregues mediante composição com outro fabricante;

9.2.7.2. Deve suportar operação em ambientes configurados para alta disponibilidade;

9.2.7.3. O dispositivo de proteção deve ser capaz de enviar arquivos trafegados para análise "in Cloud" ou local, onde o arquivo será executado e simulado em ambiente controlado;

9.2.7.4. Deve permitir de forma automática a criação e manutenção de um histórico ou fluxo de trabalho forense no qual seja possível identificar:

- Capa cidade de inspeção de malware no ambiente de rede, mesmo quando não seja detectado inicialmente como malware, e movimento lateral;

9.2.7.5. Deve permitir selecionar, através de políticas granulares, quais tipos de arquivos sofrerão esta análise, incluindo, mas não limitado a: endereço IP de origem/destino, usuário/grupo do AD/LDAP, aplicação, porta, URL/categoria de URL de destino, tipo de arquivo e todas estas opções simultaneamente;

9.2.7.6. Deve suportar a monitoração, detecção e prevenção, em tempo real, de arquivos trafegados nos seguintes protocolos: FTP, HTTP, SMTP, IMAP, POP3, como também arquivos trafegados internamente entre servidores de arquivos usando SMB, em todos os modos de implementação: transparente e L3;

9.2.7.7. Deve permitir especificar o tipo de arquivo, inclusive os comprimidos, que serão analisados em cada política de controle de malware, permitindo especificar um contexto de análise para redes, VLANs e outros objetos associados ao controle de acesso do ambiente protegido;

9.2.7.8. Deve permitir que seja definido o tamanho máximo dos arquivos a serem inspecionados;

9.2.7.9. Deve utilizar mecanismo de proteção baseado em reputação global em tempo real, permitindo que sejam adotadas ações automáticas de alerta e bloqueio de arquivos suspeitos ou malware já encontrado anteriormente;

9.2.7.10. O dispositivo não deve depender ou utilizar de forma exclusiva mecanismos de análise em ambiente virtualizado para que seja feita a detecção e o bloqueio de malware em tempo real;

9.2.7.11. A utilização de recursos de execução virtualizada não deve depender da configuração manual de imagens ou escolha de versões específicas de sistemas operacionais;

9.2.7.12. Deve possui mecanismo blacklist para implementar controles customizados de forma automatizada;

9.2.7.13. Deve possui mecanismo whitelist para implementar controles customizados de forma automatizada;

9.2.7.14. Deve possui capacidade para detecção de malware em comunicações de entrada e saída, incluindo a detecção de mecanismos de Comando e Controle;

9.2.7.15. Deve identificar ataques como: ataques direcionados, zero day, exploração de vulnerabilidades, indicadores de ofuscação e indicadores de comprometimento automático;

9.2.7.16. Deve possuir tecnologia proprietária de execução para verificação de malware avançado, inclusive mecanismos tipo sandbox;

9.2.7.17. Deve implementar a identificação e capacidade de controle de acesso em tempo real nos seguintes tipos de arquivo: MSEXE, 9XHIVE, DMG, DMP, ISO, NTHIVE, PCAP, PGD, SYLKc, SYMANTEC, VMDK, DWG, IMG_PICT, MAYA, PSD, WMF, SCRENC, UUENCODED, PDF, EPS, AUTORUN, BINARY_DATA, BINHEX, EICAR, ELF, ISHIELD_MSI, MACHO, RPM, TORRENT, AMR, FFMPEG, FLAC, FLIC, FLV, IVR, MIDI, MKV, MOV, MPEG, OGG, PLS, R1M, REC, RIFF, RIFX, RMF, S3M, SAMI, SMIL, SWF, WAV, WEBM, 7Z, ARJ, BZ, CPIO_CRC, CPIO_NEWC, CPIO_ODC, JAR, LHA, MSCAB, MSSZDD, OLD_TAR, POSIX_TAR, RAR, SIS, SIT, ZIP, ZIP_ENC, ACCDB, HLP, MAIL, MDB, MDI, MNY, MSCHM, MSOLE2, MSWORD_MAC5, MWL, NEW_OFFICE, ONE, PST, RTF, TNEF, WAB, WP, WRI, XLW, XPS. Adicionalmente, deve implementar em tempo real a inspeção, detecção e bloqueio autônomo (prevenção sem a necessidade de integrar com sistemas de terceiros para que seja feito o bloqueio da ameaça) na rede para os seguintes tipos de arquivos: 7Z, ACCDB, ARJ, BINARY_DATA, BINHEX, BZ, CPIO_CRC, CPIO_NEWC, CPIO, ODC, EICAR, FLV, GZ, ISHIELD_MSI, JAR, JARPACK, LHA, MAIL, MDB, MDI, MNY, MSCAB, MSCHM, MSEXE, MSOLE2, MSWORD_MAC5, NEW_OFFICE, OLD_TAR, PDF, POSIX_TAR, PST, RAR, RTF, SIS, SIT, SWF, TNEF, WAB, WRI, XLW, XPS, ZIP, ZIP_ENC;

9.2.7.18. Deve implementar atualização a base de dados da rede de inteligência de forma automática;

9.2.7.19. Para recurso de análise virtualizada existente, deve ser mantido um histórico dos resultados de avaliações prévias de um arquivo e utilizar esta informação para determinar de forma configurável que o arquivo seja considerado malware a partir de certo limite;

9.2.7.20. Deve dispor de múltiplos motores e mecanismos de detecção e prevenção para verificação de malware e códigos maliciosos incluindo:

- Machine learning;
- Reputação global;
- Detecção customizada local por blacklist e regras customizadas de detecção de tráfego de rede;
- Análise dinâmica (sandbox);

9.2.7.21. O processo de análise de comunicações, malware e sua prevenção deve ocorrer em tempo real, não sendo aceitas tecnologias que dependam de verificações que induzam latência suficiente para postergar a entrega de arquivos ao seu destino original;

9.2.7.22. Deve permitir o download de malware identificado a partir da própria interface de gerência;

9.2.7.23. Caso sejam necessárias licenças de sistema operacional e software para execução de arquivos no ambiente controlado (sand-box), as mesmas devem ser fornecidas em sua totalidade, sem custos adicionais para o CONTRATANTE;

9.2.7.24. Deve suportar a análise de arquivos executáveis, DLLs e ZIP no ambiente controlado;

9.2.7.25. Deve suportar a análise de arquivos do pacote Microsoft Office (.doc, .docx, .xls, .xlsx, .ppt, .pptx) e arquivos java (.jar e .class);

9.2.7.26. Deve permitir o envio de arquivos para análise no ambiente controlado de forma automática;

9.2.8. Identificação de Usuários:

9.2.8.1. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Microsoft Active Directory e base de dados local;

9.2.8.2. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos, permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários;

9.2.8.3. Deve possuir integração e suporte a Microsoft Active Directory para o sistema operacional Microsoft Windows Server 2008 e versões superiores;

9.2.8.4. Deve possuir integração com LDAP para identificação de usuários e grupos, permitindo granularidade de controle/politicas baseadas em Usuários e Grupos de usuários;

9.2.8.5. Deve permitir o controle, sem instalação de software cliente, em equipamentos que solicitem saída para Internet, para que antes de iniciar a navegação, seja exibido um portal de autenticação hospedado no firewall (Captive Portal);

9.2.9. Filtro de Dados:

9.2.9.1. Deve permitir a criação de filtros para arquivos e dados pré-definidos;

9.2.9.2. Os arquivos devem ser identificados por extensão e assinaturas;

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

9.2.9.4. Deve suportar a identificação de arquivos compactados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

9.2.9.5. Deve suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

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

9.2.10. Geo-Localização:

9.2.10.1. Deve suportar a criação de políticas por geo-localização, permitindo que o tráfego de determinado pais/países sejam bloqueados;

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

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

9.2.11. VPN:

9.2.11.1. Deve suportar VPN Site-to-Site;

9.2.11.2. Deve suportar IPSec VPN;

9.2.11.3. A VPN IPSEc deve suportar:

- 3DES;
- Autenticação MD5 e SHA-1;
- Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;
- Algoritmo Internet Key Exchange (IKEv1 e v2);
- AES 128, 192 e 256 (Advanced Encryption Standard);
- Autenticação via certificado IKE PKI;

9.2.11.4. Deve permitir habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPSEc a partir da interface gráfica da solução, facilitando o processo de throubleshooting;

9.2.11.5. Deve suportar SSL ou IPSec para "remote access VPN";

9.2.11.6. Deve garantir uso de cliente VPN para dispositivos móveis (Android, IOS).

9.2.12. Características Técnicas Específicas do Firewall:

9.2.12.1. Características de hardware:

- Deve possuir capacidade de processamento de, no mínimo, 12 Gbps para tráfego stateful inspection multiprotocolo com a funcionalidade de firewall e controle de aplicações ativas simultaneamente, considerando-se para fins de métrica, ambientes de produção;
- Deve possuir capacidade de processamento de, no mínimo, 10 Gbps para tráfego stateful inspection multiprotocolo com a funcionalidade de firewall, controle de aplicações e IPS ativas simultaneamente, considerando-e para fins de métrica, ambientes de produção;
- Suporte a, no mínimo, 9.000.000 (nove milhões) de conexões simultâneas;
- Suporte a, no mínimo, 68.000 (sessenta e oito mil) novas conexões por segundo;
- Suportar throughput mínimo de 6 Gbps para IPSEC VPN com licenças habilitadas para no mínimo 10.000 túneis Gateway-to-Gateway ou Client-to-Gateway;
- Disco de, no mínimo, 200 (duzentos) GB para armazenamento de informações locais;
- Além das 8 interfaces da configuração mínima, deve permitir adicionar a qualquer momento outras 16 interfaces de rede 1 Gbp SFP ou 10 Gbps SFP+, com seus respectivos transceivers 1 Gbps ou 10Gbps Multimodo SR lc-lc;
- Deve possuir 02 (duas) fontes de energia AC, redundante e hot-swappable com ajuste automático de tensão para operação nas tensões de 100 a 240-VAC/60 Hz;

9.2.13. Sistema de Gerência:

9.2.13.1. Características técnicas mínimas:

- Deve possuir licenciamento válido, garantia e suporte técnico do fabricante por no mínimo o período de vigência contratual, com possibilidade de renovação por igual período;
- A solução ofertada deverá ser entregue com hardware appliance dedicado e licenças, assim como qualquer outro componente necessário ao seu pleno funcionamento;
- Características físicas:
  - Possuir fontes de alimentação hot-plug em redundância (1+1);
  - Capacidade mínima de armazenamento de 900 GB;
  - Suportar no mínimo 5.000 (cinco mil) logs/flows por segundo;
  - Possuir no mínimo duas interfaces de rede Ethernet 1 (um) GbE ;
- As funcionalidades de gerência e retenção de logs que compõem a plataforma de segurança podem funcionar em múltiplos appliances, desde que obedeçam a todos os requisitos desta especificação;
- Deve centralizar logs e relatórios usando uma única interface de gerenciamento;
- O gerenciamento da solução deve suportar acesso via SSH, WEB (HTTPS) e API aberta;
- O armazenamento poderá ser realizado através de composição com solução de terceiros, como por exemplo, SIEM (Security Information and Event Management);
- Não será permitida a instalação de cliente para administração do appliance de firewall;
- O gerenciamento deve permitir/possuir:
  - Visualização de logs e relatórios relacionados às políticas de firewall e controle de aplicação;
  - Visualização de logs e relatórios relacionados ao IPS, Controle de Aplicação e Anti-Malware;
  - Visualização de logs e relatórios relacionados às políticas de Filtro de URL;
  - Monitoração de logs;
  - Ferramentas de investigação de logs;
  - Visualização das capturas de pacotes realizadas nos ataques detectados;
  - Acesso concorrente de administradores;

- Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;
- Deve suportar a definição de perfis de acesso à console, com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;
- Deve suportar autenticação integrada ao Microsoft Active Directory (AD) e servidor Radius;
- Deve possibilitar a geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;
- Deve ter capacidade de gerar relatórios gráficos que permitam visualizar as mudanças na utilização de aplicações na rede no que se refere a um período de tempo anterior, permitindo comparar os diferentes consumos realizados pelas aplicações no decorrer do tempo;
- Deve prover relatórios com visão correlacionada de aplicações, ameaças (IPS, Antivírus e Anti-Spyware), URLs e filtro de arquivos, para melhor diagnóstico e resposta a incidentes;
- Deve permitir a criação de painéis (dashboards) ou relatórios customizados com, no mínimo, as seguintes informações: visibilidade do tráfego de aplicativos, usuários, categorias de URL, ameaças identificadas pelo IPS, malware detectado, aplicações mais utilizadas, protocolos mais utilizados, principais atacantes (com informação de geolocalização);
- Deve possibilitar a coleta de estatísticas de todo o tráfego associado aos dispositivos de segurança;
- Deve prover uma visualização sumarizada das aplicações e URLs que geraram tráfego associado à solução;
- Deve possuir mecanismo "drill-down" para navegação nos dashboards em tempo real;
- Deve ser possível exportar os logs em CSV;
- Deve permitir que os logs e relatórios sejam rotacionados automaticamente em função do tempo em que estão armazenados na solução;
- Deve exibir as seguintes informações, de forma histórica ou em tempo real:
    - Situação do dispositivo e do cluster;
    - Principais aplicações;
    - Principais aplicações por risco;
    - Principais ameaças;
    - Uso de CPU e memória;
- No mínimo, os seguintes relatórios devem ser gerados:
    - Resumo gráfico de aplicações utilizadas;
    - Principais aplicações por utilização de largura de banda de entrada e saída;
    - Principais aplicações por taxa de transferência de bytes;
    - Principais hosts por número de ameaças identificadas;
    - Atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas, categorias de URL e ameaças de rede vinculadas a este tráfego;
    - Deve permitir a criação de relatórios personalizados;
- Deve gerar alertas automáticos via:
    - Email;
    - SNMP;
    - Syslog;
- O gerenciamento deve permitir/possuir:
    - Criação e administração de políticas de firewall e controle de aplicação;
    - Criação e administração de políticas de IPS e Anti-Malware;
    - Criação e administração de políticas de Filtro de URL;
    - Uso de palavras chaves para facilitar identificação de regras;
    - Alertas de alterações, no caso acesso simultâneo de dois ou mais administradores;
    - Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários e alteração de configurações;

- Autenticação integrada ao Microsoft Active Directory (AD) e servidor Radius;
- Localização das regras em que um endereço IP, IP Range, subnet ou objetos estão sendo utilizados;
- Backup das configurações e rollback de configuração para a última configuração salva;
- Mecanismo de validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras;
- Visualização e comparação de configurações atuais, configuração anterior e configurações antigas.

## 10. EQUIPAMENTOS ROTEADORES

Com objetivo de atender as necessidades dos Órgãos e Unidades da Rede de Dados do Governo do estado do Rio de Janeiro, são especificados 4 (quatro) tipos de roteadores em função das velocidades e da demanda por funcionalidades e serviços. Assim, estima-se a sua utilização do seguinte modo, considerando também o limite de 75% de utilização da CPU.

**TIPO I:** circuitos com velocidades de até 30Mbps.

**TIPO II:** circuitos com velocidade de até 50Mbps.

**TIPO III:** circuitos com velocidade de até 200Mbps.

**TIPO IV:** circuitos com velocidade de até 4Gbps.

### 10.1. Características Comuns a Todos Tipos:

10.1.1. Características de Hardware:

10.1.1.1. Deverá permitir a acomodação em rack padrão 19" e ter no máximo 1 unidade rack (1RU);

10.1.1.2. Deve possuir memória com capacidade suficiente para armazenar, no mínimo, duas novas versões de sistema operacional que tenha o tamanho de duas vezes o sistema operacional na versão atual.

10.1.1.3. Deve possuir a quantidade mínima necessária de memória RAM e memória auxiliar que atenda a todas as funcionalidades exigidas nesta especificação, em conformidade com as recomendações do Fabricante.

10.1.1.4. Deverá possuir LEDs de diagnóstico que forneçam informações de alimentação e atividade do equipamento;

10.1.1.5. Deve possuir uma porta de console para o gerenciamento e configuração do equipamento, no padrão RS-232, com conector RJ-45 ou DB-9;

10.1.1.6. Deverá possuir console com porta USB;

10.1.1.7. Deve possuir uma porta auxiliar com velocidade de até 115.2Kbps, serial assíncrona, com conector RJ-45;

10.1.1.8. Deverá ser destinado ao uso normal em ambiente tropical com umidade relativa na faixa de 20% a 80% (sem condensação) e suportar temperatura ambiente de armazenamento entre 0°C e 50°C;

10.1.1.9. O equipamento deve possuir fontes de energia interna, para Corrente Alternada (AC – Alternating Current), com chaveamento automático e capacidade de operação em 100V à 240V (50/60Hz);

10.1.1.10. Deve permitir auto-negociação de modo de transmissão half / full-duplex para as interfaces Ethernet.

10.1.1.11. Deve possuir suporte ao padrão IEEE 802.1Q nas interfaces Ethernet.

10.1.1.12. Quando solicitado pela CONTRATADA, deverá suportar a inclusão de módulo de interface E1 Clear-Channel, taxas de 2 Mbps;

10.1.1.13. Quando solicitado pela CONTRATADA, deverá suportar no mínimo 4 interfaces E1 Clear-Chanel;

10.1.1.14. Deve possuir LEDs de diagnóstico que forneçam informações de alimentação e atividade do equipamento;

10.1.1.15. Deve possuir LEDs de diagnósticos que forneçam informações e status das portas;

10.1.1.16. Caso o Fabricante possua mais de uma versão de uma mesma placa para atendimento a esta especificação, deverá ser fornecida a versão mais recente e estável da mesma;

10.1.1.17. Deverá possuir aceleração criptográfica por hardware para as seguintes certificações:

- Digital Encryption Standard (DES) e Triple DES (3DES);
- Advanced Encryption Standard (AES) 128, 192, e 256 ;
- Message Digest Algorithm 5 (MD5) e MD5 com Hashed Message Authentication Codes MD5_hmac Secure Hashing Algorithm-1 (SHA-1) and SHA1_hmac ;

10.1.2. Funcionalidades Gerais:

10.1.2.1. Deve permitir a configuração em cada porta de um texto possibilitando ao administrador a inclusão de informações que identifiquem o que está conectado na respectiva porta.

10.1.2.2. Deve permitir a reinicialização de interfaces do equipamento sem afetar o funcionamento do mesmo;

10.1.2.3. Deve possuir suporte à tradução de endereços de rede (Network Address Translation – NAT) em conformidade com a RFC 1631 e RFC 3022;

10.1.2.4. Deve possuir suporte à tradução de endereços de porta (Port Address Translation – PAT);

10.1.2.5. Permitir a atualização remota do sistema operacional e arquivos de configuração utilizados no equipamento via interface Ethernet;

10.1.2.6. Deve implementar a opção local de carga do sistema do equipamento via memória Flash;

10.1.2.7. Permitir que a sua configuração seja feita através de terminal assíncrono;

10.1.2.8. Possuir ferramentas para depuração e gerenciamento em primeiro nível para IPv4 e IPv6, implementando ao menos, testes ICMP, debug, trace e log de eventos;

10.1.2.9. Suportar protocolo de coleta de informações de fluxos que circulam pelo equipamento;

10.1.2.10. A informação coletada deve ser automaticamente exportável em intervalos pré-definidos através de um protocolo IPFIX padronizado, para no mínimo: Net Flow ou Sflow ou JFlow ou Hflow ou Cflowd;

10.1.2.11. Deve suportar a implementação da funcionalidade de DHCP Relay e DHCP Server;

10.1.2.12. Deve possibilitar a configuração dinâmica de portas por software, permitindo a definição de portas ativas/inativas;

10.1.3. Funcionalidades Gerais – Rede MPLS:

10.1.3.1. Deve suportar o protocolo de tunelamento GRE (Generic Routing Encapsulation) em conformidade com o padrão RFC 2784, contemplando, no mínimo, os seguintes recursos:

- Permitir a associação do túnel GRE a uma tabela virtual de roteamento específica;
- Operação em modo multiponto (“multipoint GRE”);
- Possibilidade de configuração de “Keepalive” nos túneis;
- Suporte a QoS – deve ser possível preservar as marcações no cabeçalho do pacote original para os pacotes transportados com encapsulamento GRE.

10.1.3.2. Deve ter a capacidade de atualização de software via FTP e via TFTP, em conformidade com as RFCs 783 e 1350;

10.1.3.3. Deve permitir a transferência segura de arquivos para o equipamento através do protocolo SCP (Secure Copy) ou SFTP (Secure FTP);

10.1.3.4. Deve permitir a gravação de log externo (syslog). Deve ser possível definir o endereço IP de origem dos pacotes syslog gerados pelo equipamento;

10.1.3.5. Deve permitir consultas de DNS com resolução de nomes em endereços IPv6;

10.1.3.6. Deve responder a pacotes para teste da implementação dos níveis de serviço especificados (SLA). Deverão ser suportadas no mínimo as seguintes operações de teste: ICMP echo, estabelecimento de conexão TCP (em porta TCP configurável), UDP echo (em porta UDP configurável);

10.1.3.7. Deve suportar o envio de traps SNMP em função do resultado dos testes ultrapassarem limiares pré-configurados ou no caso de falha.

10.1.3.8. Deve possibilitar a implementação de Lan Virtual (VLAN) por porta e compatíveis com o padrão IEEE 802.1Q e IEEE 802.1Q-in-Q;

10.1.3.9. Deve implementar o protocolo de controle de agregação de enlace (LACP) conforme o padrão IEEE 802.3ad, permitindo agrupar, no mínimo, 4 (quatro) interfaces do mesmo tipo;

10.1.3.10. Deve implementar o protocolo VRRP (Virtual Router Redundancy Protocol), em conformidade com o padrão RFC 2338;

10.1.3.11. Deve suportar mecanismo de autenticação MD5 entre os peers VRRP;

10.1.3.12. Deve suportar o protocolo HDLC (High-Level Data Link Control);

10.1.3.13. Deve possuir suporte ao protocolo PPP (Ex. PPP sobre Ethernet);

10.1.3.14. Deve possuir suporte a protocolo de redirecionamento para cache de Web;

10.1.3.15. Deve possuir suporte ao protocolo RSVP (Resource Reservation Protocol);

10.1.3.16. Deve possuir suporte a compressão de cabeçalho RTP, em conformidade com a RFC 2508;

10.1.4. Segurança:

10.1.4.1. Deve implementar filtragem de pacotes (listas de controle de acesso) para IPv4 e IPv6;

10.1.4.2. Deve implementar listas de controle de acesso (ACLs), para filtragem de pacotes, baseadas em endereço IP de origem e destino, portas TCP e UDP;

10.1.4.3. Deve implementar mecanismos de AAA (Authentication, Authorization e Accounting) com garantia de entrega;

10.1.4.4. Deve implementar mecanismo de autenticação para acesso local ou remoto ao equipamento baseado em um servidor de autenticação e autorização do tipo TACACS+;

10.1.4.5. Deve suportar a criação de VPN, com no mínimo as funcionalidades listadas abaixo: (caso esta funcionalidade seja ativada através de licença de software, não existe a necessidade de fornece-la inicialmente):

- Deve suportar serviços de VPN baseado no padrão IPSEC (IP Security Protocol);
- Deve suportar algoritmos de criptografia 56-bit DES, 168-bit 3DES, 128-bit AES e 256-bit AES para conexões VPN com IPSEC;

10.1.4.6. Deve permitir a criação de listas de acesso baseadas em endereços IP para limitar o acesso ao equipamento via Telnet, SSH e SNMP;

10.1.4.7. Deve implementar a criptografia de todos os pacotes enviados ao servidor de controle de acesso e não só os pacotes referentes à senha;

10.1.4.8. Deve permitir controlar e auditar quais comandos os usuários e grupos de usuários podem emitir;

10.1.4.9. Deve suportar a criação de VPN dinamicamente, para criar uma rede VPN totalmente ligada; (caso esta funcionalidade seja ativada através de licença de software, não existe a necessidade de fornece-la

10.1.4.10. Deve suportar serviços de Virtual Private Network (VPN) baseados no padrão IKE (Internet Key Exchange);

10.1.4.11. Deve suportar a transparência de conexões IPSEC a NAT (NAT-T) através do encapsulamento dos pacotes IPSEC com UDP;

10.1.4.12. Deve reagrupar pacotes de sessão de VPN fragmentados para análise e entrega no destino;

10.1.4.13. Deve permitir a criação de VPNs IPSec baseada em politícas de segurança;

10.1.4.14. Devem ser implementados túneis VPN nos modos de operação “tunnel mode” e “transport mode”. Devem ser suportadas no mínimo as RFCs 1828, 1829, 2401, 2402, 2406, 2407, 2408 e 2409;

10.1.4.15. Deve suportar as funcionalidades de gerenciamento de chaves para VPN;

10.1.4.16. Deve suportar a utilização de clientes baseados em IPSec;

10.1.4.17. Suportar o tráfego do protocolo GRE sobre IPSec;

10.1.4.18. Suportar o tráfego Multicast IP sobre IPSec;

10.1.5. Gerenciamento:

10.1.5.1. Deve implementar o protocolo NTPv3 (Network Time Protocol versão 3). Deve ser suportada autenticação entre os peers NTP, conforme definições da RFC 1305;

10.1.5.2. Deve suportar o protocolo SNTP (Simple Network Time Protocol), em conformidade com o padrão RFC 4330 ou 5905;

10.1.5.3. Deve suportar o protocolo de gerenciamento SNMP e MIB-II, em conformidade com os padrões RFCs 1157 e RFC 1213;

10.1.5.4. Deve suportar os protocolo SNMPv2c e SNMPv3, incluindo a geração de traps;

10.1.5.5. Implementar pelo menos os seguintes níveis de segurança para SNMP versão 3:

- Sem autenticação e sem privacidade (no AuthNoPriv);
- Com autenticação e sem privacidade (authNoPriv);
- Com autenticação e com privacidade (authPriv) utilizando algoritmo de criptografia AES.

10.1.5.6. Suportar SNMP sobre IPv6;

10.1.5.7. Implementar MIB privativa que forneça informações relativas ao funcionamento do equipamento;

10.1.5.8. Possuir descrição completa da MIB implementada no equipamento, inclusive a extensão privativa;

10.1.5.9. Possibilitar a obtenção da configuração do equipamento através do protocolo SNMP;

10.1.5.10. Possibilitar a obtenção via SNMP de informações de capacidade e desempenho da CPU, memória e portas;

10.1.5.11. Deve proteger a interface de gerência do equipamento através de senha.

10.1.5.12. Deve permitir administração e configuração através de interface de linha de comando (CLI);

10.1.6. Gerenciamento – Rede MPLS:

10.1.6.1. Deve possuir suporte nativo, no mínimo, aos 2 (dois) grupos básicos de RMON, a saber: alarms e events, em conformidade com os padrões RFC 1757 ou 2819;

10.1.6.2. Possibilitar a obtenção da configuração do equipamento através do protocolo SNMP;

10.1.6.3. Deve permitir ser configurável e gerenciável via interface gráfica (GUI), linha de comando (CLI), SNMP, Telnet, SSH, HTTP e HTTPS com, no mínimo, 15 sessões simultâneas e independentes

10.1.6.4. Deve permitir a inserção de um certificado digital PKI para autenticação do protocolo SSH e Túneis IPSEC;

10.1.6.5. O equipamento deve suportar a configuração com um único endereço IP para gerência e administração, para uso dos protocolos: SNMP, NTP, HTTPS, SSH, TELNET, TACACS+ e RADIUS, provendo identificação gerencial única ao equipamento;

10.1.6.6. Deve permitir a configuração de endereços IPv6 para gerenciamento;

10.1.6.7. Deve proteger a interface de gerência do equipamento através de senha.

10.1.6.8. Deve permitir administração e configuração através de interface de linha de comando (CLI);

10.1.6.9. Deve suportar, pelo menos, 4 (quatro) conexões de Telnet (VT-100) simultâneas;

10.1.6.10. Deve suportar a criação e manutenção de listas de acesso baseadas em endereço IP para limitar o acesso, via telnet, ao roteador;

10.1.6.11. Deve implementar facilidades de syslog;

10.1.7. Roteamento:

10.1.7.1. Deve permitir o roteamento nível 3 entre as VLANs;

10.1.7.2. Deve suportar a pilha de protocolos TCP/IP;

10.1.7.3. Deve suportar o protocolo roteável IPv4;

10.1.7.4. Deve suportar o protocolo roteável IPv6;

10.1.7.5. Deve implementar o protocolo de roteamento OSPF, em conformidade com, no mínimo, os padrões especificados abaixo:

- The OSPF Not-So-Stubby Area (NSSA) Option;
- OSPF Version 2 Management Information Base;
- OSPF Version 2;

10.1.7.6. Deve suportar o protocolo de roteamento BGP versão 4, conforme especificados abaixo:

- Border Gateway Protocol (BGP-4);
- Autonomous System Confederation for BGP;
- BGP Communities Attribute;

10.1.7.7. Deve implementar o protocolo de roteamento RIPv2;

10.1.8. Roteamento – Rede MPLS:

10.1.8.1. Deve implementar mecanismo de pilha dupla (IPv4 e IPv6), para permitir o funcionamento simultâneo dos protocolos IPv4 e IPv6;

10.1.8.2. Deve permitir a configuração de rotas estáticas para IPv4 e IPv6;

10.1.8.3. Deve suportar o protocolo de roteamento BGP versão 4, conforme especificados abaixo:

- Multi-Protocol Extensions for BGP-4;
- BGP Route Flap Damping;
- Capabilities Advertisement with BGP-4;
- Route Refresh Capability for BGP-4.

10.1.8.4. Deve implementar o protocolo VRRP (Virtual Router Redundancy Protocol), em conformidade com o padrão RFC 2338;

10.1.8.5. Deve suportar os protocolos de IP Multicast: IGMP (Internet Group Membership Protocol) e PIM (Protocol Independent Mode);

10.1.8.6. Deve suportar roteamento dinâmico OSPFv3 para IPv6, em conformidade com o padrão RFC 5340;

10.1.8.7. Deve permitir a virtualização das tabelas de roteamento (camada 3). As tabelas de roteamento virtuais deverão ser completamente segmentadas;

10.1.8.8. Deve permitir a possibilidade de alterações de roteamento automatizadas baseadas em métricas de desempenho dos enlaces, para no mínimo, perda de pacotes, atraso e jitter;

10.1.9. Qualidade de serviço:

10.1.9.1. Deve suportar o padrão IEEE 802.1p para cada porta;

10.1.9.2. Deve possuir a facilidade de priorização de tráfego através do padrão IEEE 802.1p;

10.1.9.3. Deve possuir suporte a uma fila com prioridade estrita (prioridade absoluta em relação às demais classes dentro do limite de banda que lhe foi atribuído) para tratamento do tráfego "real-time" (voz e vídeo);

10.1.9.4. Deve suportar a classificação de pacotes de dados (QoS), baseados em:

- Protocolos da camada de rede (IPv4 e IPv6) do Modelo OSI (Endereços IP origem e destino);
- Protocolos da camada de transporte do Modelo OSI (TCP e UDP);

10.1.9.5. Deve suportar a classificação, marcação e remarcação baseadas em CoS ("Class of Service") para a camada de enlace;

10.1.9.6. Deve suportar a classificação, marcação e remarcação baseados em "DSCP" ("Differentiated Services Code Point") para a camada de rede;

10.1.9.7. Deve suportar funcionalidades de QoS de "Traffic Shapping";

10.1.9.8. Deve suportar funcionalidades de QoS de "Traffic Policing";

10.1.9.9. Deve suportar o padrão IEEE 802.3x (Flow Control)

10.1.10. Qualidade de Serviço – Rede MPLS:

10.1.10.1. Deve suportar a classificação de pacotes de dados (QoS), baseados em:

- Endereços MAC de origem e destino;
- VLAN.

10.1.10.2. Deve suportar a classificação, marcação e remarcação baseados em "IP precedence";

10.1.10.3. Deve permitir a marcação de tráfego baseado no campo ToS (Type of Service), conforme RFC 2474;

10.1.10.4. Deve prover as funcionalidades de Priority Queuing (PQ), Custom Queuing (CQ) e Weighted Fair Queuing (WFQ);

10.1.10.5. Suportar no mínimo duas filas Low Latency Queueing (LLQ) por policies;

10.1.10.6. Deve ser possível a especificação de garantia de banda por classe de serviço;

10.1.10.7. O equipamento deve suportar o mapeamento das prioridades nível 2 (802.1p) em prioridades nível 3 (IP Precedence e DSCP) e vice-versa;

10.1.10.8. Deve implementar RSVP (Resource Reservation Protocol) em conformidade com no mínimo, os padrões RFC 3209, RFC 2961, RFC 2747 e RFC 2205;

10.2. **TIPO I**

10.2.1. Características de Hardware:

10.2.1.1. Deve possuir, no mínimo, 2 (duas) interfaces Gigabit Ethernet (10 Base-T/100Base-TX/1000Base-T) autosensing com conector RJ-45 em conformidade com os padrões IEEE 802.3i e 802.3u;

10.2.2. Desempenho:

10.2.2.1. Deve ter uma performance mínima de 70.000 pps com pacotes de 64 bytes;

10.2.2.2. Deve ser fornecido com capacidade de no mínimo 30 (trinta) Mbps;

10.3. **TIPO II**

10.3.1. Características de Hardware:

10.3.1.1. Deve possuir, no mínimo, 3 (três) interfaces Gigabit Ethernet (10 Base-T/100 Base-TX/1000 Base-T) autosensing com conector RJ-45 em conformidade com os padrões IEEE 802.3i e 802.3u;

10.3.2. Funcionalidades Gerais:

10.3.2.1. Deve suportar os CODECS (G.711, G.728, G.729 ou G.729b), quando solicitado pela CONTRATADA;

10.3.2.2. Deve ter a possibilidade de ser inserido em redes com serviços de Voz sobre IP (VoIP), quando solicitado pela CONTRATADA;

10.3.2.3. Deve suportar mecanismo de controle de chamadas IP sem a necessidade de um controlador central, quando solicitado pela CONTRATADA;

10.3.2.4. Deve suportar mecanismo que permita a continuidade do controle de chamadas IP mesmo após a perda de comunicação com o controlador de chamadas central, quando solicitado pela CONTRATADA;

10.3.3. Desempenho:

10.3.3.1. Deve ter uma performance mínima de 200.000 pps com pacotes de 64 bytes;

10.3.3.2. Deve ser fornecido com capacidade de no mínimo 50 (cinquenta) Mbps;

10.4. **TIPO III**

10.4.1. Características de Hardware:

10.4.1.1. Deve possuir, no mínimo, 3 (três) interfaces Gigabit Ethernet (10 Base-T/100 Base-TX/1000 Base-T) autosensing com conector RJ-45 em conformidade com os padrões IEEE 802.3i e 802.3u;

10.4.1.2. Deve suportar a inserção de interfaces analógicas (FXS ou FXO) e digitais de voz (E1);

10.4.1.3. Deve suportar no mínimo 4 (quatro) interfaces de Voz digitais E1;

10.4.2. Funcionalidades Gerais:

10.4.2.1. Deve suportar os CODECS (G.711, G.728, G.729 ou G.729b), quando solicitado pela CONTRATADA;

10.4.2.2. Deve ter a possibilidade de ser inserido em redes com serviços de Voz sobre IP (VoIP), quando solicitado pela CONTRATADA;

10.4.2.3. Deve suportar mecanismo de controle de chamadas IP sem a necessidade de um controlador central, quando solicitado pela CONTRATADA;

10.4.2.4. Deve suportar mecanismo que permita a continuidade do controle de chamadas IP mesmo após a perda de comunicação com o controlador de chamadas central, quando solicitado pela CONTRATADA;

10.4.3. Desempenho:

10.4.3.1. Deve ter uma performance mínima de 400.000 pps com pacotes de 64 bytes;

10.4.3.2. Deve ser fornecido com capacidade de no mínimo 200 (duzentos) Mbps, tanto para como um rede MPLS ou SD-WAN;

10.5. **TIPO IV**

10.5.1. Características de Hardware:

10.5.1.1. Possuir 4 (quatro) interfaces Ethernet 1000Base-X para inserção de conectores SFP;

10.5.1.2. Possuir capacidade de associação das portas 1000Base-X, no mínimo, em grupo de 4 (quatro) portas, formando uma única interface lógica com as mesmas facilidades das interfaces originais, compatível com a norma IEEE 802.3ad;

10.5.1.3. Suportar módulos com portas do tipo 10GBASE-X, E3 e OC-48;

10.5.1.4. Possuir fonte de alimentação redundante interna AC bivolt, com seleção automática de tensão (na faixa de 100 a 240V) e frequência (de 50/60 Hz);

10.5.2. Funcionalidades Gerais:

10.5.2.1. Possibilidade de criação de versões de configuração e suporte a “rollback” da configuração para versões anteriores;

10.5.3. Desempenho:

10.5.3.1. Possuir backplane de, no mínimo 5 (cinco) Gbps, devendo ser substituído proativamente em caso de problemas de esgotamento de capacidade ou quando solicitado pelo CONTRATANTE;

10.5.3.2. Suportar pelo menos 2 (dois) Gbps de throughput com todas as funcionalidades de roteamento e segurança ativas simultaneamente;

10.5.3.3. Possuir uma taxa de comutação de pacotes de no mínimo 3 (três) milhões pacotes por segundo (Mpps);

10.5.3.4. Deve ser fornecido com capacidade de no mínimo 2 (dois) Gbps;

## 11. DOS CIRCUITOS DE ACESSO DA REDE IP GOVERNO

### 11.1. CIRCUITOS DE ACESSO DO DATACENTER DO PRODERJ

Os circuitos de acessos do Backbone da Rede IP Governo conectados ao Datacenter do PRODERJ deverão atender aos seguintes requisitos.

1. 11.1.1. Todos os circuitos deverão ser atendidos obrigatoriamente através de Fibra Ótica, sendo que os acessos redundantes deverão ser atendidos por cabos de fibra ótica por caminhos distintos;
2. 11.1.2. A redundância dos enlaces e roteadores CPEs deverá ser implementada, de modo que cada enlace seja conectado a um CPE físico distinto, sendo que circuitos e roteadores deverão ser capazes de assumir todo o tráfego;
3. 11.1.3. Cada enlace contratado, principal e de contingência deverão ser conectados a um PE (Provider Edge) físico distinto do backbone da CONTRATADA;
4. 11.1.4. A CONTRATADA deverá elaborar o Projeto Físico e Lógico de Redundância, que deverá ser submetido ao PRODERJ para aprovação quando da implantação dos circuitos solicitados.

### 11.2. CIRCUITOS DE ACESSO DAS UNIDADES ESPECIAIS

11.2.1. Todos os circuitos deverão ser atendidos obrigatoriamente através de Fibra Ótica, sendo que os acessos redundantes deverão ser atendidos por cabos de fibra ótica por caminhos distintos ou por fibra ótica (principal) e rádio enlace de frequência licenciada;

11.2.2. A CONTRATADA deverá elaborar o Projeto Físico e Lógico de Redundância, que deverá ser submetido ao PRODERJ para aprovação quando da implantação dos circuitos solicitados;

11.2.3. Casos de exceções para atendimento as Redes dos Órgãos e Unidades do Governo deverão ser tratadas com Órgãos com a anuência da Gerência de Redes e Telecomunicações do PRODERJ, durante validação do Projeto Executivo com os envolvidos;

11.2.4. A solução completa de contingência deverá ser testada pela CONTRATADA periodicamente ao longo da execução do contrato. A periodicidade deverá ser semestral e o horário da realização dos testes será definido em comum acordo com o PRODERJ que deverá ser notificado para acompanhar os testes;

11.2.5. A CONTRATADA deverá disponibilizar relatório com os resultados dos testes de Contingência;

11.2.6. O PRODERJ poderá solicitar a realização extraordinária dos testes com antecedência mínima de sete dias úteis.

## 12. DOS REQUISITOS DE ROTEAMENTO

12.1. O Plano de Roteamento deverá ser proposto pela prestadora vencedora em seu Projeto Executivo. Serão definidas as características dos protocolos de roteamento que serão instalados em cada um dos sítios, de forma a garantir a interconexão entre eles;

12.2. A CONTRATADA deverá prestar os serviços de comunicação de dados, conforme os seguintes padrões: RFC 1163 (BGP - Border Gateway Protocol), RFC 2283 (Multiprotocol Extensions for BGP-4) e RFC 2547 (BGP/MPLS/VPNs);

12.3. As premissas para a criação do Plano de Roteamento da rede são:

- Ser escalável;
- Realizar agregação de rotas para endereços contíguos;
- Manter o plano de roteamento atual das redes internas da Rede IP Governo;
- Permitir o acesso de qualquer ponto da rede às aplicações compartilhadas.

12.4. Devido ao porte da rede corporativa, a configuração do roteamento através de rotas estáticas pode não ser muito atrativa, pois a tarefa de gerenciamento de rotas principais e alternativas, para o caso de falhas, se torna uma tarefa muito trabalhosa e suscetível a erros;

12.5. Ficará a cargo da CONTRATADA a definição do protocolo de roteamento a ser utilizado entre os roteadores PE e CPE. Porém, recomenda-se o uso de um protocolo com baixo tempo de convergência, como o BGP em sua última versão. Nesse sentido, a solução de roteamento deverá permitir a convergência da rede em um tempo menor que 20 (vinte) segundos para o caso de mudança topológica da rede causada por falha(s) em enlace(s) ou equipamento(s);

12.6. A solução de roteamento deverá ser projetada e implantada de forma escalável permitindo a evolução e o crescimento da rede.

## 13. DOS REQUISITOS DE SEGURANÇA

13.1. A CONTRATADA deverá manter o controle da segurança física e lógica de seus ambientes operacionais, estabelecendo as políticas de segurança a serem aplicadas aos serviços de telecomunicações contratados;

13.2. A CONTRATADA deverá implementar quaisquer controles de segurança (bloqueios, cancelamentos de links, etc), quando solicitado pelo CONTRATANTE, caso se identifique riscos de disponibilidade ou de cometimento de crimes através da rede corporativa;

13.3. A ação descrita no subitem anterior possui o intuito de prevenção de incidentes de segurança de forma a garantir níveis de segurança adequados nos ambientes de suas redes, por onde transitarão as informações do Governo do Estado do Rio de Janeiro, não eximindo a CONTRATADA das responsabilidades previstas no Termo de Referência e este Encarte Técnico;

13.4. Em relação aos aspectos técnicos de segurança da informação, a CONTRATADA deverá atender aos seguintes requisitos:

13.4.1. Prover uma rede logicamente independente e isolada de qualquer rede de terceiros, inclusive da internet. O isolamento deverá ser realizado em nível lógico do MPLS e em nível 2 (do modelo OSI) para o acesso. Esta garantia deverá ser implantada fim-a-fim e também se aplica às soluções de contingência;

13.4.2. Caso seja solicitado pelo PRODERJ, a CONTRATADA deverá aplicar nos roteadores CPEs fornecidos e em outros equipamentos, exclusivos para prestação de serviços, implementações de segurança tais como: autenticação do roteador CPE, controle de acesso aos dispositivos, listas de acesso e logging e outras configurações necessárias à segurança da Rede IP Governo;

13.4.3. Caso necessário deverá ser empregado esquema de autenticação no nível de protocolo de roteamento, de forma que roteadores não autorizados não possam injetar ou descobrir rotas da Rede IP Governo;

13.4.4. Será responsabilidade da CONTRATADA, manter em seus quadros técnicos especialistas em segurança e prover serviços específicos de prevenção e reação aos incidentes de segurança em tecnologia da informação;

13.4.5. A CONTRATADA deverá configurar de maneira apropriada os elementos de rede para habilitar o registro dos eventos da Rede IP Governo, tais como conexões externas e registro de utilização de serviços (por exemplo, arquivos transferidos através de FTP e tentativas de login não autorizados). Os registros devem estar com o horário sincronizado via protocolo NTP e possuir detalhes suficientes para identificação do evento, seu autor, seu alvo/objeto e momento de ocorrência;

13.4.6. A CONTRATADA deverá possuir um sistema dedicado à coleta e ao armazenamento dos registros gerados pelos dispositivos da Rede IP Governo;

13.4.7. A CONTRATADA deverá aplicar e manter atualizados patches de segurança nos seus roteadores, incluindo os CPE dos sítios ou em outros equipamentos de suas redes, exclusivos para prestação de serviços ao Governo do Estado;

13.4.8. A CONTRATADA deverá informar ao PRODERJ os patches de segurança necessários para a atualização dos roteadores CPEs do backbone do PRODERJ, unidades especiais e dos sítios, exclusivos para prestação de serviços a Rede do Governo.

## 14. ESPECIFICAÇÕES DE QOS DA REDE IP GOVERNO

14.1. A Rede IP Governo deverá suportar Qualidade de Serviço (QoS), de acordo com condições estabelecidas nesse item, inclusive considerando a arquitetura DiffServ;

14.2. Deverá permitir a obtenção de escalabilidade e eficácia na diferenciação dos serviços através da implementação de mecanismos de classificação e condicionamento somente nos elementos de borda da rede e aplicação "per-hop behaviors" aos agregados de tráfego que forem marcados usando se o campo DS nos campos apropriados dos cabeçalhos de pacotes MPLS;

14.3. No escopo da conexão de cada cliente, há a necessidade de diferenciação de serviços, incluindo a alocação de banda e priorização de pacotes para redução de atrasos de certas classes de tráfego;

14.4. A CONTRATADA deverá implementar e fornecer, de forma fim-a-fim, classificação e marcação de diferentes tipos de tráfego, possibilitando a configuração de pelo menos 5 (cinco) classes de serviços:

14.4.1. Supervisão de Rede: aplicações de monitoramento e controle da rede, que deverão ser priorizadas acima de todas as outras a fim de garantir a disponibilidade de recursos para as intervenções preventivas ou corretivas que se façam necessárias ao seu correto funcionamento, tais como, por exemplo: Telnet, SSH, SNMP, NTP, syslog e Radius, Esta classe de serviço deverá ser utilizada exclusivamente pela empresa prestadora do serviço para o gerenciamento da Rede;

14.4.2. Tempo Real – aplicações de Voz e Vídeo sensíveis que são sensíveis ao retardo (delay) e variações de retardo da rede (jitter), que exigem priorização de pacotes limitadas a 50% da Banda;

14.4.3. Deverá a CONTRATADA disponibilizar duas classes de serviços distintas de Tempo Real, uma para Voz e outra para Vídeo;

14.4.4. Dados Críticos: aplicações críticas que exigem a entrega garantida e tratamento prioritário, tais como acesso HTTP e HTTPS a portais corporativos internos;

14.4.5. Dados Prioritários: aplicações que sejam menos críticas, mas que também necessitem de tratamento prioritário na rede da CONTRATADA;

14.4.6. Melhor Esforço – Best Effort: todo tráfego não explicitamente atribuído às classes Supervisão da Rede, Tempo Real, Dados Prioritários deverá ser alocado nesta classe. Sua finalidade é permitir um valor muito baixo de recursos para tráfegos não previstos ou ainda não identificados como tráfegos importantes; Essa classe deverá permitir o fluxo de tráfego, se houver recursos disponíveis na rede, impedindo que esse tráfego afete negativamente as demais classes;

14.5. As classe de serviço serão aquelas específicas de uma Rede MPLS nativo ou de uma Rede SD-WAN;

14.6. A definição das classes e percentuais de reserva de banda deverá discutida com a equipe técnica do PRODERJ para definição no Projeto Executivo da solução. A equipe de engenharia de tráfego da CONTRATADA deverá, sempre que possível, auxiliar acerca de tais aspectos de modo a otimizar a operação da rede. Ademais, o PRODERJ poderá solicitar a qualquer momento a modificação nas configurações das classes de serviço, de modo a adaptar à evolução de tráfego de suas aplicações.

## 15. SERVIÇO DE SEGURANÇA GERENCIADA (MSS)

O Serviço de Segurança Gerenciada tem por objetivo ofertar uma camada de segurança adicional para a Rede IP Governo, devendo estar presente no Datacenter do PRODERJ e em todos os pontos de presença contratados e de acordo com as especificações do Termo de Referência e este Encarte Técnico.

15.1. A solução de segurança deverá ser baseada em hardware do tipo appliance, com recursos de Next Generation Firewall (NGFW), além de console de gerenciamento e monitoração;

15.2. 15.2. A solução de segurança do PRODERJ, especificada no item 9.2, e o serviço de Gerenciamento de Segurança deverá ser complementado com a implantação de um SNOC (Security and Network Operation Center), contendo as ferramentas de hardware e software necessárias ao devido monitoramento, detecção e tratamento dos incidentes, que serão operadas por equipe alocada nas dependências da autarquia em horário comercial, com os perfis especificados no item 18 do Termo de Referência, não restringindo quanto à existência de outra estrutura adicional nas dependências da CONTRATADA. ;

15.3. O SNOC nas dependências da CONTRATANTE não é obrigatório para os demais sítios e unidades especiais da Rede IP Governo;

15.4. Os dados gerados pela solução de segurança deverão ser exportáveis para formato compatível com as soluções de gestão mantidas pelo PRODERJ (OTRS, OCOMON, OSSIM) ou entregues sob a forma de relatórios;

15.5. Deverá possuir no mínimo, as características especificadas no item 9.2, e todos os seus subitens, deste encarte técnico, exceto aquelas que dizem respeito à desempenho (throughput, conexões simultâneas, pacotes por segundo);

15.6. A solução de segurança poderá fazer parte da solução de SD-WAN, desde que atenda integralmente os requisitos técnicos especificados neste encarte técnico;

15.7. A solução de segurança deverá ser capaz de inspecionar integramente o tráfego máximo do link de dados associado, com todas as funcionalidades de firewall, IPS e filtro de conteúdo web habilitadas;

15.8. Deverá ser realizado o gerenciamento da solução de Firewall para proteção dos circuitos da Rede IP Governo, administrando e configurando-o de forma a minimizar os incidentes de Segurança;

15.9. O Serviço de Segurança Gerenciada deve contemplar a monitoração proativa do (s) dispositivo (s) de segurança ofertado (s), pela CONTRATADA, sendo esses uma solução de segurança cujo fabricante é avaliado pelo Gartner Group, mencionado em seu quadrante mágico;

15.10. A monitoração deve ocorrer 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, durante os 365 (trezentos e sessenta e cinco) dias do ano;

15.11. Periodicamente sugerir alterações nas regras dos equipamentos de segurança, visando melhorar a proteção da rede, evitando o uso de equipamentos que estejam em End of Sale e End of Life;

15.12. Implementar novas regras nos equipamentos de segurança, em conformidade com o solicitado pela CONTRATANTE;

15.13. A solução ofertada pela CONTRATADA deverá contemplar:

15.13.1. A Análise e supervisão dos eventos de segurança;

15.13.2. A Detecção de alertas de segurança;

15.13.3. A Gestão e a resposta a incidentes de segurança;

15.13.4. Possibilidade de criação, alteração e manutenção de 50 (cinquenta) regras mensais na política de Segurança original.

15.14. Deve possuir solução de gerenciamento centralizado, possibilitando o gerenciamento de diversos equipamentos;

15.15. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança;

15.16. A CONTRATANTE deverá ter acesso irrestrito os appliances da solução de segurança de forma a realizar a correta fiscalização técnica dos serviços;

15.17. O gerenciamento deve contemplar:

15.17.1. Criação e administração de políticas de firewall;

15.17.2. Criação e administração de políticas de IPS/IDS;

15.17.3. Monitoração de logs.

15.18. Atuar pro ativamente para solucionar possíveis problemas e incidentes de segurança;

15.19. Os logs devem ser armazenados por um período mínimo de 12 (doze) meses;

15.20. A solução de segurança ofertada deverá ser capaz de gerenciar firewall (UTM ou NGFW) e IPS, com todos os recursos implementados;

15.21. A solução de gerência deverá disponibilizar para Relatórios Mensais de Segurança;

15.22. Os alertas deverão ser direcionados para o CONTRATANTE titular de cada circuito;

15.23. A solução de segurança ofertada pela CONTRATADA deverá atender aos seguintes Níveis de Serviços:

15.23.1. Prioridade 1: Indisponibilidade de componentes críticos do serviço, criação e alteração de regras: no máximo em até 2 horas;

15.23.2. Prioridade 2: Indisponibilidade parcial módulos ou componentes críticos do serviço: no máximo em até 8 horas;

15.23.3. Prioridade 3: Indisponibilidade de componentes não críticos do serviço: no máximo em até 24 horas;

15.23.4. Prioridade 4: Indisponibilidade parcial módulos ou componentes não críticos do Serviço: no máximo em até 4 dias (96 horas);

15.23.5. Prioridade 5: Requisições de logs, relatórios ou alteração de configurações e mudanças que não impactam na disponibilidade do ambiente: no máximo em até 7 dias (168 horas).

## 16. SERVIÇO DE GERÊNCIA DE REDE INTEGRADA

A CONTRATADA também deverá disponibilizar o Serviço de Gerência Integrada da Rede IP Governo, contemplando todos os links contratados, em conformidade com os seguintes requisitos:

16.1. A CONTRATADA deverá prover Solução de Gerência da Rede que contemple os módulos de gerência de falhas, desempenho, disponibilidade, relatórios, tickets e de nível de serviço para todos os lotes contratados;

16.2. O serviço de gerência de rede integrada deverá ser parte do SNOC (Security and Network Operation Center), contendo as ferramentas de hardware e software necessárias ao devido monitoramento, detecção e tratamento dos incidentes, que serão instaladas no Datacenter do PRODERJ e operadas por equipe alocada nas dependências da autarquia, com os perfis especificados no item 18 do Termo de Referência, não restringindo a existência de outra estrutura adicional nas dependências da CONTRATADA;

16.3. A CONTRATADA deverá integrar física e logicamente os serviços dos Lotes I e II de forma que se permita realizar a gestão integrada dos serviços, processos e infraestruturas disponibilizadas;

16.4. A Solução de Gerência da Rede não deverá demandar ao CONTRATANTE quaisquer custos de licenciamento para o seu funcionamento pleno;

16.5. A Solução de Gerência da Rede deverá disponibilizar a visualização de informações on-line (de forma gráfica) da rede para o acompanhamento e monitoração do estado global e detalhado do ambiente;

16.6. A Solução de Gerência da Rede da CONTRATADA deverá atuar de forma proativa, antecipando-se aos problemas na rede e garantindo o cumprimento do Acordo de Nível de Serviço (ANS), realizando abertura, acompanhamento e fechamento de chamados de falhas relacionados com indisponibilidade, operando em regime 24 horas por dia, 7 dias por semana, todos os dias do ano;

16.7. A abertura do chamado deverá ser realizada pela equipe do Serviço de Gerência de Rede da CONTRATADA, imediatamente após a constatação de defeito ou falha em qualquer circuito ou serviço que esteja em funcionamento e seja da responsabilidade da Operadora correspondente. Após a abertura do chamado, em um prazo máximo de 20 (vinte) minutos, o atendente responsável pela abertura de chamado deverá entrar em contato com técnico do CONTRATANTE, informando as providências já tomadas e a estimativa para solução do problema;

16.8. A solução de Gerência da Rede da CONTRADA deverá enviar os alertas de incidentes no mínimo via e-mail, opcionalmente via SMS de forma adicional;

16.9. A solução fornecida deve permitir acesso a todos os recursos e módulos através de única autenticação, sem a necessidade de realizar outros logins para acessar qualquer outro recurso de gerenciamento;

16.10. A Solução de Gerência da Rede deverá ser operada e administrada através de uma console única, portanto não serão aceitas soluções que possuem acessos segmentados aos módulos;

16.11. Deverá ser escalável, permitindo futuras ampliações no número de elementos de rede a serem gerenciados;

16.12. Deverá permitir acessos de usuários com perfis diferenciados com limitação de acesso a consoles, dispositivos, menus, alarmes, indicadores, etc;

16.13. Deverá permitir acesso de até 5 (cinco) usuários logados simultaneamente;

16.14. A Solução de Gerência da Rede deverá permitir a criação de grupos de perfis de acesso, que serão associados a tipos de usuários;

16.15. A Solução de Gerência da Rede deverá ser 100% web sem necessidade de instalação de clients específicos, portanto não serão aceitas soluções que não sejam nativas em WEB ou que requeiram a instalação de agentes ou plug-ins nos desktops dos colaboradores da CONTRATANTE;

16.16. O acesso deverá ser via web padrão HTTP e suportar a HTTPS, e em português, portanto não serão aceitas soluções que não possuam toda a sua estrutura em português;

16.17. A Solução de Gerência da Rede deverá ser compatível para acesso através de smartphones e tablets, portanto não serão aceitas soluções que não possuam essa compatibilidade;

16.18. A Solução de Gerência da Rede deverá ser escalável, mas transparente para a CONTRATANTE em termos de console única;

16.19. A Solução de Gerência da Rede deverá ser acessível através dos principais browsers do mercado, tais como, Internet Explorer, Firefox, Google Chrome e Safari;

16.20. Deverá permitir a exportação das informações para relatórios em formatos comerciais;

16.21. A Solução de Gerência da Rede deverá fornecer, através do portal, visualização de informações on-line (em intervalos de 5 minutos e de forma gráfica) da rede que deverá apresentar, no mínimo, os seguintes itens para cada um dos elementos monitorados:

- Topologia da rede, incluindo os roteadores CPE e seus enlaces, com visualização do estado operacional de todos os elementos da rede (enlaces e equipamentos). O estado operacional dos elementos da rede deverá ser atualizado automaticamente na Solução de Gerência da Rede, sempre que os mesmos sofrerem alterações;
- Alarmes e eventos ocorridos na rede com informações de data, hora e duração de ocorrência e identificação dos recursos gerenciados;
- Consumo de banda dos enlaces (entrada e saída) separados por dia e mês;
- Consumo de banda por classe de serviço, separados por dia e mês;
- Ocupação de memória e CPU dos roteadores CPE;
- Retardo dos enlaces separados por dia e mês;
- Perda de pacotes (descarte) no sentido IN e OUT em %;
- Taxa de pacotes com erros em erros por segundo;
- Latência em milissegundos;
- A Solução de Gerência da Rede deverá permitir a apresentação de indicadores que reflitam o nível de SLA (Service Level Agreement) e SLM (Service Level Management) dos serviços contratados;
- Inventário dos equipamentos e enlaces da rede contendo, no mínimo, as seguintes informações:
    - Enlace: designação, tecnologia e nível de serviço;
    - Roteador CPE: fabricante e modelo e configuração física (interfaces, memória, slots, dentre outros);
    - Endereçamento lógico: endereços IPs e máscaras.
- A Solução de Gerência da Rede deverá permitir adicionar a nomenclatura conhecida pelo CONTRATANTE para os recursos gerenciados.

16.22. A Solução de Gerência da Rede deverá permitir a criação de Relatórios:

- Permitir ser exportados conforme os principais métodos como: pdf, csv, pacote office;
- Relatórios de desempenho sumarizados por período específicos;
- Relatórios de desempenho classificados em uma visão TOP N;
    - Top Roteadores % de utilização de CPU
    - Top N Interfaces % de utilização

    - Top N Interfaces com descartes
    - Top N Interfaces com eventos de Latência
- Relatórios de disponibilidade com períodos específicos;
- Dashboards relacionando falhas, desempenho e disponibilidade;
- Dashboards executivos com visão sumarizada de indicadores operacionais (Pro atividade, Taxa de Reincidência, Reparos no Prazo e Taxa de Falha).

16.23. A Solução de Gerência da Rede deverá realizar registro de todas as ocorrências de alarmes/eventos em log de históricos e/ou em base de dados contendo informações de data e hora de ocorrência, identificando os recursos gerenciados;

16.24. Os dados gerados pela solução de Gerência de Rede deverão ser exportáveis para formato compatível com as soluções de gestão mantidas pelo PRODERJ (Zabbix, OTRS, OCOMON, OSSIM) ou entregues sob a forma de relatórios;

16.25. A Solução de Gerência da Rede deverá armazenar os dados por um período de 12 (doze) meses;

## 17. NÍVEIS MÍNIMOS DE SERVIÇOS (NMS) PARA A REDE IP GOVERNO

17.1. Os sítios de interesse da CONTRATANTE para a Rede IP Governo são classificados conforme os seguintes tipos:

- Sede da Rede IP Governo;
- Unidades especiais: Palácio Guanabara e Palácio das Laranjeiras;
- Demais unidades: secretarias e órgãos do Governo Estadual e outras unidades descentralizadas.

17.2. Adicionalmente, classificam-se cada sítio como básico ou crítico, sendo o primeiro com atendimento 8x5 e dias comerciais, e o segundo 24x7x365;

17.3. Cada endereço constante no Anexo I receberá uma única classificação, e a CONTRATADA deverá ter condições de atender a possível mudança quando solicitado pelo CONTRATANTE durante a vigência contratual;

17.4. Uma série de indicadores deverá ser a calculada pela CONTRATADA periodicamente como condição para pagamento dos serviços. A CONTRATADA deverá disponibilizar mensalmente ao PRODERJ, relatórios digitais com o cálculo dos indicadores, totalizados e apresentados mensalmente por enlace;

17.5. Essas métricas servirão como limiar de qualidade do serviço, compondo o que será denominado de Níveis Mínimos de Serviço (NMS);

17.6. No Termo de Referência encontram-se a definição básica destes indicadores e sua fórmula de cálculo.

### 17.7. Índice Disponibilidade Mensal do Enlace (IDM)

17.7.1. O primeiro desses indicadores será o Índice de Disponibilidade Mensal do Enlace (IDM), que deverá representar o percentual de tempo em que o serviço de conectividade à rede WAN estará operacional em um determinado período de tempo, para cada sítio da rede corporativa do Governo do Estado do Rio de Janeiro. A disponibilidade é comumente medida mensalmente através do número de minutos em que este esteve operacional no referido mês;

17.7.2. Para cumprir com o Índice de Disponibilidade, a prestadora de serviços deve trabalhar com duas variáveis principais: o MTBF (tempo médio entre falhas) da solução e o MTTR (tempo médio de reparação de falhas). Para aumentar a disponibilidade deve-se aumentar o MTBF e diminuir o MTTR, de forma que o sistema apresente falhas com menor frequência e que estas sejam recuperadas mais rapidamente;

17.7.3. Para cada sítio conectado, deverá ser garantida o Índice de Disponibilidade Mensal do Enlace (IDM) conforme os níveis a seguir.

| Nível | IDM | Sítios |
|---|---|---|
| N1 | ≥ 99,80%<br>ou<br>1h 27m 7s / mês | Core de Rede IP Governo e Unidades Especiais |
| N2 | ≥ 99,30%<br>ou<br>5hs 4m 55s / mês | Demais Unidades pertencentes à Região Metropolitana do Estado |
| N3 | ≥ 99,03%<br>ou<br>7hs 2m 31s / mês | Demais Unidades pertencentes à Região Interior do Estado |

Tabela 1 – Índice de Disponibilidade Mensal (IDM) de cada Enlace

17.8. **Taxa de Erro de Bit (TxErr)**

Para Rede IP Governo a TxErr será medida da Taxa de Erro da conexão de acesso ao Backbone IP MPLS da CONTRATADA.

| Nível | TxErr | Tipo de Acesso |
|---|---|---|
| N1 | $\leq 10^{-7}$ | Fibra Ótica e Rádio Terrestre |
| N2 | $\leq 10^{-6}$ | Par metálico e Acesso Satélite |

Tabela 2 – Taxa de Erro de Bit (TxErr)

17.9. **Taxa de Perda de Pacotes (TPP)**

Para Rede IP Governo a Taxa de Perda de Pacotes deverá ser menor ou igual a 2% para qualquer tipo de acesso.

A perda de pacote do Backbone IP do Núcleo do Backbone IP da CONTRATADA deverá ser menor que 1%.

17.10. **Tempo de Retardo (RTT)**

Para Rede IP Governo a Taxa o Tempo de Retardo deverá atender para os limiares abaixo conforme o tipo de acesso.

| Nível | RTT | Sítios |
|---|---|---|
| N1 | ≤ 100ms | Fibra Ótica, Rádio Terrestre e Par Metálico |
| N2 | ≤ 1000ms | Acesso Satélite |

Tabela 3 – Tempo de Retardo (RTT)

17.11. **Prazo de Reparo (PR)**

Para Rede IP Governo o Prazo de Reparo deverá atender para os limiares abaixo.

| Nível | PR | Sítios |
|---|---|---|
| N1 | ≤ 2 horas | Core de Rede IP Governo e Unidades Especiais |
| N2 | ≤ 5 horas | Demais Unidades pertencentes à Região Metropolitana do Estado |
| N3 | ≤ 7 horas | Demais Unidades pertencentes à Região Interior do Estado |

Tabela 4 – Prazo de Reparo (PR)

17.12. **Prazo de Alteração de Configuração dos Serviços (PAC)**

Para Rede IP Governo o prazo de Alteração de Configuração dos Serviços deverá atender para os limiares conforme abaixo.

| Nível | PAC | Complexidade |
|---|---|---|
| N1 | ≤ 72 horas | Baixa |
| N2 | ≤ 10 dias | Média |
| N3 | ≤ 60 dias | Alta |

Tabela 5 – Prazo de Alteração de Configuração dos Serviços (PAC)

17.13. **Prazo de Alteração da Taxa de Transmissão de um Enlace (PAT)**

Para Rede IP Governo o prazo de Alteração de Taxa de Transmissão de um Enlace.

| Nível | PAT | Sítios |
|---|---|---|
| N1 | ≤ 30 dias | Core de Rede IP Governo e Unidades Especiais |
| N2 | ≤ 60 dias | Demais Unidades pertencentes à Região Metropolitana e Interior do Estado |

Tabela 6 – Prazo de Alteração de Transmissão (PAT)

17.14. **Prazo de Atendimento a Novos Endereços (PAN)**

17.14.1. Para Rede IP Governo o prazo de Atendimento a Novos Endereços será de 60 dias;

17.14.2. As métricas apresentadas neste item servirão de base para avaliação e verificação da qualidade dos serviços prestados pela CONTRATADA.

## 18. REQUISITOS DO SERVIÇO DE SUPORTE TÉCNICO

18.1. A CONTRATADA deverá disponibilizar um número único nacional não tarifado (0800) para abertura de chamados de suporte técnico, como também o Serviço de Gerência fornecido pela CONTRATADA deverá ser capaz de gerenciar os níveis de serviços acordados;

18.2. A assistência técnica on-site deverá ser prestada nas instalações do CONTRATANTE conforme os prazos estipulados nos Níveis Mínimos de Serviço (NMS);

18.3. No momento de abertura do chamado deverá ser fornecido ao CONTRATANTE um número único de identificação do chamado;

18.4. Os chamados somente poderão ser abertos e fechados após autorização do CONTRATANTE;

18.5. Os serviços de suporte técnico deverão incluir serviços de atualização dos Equipamentos componentes da solução ofertada, sendo responsáveis pelo fornecimento de patches, correções e novas versões de software de Equipamentos;

18.6. A CONTRATADA deverá disponibilizar, ainda, um número de telefone ao CONTRATANTE para contato com a área de 2º nível para solução de problemas urgentes que necessitem a atuação imediata, tais como: reinício de interfaces de roteadores, conferência de aplicação de políticas nos roteadores, lista de acesso, ativação de modo debug de forma temporário para diagnóstico, verificação de logs, configuração de velocidade e modo de operação de interfaces, elaboração de listas de acesso temporárias e reinício de equipamentos;

18.7. O CONTRATANTE reserva-se o direito de promover, a qualquer tempo, alterações nas políticas de utilização do serviço de acesso à Internet, ficando a CONTRATADA, neste caso, obrigada a prestar o suporte técnico necessário à implementação dessas diretrizes nos equipamentos por ela empregados na prestação os serviços, inclusive nos roteadores locados, sem prejuízo das condições de funcionamento previstas no edital;

18.8. Durante a vigência do contrato, a CONTRATADA deverá responder, por escrito, no prazo máximo de 5 (cinco) dias úteis, a quaisquer esclarecimentos de ordem técnica pertinentes à execução dos serviços, que venham porventura ser solicitados pelo CONTRATANTE;

18.9. Em caso de reiterado inadimplemento do SLA, o CONTRATANTE poderá, concomitantemente à multa, aplicar sanção de advertência ou outras sanções previstas no contrato;

18.10. Durante a vigência do contrato, a CONTRATADA deverá manter preposto aceito pela Administração do CONTRATANTE para representá-la administrativamente sempre que houver necessidade.

## 19. REQUISITOS DE GERENCIAMENTO DOS SERVIÇOS

19.1. Mensalmente, a CONTRATADA deverá encaminhar ao CONTRATANTE relatório com todos os chamados de suporte técnicos abertos / fechados, com a identificação do chamado, data e hora de abertura, nome da pessoa que abriu e do técnico alocado, bem como as atividades executadas, data e hora de fechamento do chamado e resolução aplicada;

19.2. O relatório deverá ser enviado juntamente com a fatura de prestação dos serviços e deverá apresentar informações acerca da aferição dos níveis de serviço contratados, como descrição dos períodos de indisponibilidade, para cada um dos acessos contratados;

19.3. Os relatórios deverão ser detalhados dia, período e causas de eventuais indisponibilidades de serviço ocorridas, bem como o somatório total de minutos de todas as ocorrências e o cálculo do Índice de Disponibilidade Mensal (D) correspondente ao período de faturamento;

19.4. A entrega dos relatórios mensais é condição necessária à atestação dos serviços, pelo CONTRATANTE, para fins de pagamento;

19.5. Caso o Índice de Disponibilidade Mensal, seja inferior ao especificado neste Termo de Referência, a CONTRATADA deverá encaminhar relatório com o cálculo do total de desconto a ser aplicado no valor da fatura, de acordo com a seguinte fórmula:

$$VD = CM * [(100 - D) / 100],$$

Onde:

VD é o valor do desconto;

CM é o custo mensal dos serviços prestados;

D é o índice de disponibilidade mensal dos serviços, calculado pelas fórmulas especificadas nos Níveis Mínimos de Serviço (NMS)