Governo do Estado de Mato Grosso
SEPLAG - Secretaria de Estado de Planejamento e Gestão
Secretaria Adjunta de Administração Sistêmica
Superintendência de Tecnologia da Informação Setorial

TERMO DE REFERÊNCIA	
I – INFORMAÇÕES PRIMÁRIAS SOBRE A DESPESA	
1 – ÓRGÃO: SEPLAG	**2 – TERMO DE REFERÊNCIA nº 05/2020/SUTIS/SAAS/SEPLAG**
3 – Número da Unidade Orçamentária: **( ) SEPLAG – 11.101** **(x) FUNDESP – 11.601**	**4 – Descrição de Categoria de Investimento:** **( ) Capacitação** **( ) Equipamento de Apoio** **(X) Equipamento de TI** **( ) Consultoria/Auditoria/Assessoria** **( ) Despesa de Custeio** **( ) Bens Permanente** **( ) Serviços**
5 – Unidade Administrativa Solicitante: Superintendência de Tecnologia da Informação Setorial/SAAS/SEPLAG	

II – FUNDAMENTAÇÃO MÍNIMA PARA CONTRATAÇÃO DE SERVIÇOS

1. OBJETO

Aquisição de equipamentos de switches e fibra ótica para interligação dos racks.

2. DESCRIÇÃO DOS ITENS E QUANTIDADE

LOTE 1 -SOLUÇÃO DE ATIVOS DE REDE E SOFTWARE						
ITEM	**QTDE.**	**UNID.**	**DESCRIÇÃO**	**SIAG**	**PREÇO UNITÁRIO R$**	**TOTAL PARCIAL R$**
1	**EQUIPAMENTOS**					
1.1	18	pç	Switches de acesso Tipo I - 48 portas 10/100/1000 Base-T POE+ + 4 Portas 10Gbe SFP+	1096040	R$ 40.800,02	R$ 734.400,30
1.2	18	pç	Switche de acesso Tipo II - 48 portas 10/100/1000 Base-T + 4 Portas 10Gbe SFP+	1096041	R$ 29.795,97	R$ 536.327,46
1.3	05	pç	Switches de acesso Tipo III - 24 portas 10/100/1000 Base-T POE+ + 4 Portas 10Gbe SFP+	1096042	R$ 30.710,84	R$ 153.554,18
1.4	02	pç	Switche de acesso Tipo IV - 24 portas 10/100/1000 Base-T + 4 Portas 10Gbe SFP+	1096043	R$ 24.676,23	R$ 49.352,47
1.5	02	pç	Switche Core de Rede Tipo I - 48 portas 10/25 Gbps SFP28 portas, 7 portas QSFP 28	1096044	R$ 142.712,63	R$ 285.425,27

1.6	01	pç	Switche Core de Rede Tipo II - 12 portas 1/10 Gbps SFP+ e 12 portas 1/10 Gbps RJ45	1096045	R$ 101.781,75	R$ 101.781,75
1.7	02	pç	Switche Core de Rede Tipo III - 48 portas 10/100/1000BASE-T + 2 Portas 25 gigas SPF28	1096046	R$ 109.302,49	R$ 218.604,99
1.8	01	pç	Controladora de rede Wireless	1095442	R$ 45.386,48	R$ 45.386,48
1.9	60	pç	Access Point 802.11 ax/ac/abgn 4x4:4 MIMO	1095443	R$ 7.463,53	R$ 447.812,00
1.10	42	pç	Módulo Transceiver SFP+ 10GBASE-SR para switch de acesso	1096047	R$ 1.736,06	R$ 72.914,66
1.11	108	pç	Módulo Transceiver SFP+ 10GBASE-SR para switch core	1096048	R$ 1.656,74	R$ 178.927,92
1.12	06	pç	Módulo Transceiver SFP+ 10GBASE-LR para switch de acesso	1096049	R$ 3.166,27	R$ 18.997,60
1.13	10	pç	Módulo Transceiver SFP+ 10GBASE-LR para switch core	1096050	R$ 3.215,75	R$ 32.157,50
1.14	255	pç	Cabo de empilhamento 10 G para switch de acesso	1096055	R$ 171,53	R$ 4.288,33
1.15	02	pç	Cabo de empilhamento 100 G para switch de core	1096056	R$ 2.235,87	R$ 4.471,73
1.16	04	pç	Cabo DAC 25 G para switch de core	1096057	R$ 1.471,17	R$ 5.884,69
1.17	01	sw	Software de gerenciamento de rede	1096058	R$ 153.781,97	R$ 153.781,97
1.18	01	sw	Software de gerenciamento de controle de acesso em rede	1096059	R$ 100.147,02	R$ 100.147,02
1.19	01	sw	Software de análise de aplicações	1096060	R$ 100.147,02	R$ 100.147,02
1.20	42	srv	Serviço especializado para instalação, ativação e teste de switches de acesso	1096077	R$ 1.289,20	R$ 54.146,54
1.21	05	srv	Serviço especializado para instalação, ativação e teste de switches de core	1096076	R$ 5.610,60	R$ 28.053,02
1.22	60	srv	Serviço especializado para instalação, ativação e teste de rede Wireless	1096075	R$ 356,31	R$ 21.378,40
1.23	01	srv	Serviço especializado para instalação, ativação e teste de software de gerenciamento	1096074	R$ 13.760,83	R$ 13.760,83

1.23	01	srv	Serviço especializado para instalação, ativação e teste de software de controle de acesso na rede	1096073	R$ 8.607,48	R$ 8.607,48
1.24	01	srv	Serviço especializado para instalação, ativação e teste de software de análise de aplicações	1096061	R$ 8.833,85	R$ 8.833,85
1.25	04	srv	Treinamento	1096079	R$ 7.163,35	R$ 28.653,40
VALOR GLOBAL						**R$ 3.413.990,94**

LOTE 2 – SERVIÇO DE INFRAESTRUTURA DE REDE						
ITEM	**QTD.**	**UND.**	**DESCRIÇÃO**	**SIAG**	**PREÇO UNITÁRIO R$**	**TOTAL PARCIAL R$**
	SERVIÇOS					
1.1	09	srv	Serviços de interligação de racks por link de fibra óptica ao data center, com os materiais aplicados, conforme descrito neste termo.	1096078	R$ 18.599,67	R$ 167.397,00
1.2	12	pç	Cordão Duplex Conectorizado SM LC-SPC/LC-SPC 2.5M	1096051	R$ 119,51	R$ 1.434,12
1.3	05	pç	Cordão Duplex Conectorizado MM (50.0) LC-SPC/LC-SPC 30.0M	1096052	R$ 514,28	R$ 2.571,42
1.4	03	pç	Cordão Duplex Conectorizado SM LC-SPC/LC-SPC 30.0M	1096053	R$ 626,67	R$ 1.880,00
1.5	54	pç	Cordão Duplex Conectorizado MM (50.0) OM3 10 Gigabit LC-UPC/LC-UPC 2.5M - Acqua (A - B)	1096054	R$ 137,32	R$ 7.415,10
VALOR GLOBAL						**R$ 180.697,64**

TOTAL GERAL: R$ 3.594.688,57

3. JUSTIFICATIVA DA AQUISIÇÃO

Esse projeto para aquisições dos equipamentos de switches se faz necessário devido a defasagem de equipamento que temos em nosso parque da Secretaria, pois temos equipamentos que foram comprados no ano de 2009 e contanto com todo esse tempo já passado, esses equipamentos estão totalmente obsoletos e sem suporte do fabricante. Devido a isso estamos enfrentando problemas recorrentes em algumas pilhas de Switches que param de funcionar fazendo com que os usuários fiquem sem conexão em suas estações de trabalho. Além dessa defasagem de equipamentos, temos outro problema que se deu devido a fusão entre as secretárias que são diferentes fabricantes

de switches que havia no Parque de Switches da antiga Seplan. Neste parque há HP, 3com e Allied, portanto a falta de homogeneidade de tecnologias faz com que as configurações de segurança da rede de computadores se tornaram comprometida.

4. DA PARTICIPAÇÃO

4.1. Participação de Microempresa, Empresa de Pequeno Porte e Microempreendedor Individual:

4.1.1. Justifica-se a **não reserva de cotas** nos termos estabelecidos no art. 48, inciso III, da Lei nº 123/2006 alterada pela Lei nº 147/2014, tendo em vista que o objeto envolve contratação de serviços, e o referido dispositivo impõe o tratamento diferenciado apenas quanto à aquisição de bens de natureza divisível;

4.2. Condições de Participação – das Cooperativas e dos Consórcios:

4.2.1. **NÃO será admitida nesta licitação a participação de cooperativas**, uma vez que vedada a participação de cooperativas em procedimento licitatório para os casos em que o objeto social destas seja incompatível com o objeto do certame respectivo (Acórdão-TCU 22/2003), bem como é irregular a participação de cooperativa em procedimentos licitatórios quando o objeto refoge ao seu campo de atuação. (Acórdão-TCU 6.552/2009);

4.2.2. **Não será permitida a participação de consórcios**, pois não se trata de objeto complexo e de grandes dimensões. E, dadas as características do mercado, as empresas podem, de forma isolada, participar da licitação, atender às condições e os requisitos de habilitação previstos neste Termo de Referência, e posteriormente fornecer o objeto. A vedação à participação de consórcio, nesta situação, não acarretará prejuízo à competitividade do certame, e facilitará a análise dos documentos de habilitação, que certamente são mais complexos em se tratando de empresas reunidas em consórcio. Conforme Acórdãos 1.094/2004-TCU e 1.165/2012-TCU, ambos do Plenário, a formação de consórcio, em regra, é admitida quando o objeto a ser licitado envolve questões de alta complexidade ou de relevante vulto, em que empresas, isoladamente, não teriam condições de suprir os requisitos de habilitação do edital, ficando o administrador obrigado a prever a participação de consórcios no certame com vistas à ampliação da competitividade e à obtenção da proposta mais vantajosa. [...]
Quanto à admissão de consórcios em certames licitatórios, convém transcrever análise constante do relatório do Ministro Relator Marcos Bemquerer na Decisão 480/2002-TCU-Plenário:

> 'Em regra, o consórcio não é favorecido ou incentivado em nosso Direito. Como instrumento de atuação empresarial, o consórcio pode conduzir a resultados indesejáveis. A formação de consórcios acarreta risco da dominação do mercado, através de pactos de eliminação de competição entre os empresários. No campo das licitações, a formação de consórcios pode reduzir o universo da disputa. O consórcio poderia retratar uma composição entre eventuais interessados: em vez de estabelecerem disputa entre si, formalizariam acordo para eliminar a competição. Mas o consórcio também pode prestar-se a resultados positivos e compatíveis com a ordem jurídica. Há hipóteses em que as circunstâncias de mercado e (ou) a complexidade do objeto torna problemática a competição. Isso se passa quando grande quantidade de empresas, isoladamente, não dispuser de condições para participar da licitação. Nesse caso, o instituto do consórcio é a via adequada para propiciar ampliação do universo de licitantes. É usual que a administração pública apenas autorize a participação de empresas em consórcio quando as dimensões e complexidade do objeto ou as circunstâncias concretas exijam a associação entre particulares' (Marçal Justen Filho, 'Comentários à Lei de Licitação e Contratos Administrativos', 8ª Edição, pags. 369/370).

Ademais, os Acórdãos nº 1.305/2013 – TCU – Plenário, nº 1.636/2007 - TCU – Plenário e nº 566/2006 - TCU - Plenário, são no sentido de que a permissão de empresas participarem da licitação pública reunidas em consórcio recai na discricionariedade da Administração.

Nesse sentido, merece destaque o posicionamento de Jessé Torres Pereira Junior, o qual, fazendo menção ao entendimento do Tribunal de Contas da União sobre a matéria, assim se manifesta:

> "(...)
>
> Averbe-se a orientação do Tribunal de Contas da União:
>
> Ademais, a participação de consórcios em torneios licitatórios não garante aumento de competitividade, consoante arestos do relatório e voto que impulsionaram o Acórdão n° 2.813/2004-1ª Câmara, que reproduzo: "O art. 33 da Lei de Licitações expressamente atribui a Administração a prerrogativa de admitir a participação de consórcios. Está, portanto, no âmbito da discricionariedade da Administração. Isto porque a formação de consórcios tanto pode se prestar para fomentar a concorrência (consórcio de empresas menores que, de outra forma, não participariam do certame), quanto cerceá-la (associação de empresas que, em caso contrário, concorreriam entre si) (...) vemos que é praticamente comum a não aceitação de consórcios (...)" (Comentários à Lei de Licitações e Contratações da Administração Pública". 7º edição. Ed. Renovar. 2007. Páginas 442 a 443.)

5. DO JULGAMENTO E COMPOSIÇÃO DA PROPOSTA DE PREÇOS

5.1. O Julgamento visará o **MENOR PREÇO GLOBAL POR LOTE.**

5.1.1. Consistirá em 02 (dois) LOTES, com cotações de valor unitário e valor total para as quantidades solicitadas, conforme item 02 deste Termo de Referência.

5.1.2. O valor unitário ofertado, pós fase de lances (proposta realinhada), não poderá ser superior em relação ao valor unitário ofertado inicialmente pela Licitante (proposta inicial), tão pouco ser maior que o valor unitário estimado para licitação.

5.2. A proposta da licitante deverá conter:

5.2.1. CNPJ/MF, endereço completo e telefone para contato, endereço eletrônico (e-mail), nº da conta corrente, agência e respectivo Banco, e assinatura do representante legal da empresa.

5.2.2. O prazo de eficácia da proposta, que não poderá ser inferior a 60 (sessenta) dias corridos, a contar da data da apresentação da proposta realinhada, prazo este que será suspenso caso haja recursos administrativos ou judiciais.

5.2.3. Preços unitários e totais

5.2.4. As propostas apresentadas pelas licitantes deverão incluir todos os custos e despesas, tais como: custos diretos e indiretos, tributos incidentes, materiais, equipamentos, encargos trabalhistas, previdenciários, fiscais, comerciais, fretes, seguros, serviços, treinamento, deslocamentos de pessoal, transporte, garantia, lucro e quaisquer outros que incidam ou venham a incidir sobre o valor do objeto licitado, constante da proposta, conforme exigências editalícias e contratuais, não sendo admitido pleito posterior em decorrência da exclusão de quaisquer despesas incorridas.

6. DA HABILITAÇÃO

6.1. Licitante deverá apresentar, a título de habilitação, os documentos relativos à Habilitação Jurídica (Art.28), a Regularidade Fiscal e Trabalhista (Art.29) e a Qualificação econômico-financeira (Art.31) previstos na Lei nº 8.666/93, que poderão ser substituídos pelo Certificado de Registro Cadastral vigente na SEPLAG/MT, além dos relacionados na sequência:

6.2. Quanto à **qualificação técnica**, a licitante deverá apresentar:

6.2.1. A empresa licitante deverá comprovar que possui registro da empresa no Conselho Regional de Engenharia e Agronomia - CREA (Registro ou Inscrição na Entidade Profissional Competente - Inciso I, Art. 30, Lei nº 8.666/93), com apresentação de atestado de capacitação técnica;

6.2.2. A empresa licitante deverá comprovar que possui em seu quadro técnico, na data da licitação, profissionais de nível superior que sejam responsáveis técnicos pela empresa, devidamente

registrados junto ao CREA, a saber: 01 Engenheiro Eletricista que possua a atribuição do Artigo 9º da Resolução n. 218/73 do CONFEA ou Engenheiro de Computação ou Eng. de Telecomunicações, que possua especialização em engenharia de segurança no trabalho.

6.2.3. A empresa licitante deverá comprovar, mediante atestados de capacidade técnica emitidos em nome da empresa licitante, por entidades da Administração Federal, Estadual ou Municipal, direta ou indireta, e/ou empresa privada, lavrado(s) e assinado(s) por servidor/funcionário competente do respectivo órgão ou empresa, devidamente registrado(s) junto ao CREA, que comprove que a empresa e o seu responsável técnico tenham executado serviços compatíveis com o objeto, será considerado como compatível serviços executados em um único cliente base, contendo no mínimo:

6.2.4. Instalação equipamentos ativos de rede (switches de acesso), com no mínimo 400 (quatrocentas) portas 10/100/1000.

6.2.5. Instalação equipamentos ativos de rede (switches core), com portas 10 gigas SFP+.

6.2.6. Instalação de software de gerenciamento de ativos de rede.

6.2.7. Instalação de equipamentos ativos de rede (controladora wireless e access point - AP's), com no mínimo uma controladora e 30 AP's;

6.2.8. O Atestado de capacidade técnica deverá vir acompanhando de Certidão de Acervo Técnico – CAT comprovando que os serviços indicados no(s) atestado(s) consta(m) efetivamente do acervo técnico do profissional apresentado como responsável técnico.

6.2.9. A empresa licitante deverá comprovar que possui em seu quadro técnico permanente, na data da licitação, ao menos 01 (um) profissional com certificado de treinamentos válidos e que atendam a norma regulamentadora, de NR10 - Segurança em Instalações e Serviços em Eletricidade.

7. DA PROPOSTA DE PREÇO

7.1. A empresa licitante deverá entregar junto com sua proposta, planilha onde demonstre o atendimento ponto a ponto de todas especificações técnicas dos equipamentos/acessórios apresentadas neste termo de referência, indicando as respectivas páginas que se encontra a comprovação podendo ser estes documentos ser: datasheet, folders, prospectos ou qualquer tipo de documento oficial do fabricante da solução, tais documentos deverão ser anexados obrigatoriamente junto com a planilha e deverá apresentar os partnumber/modelos/fabricante dos equipamentos ofertados.

7.2. Todas as características técnicas obrigatórias deverão ser comprovadas por meio de folders, catálogos, manuais, guias de instalação, informações da interface de gerência da solução e impressão de páginas do fabricante na Internet;

7.3. Apresentação de documento denominado "Atendimento às Especificações" para demonstrar o atendimento ponto-a-ponto dos itens e subitens obrigatórios constantes deste Termo de Referência;

7.4. No documento "Atendimento às Especificações", deverá estar indicada a localização exata da informação que garante o atendimento ao item e subitem, explicitando o documento/página; A informação deverá estar grifada para melhor visualização.

8. DOS PRAZOS, FORMA E LOCAIS DE ENTREGA

8.1. DO PRAZO E HORÁRIOS DE ENTREGA

8.1.1. A empresa contratada se obriga ao fornecimento dos produtos solicitados e empenhados, nos moldes do Termo de Referência, no prazo máximo de 15 (quinze) dias úteis, prorrogáveis por igual período com a devida justificativa, segundo a solicitação da mesma;

8.1.2. A solicitação de entrega dos equipamentos será feita pela Secretaria de Estado de Planejamento e Gestão à empresa CONTRATADA, após assinatura do Contrato, mediante Ordem de Serviço;

8.1.3. Os equipamentos deverão ser novos e sem uso. Não serão aceitos equipamentos usados, remanufaturados ou de demonstração; Os equipamentos deverão ser entregues nas caixas lacradas pelo fabricante, não sendo aceitos equipamentos com caixas violadas;

8.1.4. Este órgão poderá efetuar consulta do número de série do equipamento, junto ao fabricante,

8.1.5. Este órgão também poderá efetuar consulta junto aos órgãos competentes para certificar a legalidade do processo de importação;

8.1.6. A CONTRATADA será responsável, nos casos aplicáveis, pela aprovação de projetos de construção de infraestrutura, ou de instalação de cabos, junto a Prefeitura e a outros órgãos públicos em cada demanda solicitada pelo CONTRATANTE e pela obtenção de licenças de construção e de autorizações para utilização de infraestrutura de terceiros (Ex: Rede Cemat/Energisa) se aplicáveis, como postes, servidões, entre outros, sendo que em caso de eventuais taxas decorrentes destes serviços, ficará a cargo do CONTRATANTE, estes valores.

8.1.6.1. A execução de atividade que implique em gerar a indisponibilidade do ambiente tecnológico deverá ser feita, preferencialmente, a critério do CONTRATANTE, em horários fora de expediente normal ou de menor fluxo de utilização (ex: madrugadas, sábados, domingos e feriados);

8.1.7. A CONTRATADA não poderá executar qualquer espécie de serviços que não estejam descritos no detalhamento técnico e sem que haja a autorização da equipe técnica do contratante por escrito, sob pena de não ser ressarcida.

8.1.8. Havendo causa impeditiva para o cumprimento dos prazos, a Contratada deverá apresentar ao Contratante justificativa por escrito ao Fiscal do Contrato indicando o prazo necessário para entrega, que por sua vez analisará e tomará as necessárias providências para a aceitação ou não das justificativas apresentadas.

8.1.8.1. A justificativa para eventual atraso, só será considerada em casos fortuitos ou de força maior, devendo ser apresentada por escrito, até 24 (vinte e quatro) horas antes do término do prazo para a entrega do produto, quando o caso fortuito e de força maior ocorrer nesse lapso de 24 (vinte e quatro horas);

8.2. DO LOCAL DE EXECUÇÃO DOS SERVIÇOS

8.2.1. Os equipamentos serão entregues à Secretaria de Estado de Planejamento e Gestão – SEPLAG – Centro Político Administrativo – Palácio Paiaguás – Cuiabá – MT – CEP: 78.050-970 na Gerência de Patrimônio e Materiais;

8.3. CONDIÇÕES DE PARTICIPAÇÃO E REALIZAÇÃO DOS SERVIÇOS

8.3.1. A solução deverá ser constituída dos equipamentos relacionados nos itens deste grupo (lote), sendo todos de um mesmo fabricante, garantindo a entrega e execução dos serviços por uma única empresa e a total compatibilidade entre eles;

8.3.2. A escolha do agrupamento dos itens em grupo visa a plena qualificação da empresa fornecedora que prestará os serviços de fornecimento, bem como prestará os serviços de suporte durante a vigência do contrato de garantia dos equipamentos, a total compatibilidade entre os equipamentos solicitados, a redução de custos operacionais e de infraestrutura física, a capacidade técnica de manter a solução em operação, os recursos humanos disponíveis para prestarem o devido apoio, treinamento e curva de aprendizagem e o custo total de propriedade

8.4. COMUNICAÇÃO ENTRE CONTRATANTE E CONTRATADA

8.4.1. A presente contratação prevê a realização de reuniões formais entre a CONTRATADA e o CONTRATANTE para que seja feito o acompanhamento dos serviços e do andamento da Ordem de Serviço emitida ou a ser emitida.

8.4.2. Reuniões extraordinárias de acompanhamento poderão ser realizadas a qualquer tempo, desde que convocadas pelo Fiscal Técnico ou Gestor do Contrato com antecedência mínima de 24 horas.

8.4.3. É responsabilidade da CONTRATADA apresentar sugestões de medidas corretivas visando estabelecimento ou reestabelecimento do nível de serviço previsto neste contrato. As propostas apresentadas pela Contratada serão discutidas e avaliadas pelo CONTRATANTE, podendo a mesma solicitar alterações e/ou esclarecimentos.

8.4.4. Ao término da reunião, o CONTRATANTE gerará uma ata da reunião onde devem constar os principais assuntos tratados, as decisões tomadas e as notificações realizadas.

8.4.4.1. A ata da reunião deve ser assinada pelos presentes e juntada aos autos do processo de fiscalização do contrato.

8.4.5. O CONTRATANTE pode utilizar-se de outros mecanismos formais de comunicação com a CONTRATADA, que serão juntados ao processo de fiscalização, de modo que haja rastreabilidade dos fatos ocorridos ao longo da vigência do contrato.

8.4.6. Na execução do contrato as metas definidas podem, motivadamente, serem flexibilizadas por acordo das partes, com vista a adaptar-se as possíveis mudanças de cenário do CONTRATANTE.

8.4.7. DO PREPOSTO DA CONTRATADA

8.4.7.1. A Contratada manterá, durante todo o período de vigência do Contrato, um Preposto, com fins de representá-la administrativamente, sempre que necessário, devendo indicá-lo mediante declaração específica, na qual constarão todos os dados necessários, tais como nome completo, número de identidade e do CPF, endereço, telefones comercial e de celular, além dos dados relacionados à sua qualificação profissional, entre outros.

8.4.7.2. O Preposto deverá estar apto a esclarecer as questões relacionadas às faturas dos serviços executados.

8.4.7.3. A Contratada orientará seu Preposto quanto à necessidade de acatar as orientações do Contratante, inclusive quanto ao cumprimento das Normas Internas e de Segurança e Medicina do Trabalho.

8.4.7.4. O Preposto designado não necessitará permanecer em tempo integral à disposição do Contratante, devendo, contudo, serem observadas todas as exigências relativas à sua vinculação ao Contrato

8.4.7.5. A Contratada deverá instruir seu Preposto quanto à necessidade de atender prontamente a quaisquer solicitações do Contratante, por intermédio da Fiscalização do Contratante ou de seu substituto, acatando imediatamente as determinações, instruções e orientações destes, inclusive quanto ao cumprimento das normas internas, desde que de acordo com a legalidade, e devendo, ainda, tomar todas as providências pertinentes para que sejam corrigidas quaisquer falhas detectadas na execução dos serviços objeto do Contrato.

8.4.7.6. São atribuições do Preposto, dentre outras:

a) Comandar, coordenar e controlar a execução dos serviços contratados

b) Zelar pela segurança dos empregados responsáveis pela entrega do serviço ao Contratante;

c) Cumprir e fazer cumprir todas as determinações, instruções e orientações emanadas da Fiscalização e das autoridades do Contratante;

d) Apresentar informações e/ou documentação solicitada pela Fiscalização e/ou pelas autoridades do Contratante, inerentes à execução e às obrigações contratuais, em tempo hábil;

e) Reportar-se à Fiscalização do Contratante para dirimir quaisquer dúvidas a respeito da execução dos serviços e das demais obrigações contratuais;

f) Relatar à Fiscalização, pronta e imediatamente, por escrito, toda e qualquer irregularidade observada;

g) Encaminhar à Fiscalização do Contratante todas as Notas Fiscais/Faturas dos serviços executados, bem como toda a documentação complementar exigida

g.1) Esclarecer quaisquer questões relacionadas às Notas Fiscais/Faturas ou de qualquer outra documentação encaminhada, sempre que solicitado;

h) Administrar todo e qualquer assunto relativo aos empregados da Contratada, respondendo perante ao Contratante por todos os atos e fatos gerados ou provocados por eles.

8.5. DA SUBCONTRATAÇÃO

8.5.1. Nos termos do art. 72, da Lei nº 8.666/93, a CONTRATADA não poderá subcontratar quaisquer partes do serviço a serem desenvolvidos.

9. DO CONTRATO

9.1. Após a homologação da licitação, a Adjudicatária terá o prazo de 03 (três) dias úteis, contados a partir da data de sua convocação formal pelo Órgão/Entidade Contratante, para assinar o Contrato, sob pena de decair o direito à contratação, sem prejuízo das sanções previstas no Termo de Referência.

9.1.1. O prazo previsto no subitem anterior poderá ser prorrogado, por igual período, por solicitação justificada da Adjudicatária e aceita pela Administração.

9.2. O prazo da contratação será de 12 (doze) meses contados a partir da assinatura do contrato, adstrito à vigência dos respectivos créditos orçamentários, podendo ser aditado, conforme prevê a Lei nº 8.666/93.

9.3. A licitante vencedora deverá apresentar no ato da assinatura do Contrato:

a) Preposto, indicar o responsável pela comunicação entre o Contratante e a Contratada.

10. DA GARANTIA CONTRATUAL

10.1. A CONTRATADA deverá apresentar ao CONTRATANTE, no prazo máximo de 10 (dez) dias úteis, contado da data do protocolo de entrega da via do contrato assinada, comprovante de prestação de garantia correspondente ao percentual de 5% (cinco por cento) do valor do Contrato, em conformidade com o parágrafo 1º do artigo 56 da Lei Federal nº 8.666/93, com a mesma vigência contratual do referido item, podendo optar por caução em dinheiro, seguro-garantia ou fiança bancária.

a) Caução em dinheiro ou títulos da dívida pública, sendo estes emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil e avaliados pelos seus credores econômicos, definido pelo Ministério da Fazenda, conforme orientação técnica n. 040/2010/AGE;

a1) A garantia em apreço, quando em dinheiro, deverá ser efetuado o recolhimento de DAR (Documento de Arrecadação). Para a emissão do referido documento, deve-se realizar o seguinte procedimento:

1. Acessar site da SEFAZ, no endereço http://www.sefaz.mt.gov.br;
2. Na aba Serviços, clicar em Documentos Arrecadação, clicar em DAR-1 - Órgãos;
3. Selecionar o Órgão/Entidade Contratante e escolher o tipo de pessoa (no caso, Jurídica);
4. Preencher o Formulário para emissão do DAR:
5. Preencher os dados necessários;

a2) Após a emissão do Documento de Arrecadação (DAR), efetuar o pagamento em qualquer agência do Banco do Brasil e, em seguida, encaminhar ao Contratante, ambos documentos: as cópias do DAR e do comprovante de pagamento;

b) Seguro-garantia, modalidade "Seguro-garantia do Construtor, do Fornecedor e do Prestador de Serviço"; ou

c) Fiança bancária.

10.2. A inobservância do prazo fixado para apresentação da garantia acarretará a aplicação de multa de 0,2% (dois décimos por cento) do valor do contrato por dia de atraso, até o máximo de 5% (cinco por cento);

10.2.1. O atraso superior a 25 (vinte e cinco) dias autoriza a Administração a promover a retenção dos pagamentos devidos à Contratada, até o limite de 2% (dois por cento) do valor total do contrato, a título de garantia;

10.2.2. A retenção efetuada com base no item 12.2.1 não gera direito a nenhum tipo de compensação financeira à Contratada;

10.2.3. A Contratada, a qualquer tempo, poderá substituir a retenção efetuada com base no item 12.2.1. desta cláusula por quaisquer das modalidades de garantia, caução em dinheiro ou títulos da dívida pública, seguro-garantia ou fiança bancária;

10.3. A garantia contratual deverá ter validade durante toda a vigência do Contrato;

10.4. Caso o valor ou o prazo da garantia seja insuficiente para garantir o contrato, a contratada providenciará, compulsoriamente, tantos aditamentos quantos forem necessários até o término da vigência do contrato;

10.5. A garantia prestada pela contratada só será liberada ou restituída após o término da vigência do contrato, ou ainda na ocorrência de outras hipóteses de extinção contratual previstas em Lei.

10.6. DA GARANTIA DOS MATERIAIS

10.6.1. Os equipamentos fornecidos deverão estar cobertos por garantia do fabricante no Brasil pelo período especificado em cada item;

10.6.2. A garantia deve incluir substituição de peças decorrente de vícios de projeto, fabricação, construção e montagem, pelo período especificado no termo de referência, a contar da data de aceite provisório dos equipamentos;

10.6.3. Os softwares fornecidos deverão estar cobertos por garantia que ofereça atualizações necessárias para a correção de vícios, pelo período especificado no termo de referência, a contar da data do aceite provisório dos softwares;

10.6.4. A garantia deve incluir também envio de peças/equipamentos de reposição, que deverão ser entregues nos locais especificados neste termo de referência, ou na sua ausência, na sede da contratante, abrangendo-se todos os custos de deslocamento (envio e retorno) das peças/equipamentos de substituição. Obrigatoriamente o envio de peças/equipamentos de reposição deve ser realizado pelo fabricante dos equipamentos, sendo este responsável pelo controle e logística de peças de reposição;

10.6.5. Devem ser descritos, no momento da proposta, qual o tipo de garantia fornecida. Os equipamentos devem ter seus números seriais atrelados ao sistema de suporte do fabricante dos equipamentos com data específica de início e fim do suporte.

10.7. DA GARANTIA DOS SERVIÇOS

10.7.1. Os serviços de instalação deverão ter prazo de garantia de 03 (três) meses, contados a partir da data de aceite da execução da Ordem de Serviço.

10.7.2. A CONTRATADA deverá garantir a qualidade dos serviços executados, devendo, às suas expensas, corrigir ou refazer item de serviço concernente ao objeto deste Termo de Referência que apresentar defeito ou incorreção.

10.7.3. Durante o prazo de 03 (três) meses, contados a partir da data de aceite da Ordem de Serviço, a CONTRATADA deverá atender aos chamados e realizar a substituição de materiais defeituosos no prazo máximo de 5 (cinco) dias úteis, contados da comunicação do CONTRATANTE sem prejuízo ou ônus para ao CONTRATANTE.

11.OBRIGAÇÕES DA CONTRATANTE

O Estado de Mato Grosso, através dos Órgãos/Entidades do Poder Executivo Estadual, obriga-se a:Designar, servidor(es) ao(s) qual(is) caberá(ão) a responsabilidade de acompanhar, fiscalizar e avaliar a execução do Contrato, conforme legislação vigente;

11.2. Fornecer à Contratada todos os elementos e dados necessários à perfeita execução do objeto do Termo de Referência e do Contrato, inclusive permitindo o acesso de empregados, prepostos ou representantes da Contratada em suas dependências, desde que observadas às normas de segurança;

11.3. Emitir ordem de serviço estabelecendo dia, hora, quantidade, local e demais informações que achar pertinentes para o bom cumprimento do objeto;

11.4. Receber o objeto contratado, nos termos, prazos, quantidade, qualidade e condições estabelecidas no processo licitatório;

11.5. Rejeitar, no todo ou em parte, os serviços entregues em desacordo com as obrigações assumidas pela Contratada;

11.6. Notificar a Contratada de qualquer alteração ou irregularidade encontrada na execução do Contrato;

11.7. Após comunicação as possíveis irregularidades devem ser imediatamente corrigidas, como refazimento do serviço em que se verificarem problemas;

11.8. Inserir as informações pertinentes ao objeto contratado no sistema SIAG-C, após firmar o Contrato e/ou emitir a Nota de Empenho, em atendimento à Lei de Acesso as Informações (Lei Federal nº 12.527/11), regulamentada pelo Decreto Estadual nº 1.973/13;

11.9. Efetuar o pagamento à Contratada, nas condições estabelecidas neste Termo de Referência e em Edital;

11.9.1. Não será efetuado pagamento à empresa Contratada, enquanto pendente de liquidação qualquer obrigação. Esse fato não será gerador de direito a reajustamento de preços ou a atualização monetária.

12.DAS OBRIGAÇÕES DA CONTRATADA

12.1. Para garantir o fiel cumprimento do objeto deste, a Empresa CONTRATADA se compromete a:

12.1.1. Retirar a Nota de Empenho no prazo de 02 (dois) dias, contados do recebimento da convocação formal;

12.1.2. Manter contato com a contratante sobre quaisquer assuntos relativos aos serviços contratados, sempre por escrito, ressalvados os entendimentos verbais determinados pela urgência de cada caso;

12.1.3. A contratada deverá disponibilizar, na vigência do contrato, todas as atualizações dos softwares e firmwares dos equipamentos, concebidas em data posterior ao seu fornecimento, pelo período especificado no termo de referência, sem qualquer ônus adicional para o contratante;

12.1.4. As atualizações incluídas devem ser do tipo "minor release" e "major release", permitindo manter os equipamentos atualizados em sua última versão de software/firmware.

12.1.5.

12.1.6. Arcar com todas as despesas, diretas ou indiretas, decorrentes do cumprimento das obrigações assumidas, sem qualquer ônus para a CONTRATADA;

12.1.7. Respeitar e fazer cumprir a legislação de segurança e saúde no trabalho, previstas nas normas regulamentadoras pertinentes;

12.1.8. Fiscalizar o perfeito cumprimento da prestação a que se obrigou, cabendo-lhe, integralmente, os ônus decorrentes. Tal fiscalização dar-se-á independentemente da que será exercida pela Secretaria de Estado de Planejamento e Gestão;

12.1.9. Comunicar imediatamente à SEPLAG qualquer alteração ocorrida no endereço, conta bancária e outros julgáveis necessários para o recebimento de correspondência;

12.1.10. Efetuar a imediata correção das deficiências apontadas pela SEPLAG, com relação aos bens adquiridos;

12.1.11. Executar a prestação, de acordo com a solicitação da SEPLAG, obedecendo a proposta apresentada, dentro dos padrões estabelecidos, de acordo com as especificações do Termo de Referência e da proposta de preço apresentada, responsabilizando-se por eventuais prejuízos decorrentes do descumprimento de condição estabelecida, obedecendo a proposta apresentada, responsabilizando-se por eventuais prejuízos decorrentes do descumprimento de qualquer cláusula ou condição aqui estabelecida;

12.1.12. Prestar os esclarecimentos que forem solicitados pela SEPLAG, cujas reclamações se obrigam a atender prontamente, bem como dar ciência a Defensoria, imediatamente, por escrito, de qualquer anormalidade que verificar quando do objeto adquirido;

12.1.13. Dispor-se a toda e qualquer fiscalização da SEPLAG, no tocante ao fornecimento do objeto, assim como ao cumprimento das obrigações constantes neste Termo;

12.1.14. Indenizar terceiros e/ou este Órgão, mesmo em caso de ausência ou omissão de fiscalização de sua parte, por quaisquer danos ou prejuízos causados, devendo a CONTRATADA adotar todas as medidas preventivas, com fiel observância às exigências das autoridades competentes e às disposições legais vigentes;

12.1.15. Os preços ofertados pela empresa deverão incluir todas as despesas relativas ao objeto contratado (tributos, seguros, encargos sociais, frete, etc);

12.1.16. Responsabilizar-se por todo e qualquer dano que causar ao Órgão, ou a terceiros, ainda que culposo praticado por seus prepostos, empregado ou mandatários, não excluindo ou reduzindo essa responsabilidade a fiscalização ou acompanhamento pela SEPLAG;

12.1.17. Responsabilizar-se por todo e qualquer tipo de atuação ou ação que venha a sofrer em decorrência do fornecimento em questão, bem como pelos Contratos de trabalho de seus empregados, mesmo nos casos que envolvam eventuais decisões judiciais, eximindo esta instituição de qualquer solidariedade ou responsabilidade;

12.1.18. Credenciar junto a SEPLAG um preposto para prestar esclarecimentos e atender às reclamações/solicitações que surgirem durante a execução do contrato;

12.1.19. A empresa CONTRATADA deverá cumprir quaisquer outras exigências legais pertinentes ao objeto licitado, que por ventura não tenham sido explicitados no Termo de Referência;

12.1.20. Não transferir a outrem, no todo ou em parte, o Objeto;

12.1.21. Executar os serviços dentro do quantitativo estimado na tabela constante neste instrumento;

12.1.22. Observar conduta adequada na utilização dos materiais, equipamentos, ferramentas e utensílios, objetivando ao correto fornecimento do objeto;

12.2. DO SIGILO, PROPRIEDADE DAS INFORMAÇÕES, DIREITO PATRIMONIAL E PROPRIEDADE INTELECTUAL

12.2.1. Manter sigilo, sob pena de responsabilidades civis, penais e administrativas, sobre todo e qualquer assunto de interesse do CONTRATANTE ou de terceiros de que tomar conhecimento em razão da execução do objeto deste Contrato, devendo orientar seus empregados nesse sentido.

12.2.2. Não veicular publicidade ou qualquer outra informação acerca dos serviços/atividades contratados, sem prévia autorização, por escrito, do CONTRATANTE.

12.2.3. Manter em caráter confidencial, mesmo após o término do prazo de vigência ou rescisão do contrato, as informações relativas à política de segurança adotada pelo CONTRATANTE e as configurações de hardware e de softwares decorrentes.

12.2.4. Manter em caráter confidencial, mesmo após o término do prazo de vigência ou rescisão do contrato, as informações relativas ao processo de instalação, configuração e adaptações de produtos, ferramentas e equipamentos.

12.2.5. Manter em caráter confidencial, mesmo após o término do prazo de vigência ou rescisão do contrato, as informações relativas ao serviço prestado no ambiente do CONTRATANTE e se aplicável, dos mecanismos de criptografia e autenticação utilizados.

12.2.6. Manter sigilo dos dados e informações confidenciais a que tiverem acesso, de acordo com as Normas de Segurança Estadual para Acesso à Informação no âmbito do Poder Executivo do Estado de

Mato Grosso e normatizada pela Resolução 008/2010-COSINT – Conselho Superior de Informação e Tecnologia da Informação do Estado de Mato Grosso.

12.2.7. Respeitar as normas e procedimentos de segurança do CONTRATANTE, de acordo com as Políticas e Diretrizes de Segurança da Informação no âmbito do Poder Executivo do Estado de Mato Grosso e normatizada pela Resolução 003/2010-COSINT – Conselho Superior de Informação e Tecnologia da Informação do Estado de Mato Grosso.

13. DA FISCALIZAÇÃO DO CONTRATO

13.1. A fiscalização será exercida por servidor(es) designado(s) pelo Contratante, o(s) qual(is) competirá dirimir as dúvidas que surgirem no curso da execução do presente Contrato, conforme art. 67 da Lei nº 8.666/93.

13.2. Não obstante a Contratada seja a única e exclusiva responsável pela execução do Contrato, ao Contratante reserva-se o direito de, sem que de qualquer forma restrinja a plenitude dessa responsabilidade, exercer a mais ampla e completa fiscalização sobre a execução do serviço, podendo para isso:

a) Ordenar a imediata retirada do local, bem como a substituição de empregado da Contratada que estiver sem uniforme ou crachá, que embaraçar ou dificultar a sua fiscalização ou cuja permanência na área, a seu exclusivo critério, julgar inconveniente;

b) Supervisionar as entregas realizadas pela Contratada, observando as normas técnicas e legais aplicáveis aos serviços, emitindo mensalmente relatório analítico, que deve ser anexado à Nota Fiscal;

13.3. A fiscalização de que trata este item não exclui nem reduz a responsabilidade da Contratada, inclusive perante terceiros, por qualquer irregularidade, resultante de imperfeições técnicas, vícios redibitórios, ou emprego de material inadequado ou de qualidade inferior e, na ocorrência desta, não implica co-responsabilidade do Contratante ou de seus agentes e prepostos, conforme preceitua art. 70 da Lei nº 8.666/93.

13.4. Será de responsabilidade do Fiscal de cada Órgão/Entidade Contratante, a salva guarda dos documentos relacionado à liberação do pagamento referente a execução do objeto contratado.

13.5. Para efeito de gestão dos contratos originados desta operação serão utilizadas as seguintes definições:

a) Gestor/Fiscal de Contrato (unidade administrativa de controle ou equivalente) – Trata-se de servidor designado pelo Órgão/Entidade Contratante, indicado em Contrato responsável por:

1 - Controlar a utilização do saldo existente, bem como os valores empenhados e a empenhar;

2 - Responsável pelo contato com a Contratada;

3 - Aplicar todas as determinações e normas de conduta, acompanhamento e fiscalização de Contrato previstos em manual de gerenciamento de contrato, caso houver, e as orientações e determinações oriundas dos Órgãos de Controle Interno e Externo, bem como as previstas nos instrumentos legais;

4 - Notificar a Contratada sobre situações irregulares;

b) Gestor/Fiscal da Unidade – Trata-se do responsável pela unidade onde será executado o objeto contratado. Este, poderá incumbir a outro servidor o papel de Fiscal da Unidade, contudo ambos respondem solidariamente. A este(s) compete(m):

1. O Acompanhamento e a fiscalização da execução do serviço;
2. Prestar informações e esclarecimentos ao preposto da Contratada, sempre que for preciso;
3. Conferir e atestar as Notas Fiscais da entrega do serviço;
4. Notificar a Contratada e informar o Gestor do Contrato sobre situações irregulares;

13.5.1. O Gestor/Fiscal do Contrato e Gestor/Fiscal da Unidade podem ser a mesma pessoa, conforme definição e conveniência de cada Órgão/Entidade, devendo ser especificado no Contrato o nome do(s) mesmo(s).

13.6. Acompanhar e fiscalizar a execução dos serviços, prestando informações mensais e/ou sempre que solicitado à Secretaria Adjunta de Patrimônio e Serviços/SEPLAG referente ao objeto contratado.

13.7. Emitir informação ou relatório a respeito de todos os atos da Contratada relativos à execução do Contrato, em especial quanto à aplicação de sanções, alterações, prorrogações e rescisão do Contrato.

13.8. A Fiscalização do Contratante poderá solicitar informações ou esclarecimentos formalmente à Contratada diretamente ao Preposto, sendo que o prazo para resposta será no prazo máximo de 24 (vinte e quatro) horas.

13.8.1. Caso os esclarecimentos demandados impliquem indagações de caráter técnico ou em qualquer outra hipótese de exceção, deverá ser encaminhada justificativa formal, dentro do mesmo prazo supracitado, à Fiscalização do Contratante, para que esta, caso entenda necessário, decida sobre a dilação do prazo para resposta da Contratada.

13.9. A fiscalização da execução do contrato deverá ser realizada nos exatos termos da Instrução Normativa nº 01/2020/SEPLAG.

13.10. Serão nomeados para fiscal os seguintes servidores:

Titular: Alisson Paulo Scheibe

Suplente: Enilson Martins de Oliveira

13.11. DAS CONDIÇÕES DE RECEBIMENTO PROVISÓRIO E DEFINITIVO

13.11.1. Os serviços contratados, serão recebidos da seguinte forma:

a) Provisoriamente: o recebimento provisório dar-se-á por servidor indicado pelo Órgão/Entidade Contratante, no ato da entrega dos relatórios ou documento equivalente e, encontrando irregularidade, fixará prazo para correção, ou, se aprovado, autorizará a emissão da NF;

b) Definitivamente: após recebimento provisório, será verificada as informações dos relatórios, incluindo qualidade e quantidade dos serviços prestados no mês vigente, e sendo aprovados, será efetivado o recebimento definitivo, com aposição de assinatura nas vias do Documento Auxiliar da NF-e (Danfe) ou na Nota Fiscal, emitida pela Contratada para os serviços prestados;

13.11.2. Na hipótese de irregularidade não sanada pela Contratada, a fiscalização do Órgão/Entidade Contratante reduzirá a termo os fatos ocorridos e encaminhará à autoridade superior, para procedimentos inerentes à aplicação de penalidades;

13.11.3. O recebimento provisório ou definitivo não exclui a responsabilidade pela garantia do(s) serviços(s) executado(s) e não exclui a responsabilidade civil da Contratada por vícios de quantidade ou qualidade do(s) serviço(s) ou disparidades com as especificações estabelecidas, verificadas, posteriormente, garantindo-se ao Órgão/Entidade Contratante as faculdades previstas no art. 18 da Lei nº 8.078/90.

14. DAS CONDIÇÕES DE PAGAMENTO

14.1. O pagamento será efetuado pelo Contratante em favor da Contratada mediante ordem bancária a ser depositada em conta corrente, no valor correspondente e data fixada de acordo com a legislação para pagamento vigente no âmbito do Estado do Mato Grosso, após a apresentação da Nota Fiscal/Fatura devidamente atestada pelo Fiscal do Contratante.

14.2. O pagamento será realizado de acordo com a execução do objeto do Contrato, mediante emissão da respectiva Nota Fiscal.

14.2.1. O pagamento será efetuado após a Nota Fiscal/Fatura estar devidamente atestada pela Gerência responsável e/ou pela fiscalização do Contrato (nomeada pela autoridade competente) e acompanhada dos certificados de Regularidade Fiscal descritos nos Decretos Estaduais n°s 840/17, 8.199/06 alterado pelo 8426/06, obedecendo aos prazos estabelecidos no Decreto Orçamentário vigente.

14.2.2. Caso o objeto tenha sido recebido parcialmente, o pagamento da Nota deverá ser equivalente apenas ao serviço recebido definitivamente.

14.2.3. A Contratada deverá indicar no corpo da Nota Fiscal/Fatura, além dos serviços realizados, o número do Contrato/Ordem de Fornecimento, o número da OS, o número e nome do banco, agência e número da conta onde deverá ser feito o pagamento, via ordem bancária.

14.2.4. O pagamento será efetuado mediante cobrança por meio de Notas Fiscais dos serviços emitidas pela CONTRATADA e após o aceite do CONTRATANTE referente a cada Ordem de Serviço concluída.

14.3. Caso constatada alguma irregularidade nas Notas Fiscais/Faturas, estas serão devolvidas à Contratada, para as necessárias correções, com as informações que motivaram sua rejeição, contando-se o prazo para pagamento da data da sua reapresentação.

14.3.1. Constatando-se qualquer incorreção na Nota Fiscal, bem como, qualquer outra circunstância que desaconselhe o seu pagamento, o prazo para pagamento fluirá a partir da respectiva data de regularização.

14.3.2. Não será efetuado pagamento de Nota pendente de adimplemento por parte da Contratada, quais sejam, nos casos em que o objeto não tenha sido recebido definitivamente.

14.4. Não haverá, sob hipótese alguma, pagamento antecipado.

14.5. O Contratante efetuará retenção na fonte de todos os tributos inerentes ao Contrato em questão.

14.5.1. O faturamento dos itens de serviço deverá ser feito através de Nota Fiscal de Serviços devendo constar a alíquota de ISS do município onde foi prestado os serviços.

14.5.2. A retenção dos tributos federais não será efetuada caso a CONTRATADA apresente, junto com sua Nota Fiscal, a comprovação de que é optante do Sistema Integrado de Pagamento de Impostos e Contribuições das Microempresas e Empresas de Pequeno Porte - SIMPLES.

14.6. Nos casos de aplicação de penalidade em virtude de inadimplência contratual pela Contratada não serão efetuados pagamentos enquanto perdurar pendência de liquidação das respectivas obrigações.

14.6.1. As notas a serem pagas poderão sofrer desconto devido aplicação das multas/glosas previstas no Contrato.

14.7. O Contratante não efetuará pagamento de título descontado, ou por meio de cobrança em banco, bem como, os que forem negociados com terceiros por intermédio da operação de "factoring".

14.8. As despesas bancárias decorrentes de transferência de valores para outras praças serão de responsabilidade da Contratada.

14.9. Nenhum pagamento isentará a Contratada das suas responsabilidades e obrigações vinculadas ao objeto especialmente àquelas relacionadas com a qualidade e a garantia, nem implicará aceitação definitiva do objeto.

14.10. Havendo acréscimo de quantitativo, isto imporá ajustamento no pagamento, pelos preços unitários constantes da proposta de preços, em face dos acréscimos realizados.

14.11. Os pagamentos não realizados dentro do prazo, motivados pela Contratada, não serão geradores de direito a reajustamento de preços.

14.12. Para as operações de vendas destinadas a Órgão Público da Administração Federal, Estadual e Municipal, deverão ser acobertadas por Nota Fiscal Eletrônica, conforme Protocolo ICMS42/2009, recepcionado pelo Artigo 198-A-5-2 do RICMS. Informações através do site www.sefaz.mt.gov.br/nfe.

14.13. O pagamento somente será efetuado mediante a apresentação dos seguintes documentos:

I) Prova de regularidade junto à Fazenda Estadual, expedida pela Secretaria de Estado de Fazenda da sede ou domicílio do credor;

II) prova de regularidade junto à Dívida Ativa do Estado, expedida pela Procuradoria-Geral do Estado da sede ou domicílio do credor;

III) Prova de regularidade relativa à Seguridade Social (INSS), Certidão Negativa de Débitos Trabalhistas (CNDT) e ao Fundo de Garantia por Tempo de Serviço (FGTS), quando o Poder Executivo do Estado de Mato Grosso for solidário na obrigação.

14.13.1. Se, quando da efetivação do pagamento, os documentos comprobatórios de situação regular em relação à Fazenda Federal, ao INSS e ao FGTS, apresentados em atendimento às exigências de habilitação, estiverem com a validade expirada, o pagamento ficará retido até a apresentação de novos documentos dentro do prazo de validade.

15.DAS SANÇÕES ADMINISTRATIVAS

15.1. Comete infração administrativa nos termos da Lei nº 10.520/02, a Contratada que:

a) Ensejar injustificado retardamento da execução de seu objeto;

b) Falhar ou fraudar na execução do Contrato;

c) Comportar-se de modo inidôneo;

d) Cometer fraude fiscal;

e) Não executar, parcial ou total o Contrato;

15.2. A Contratada que cometer infração administrativa, estará sujeita à aplicação das seguintes sanções a saber:

15.2.1. Advertência, por faltas leves, nas hipóteses de execução irregular de que não resulte prejuízo para o Contratante.

15.2.2. Multas:

a) Por atraso: será aplicado multa moratória de 0,5% (cinco décimos por cento) do valor da parcela inadimplida por dia de atraso injustificado na providência necessária e 1% (um por cento) por dia após o 30º dia de atraso até o limite 60 (sessenta) dias, após será considerado inexecução total do Contrato;

b) Por faltas médias ou inexecução parcial: será aplicada multa de até 5% (cinco por cento) do valor do total do Contrato, assim entendidas aquelas que acarretam transtornos significativos ao Contratante e, na sua reincidência, esse percentual será de até 10% (dez por cento);

c) Por falta grave ou inexecução total: será aplicada multa de até 10% (dez por cento) do valor total do Contrato. Será entendida como falta grave aquela que acarrete prejuízo para o Contratante. Quanto a inexecução total a multa será aplicada independentemente da existência ou não do prejuízo ao Contratante, implicando ainda na possibilidade de rescisão do Contrato;

15.2.2.1. A multa eventualmente imposta à Contratada, poderá ser descontada da fatura a que fizer jus ou deduzidos da garantia, garantido o contraditório e ampla defesa.

15.2.2.2. Caso a Contratada não tenha nenhum valor a receber do Órgão/Entidade Contratante, ou os valores do pagamento e da garantia forem insuficientes, ser-lhe-á concedido o prazo de 05 (cinco) dias úteis, contados do recebimento de sua intimação, para efetuar o pagamento da multa.

15.2.2.3. Esgotados os meios administrativos para cobrança, não sendo efetuado o pagamento, seus dados serão encaminhados ao órgão competente para que seja inscrita na dívida ativa do Estado, podendo ainda, o Órgão/Entidade proceder à cobrança judicial da multa.

15.2.2.4. As multas previstas nesta seção não eximem a Contratada da reparação dos eventuais danos, perdas ou prejuízos que seu ato punível venha causar ao Órgão/Entidade.

15.2.3. Suspensão temporária do direito de participar em licitação e impedimento de contratar com o Poder Executivo do Estado de Mato Grosso, pelo prazo de até 02 (dois) anos.

15.2.4. Impedimento de licitar e contratar com o Poder Executivo do Estado de Mato Grosso e com consequente descredenciamento no sistema de cadastro de fornecedores, pelo prazo de até 05 (cinco) anos.

26
45R

15.2.5. Declaração de inidoneidade para licitar ou contratar com a Administração Pública enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a Contratada ressarcir o Contratante pelos prejuízos causados e após 02 (dois) anos de sua aplicação.

15.3. As sanções previstas nos subitens 15.2.3 e 15.2.4 também são aplicáveis em quaisquer das hipóteses previstas como infração administrativas referenciadas no item 15.1 deste Termo Referência.

15.4. As sanções previstas nas alíneas "b", "c", "d" e "e" do item 15.1 poderão ser aplicadas juntamente com as de multa.

15.5. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa, observando-se o procedimento previsto na Lei nº 8.666/93 e subsidiariamente na Lei Estadual nº 7.692/02.

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

15.7. Todas as sanções aplicadas devem ser comunicadas ao Cadastro Geral de Fornecedores do Estado de Mato Grosso para registro no cadastro da respectiva sancionada e ao Cadastro de Empresas Inidôneas e Suspensas-CEIS/MT.

16. PÚBLICO/CLIENTELA ALVO

16.1. Servidores da Secretaria de Planejamento e Gestão - MT

17.RESULTADOS ESPERADOS

17.1. Proteção e gerenciamento seguro da rede lógica da SEPLAG;

17.2. Controle de tráfego de rede e gestão otimizada de recursos de segurança;

17.3. Gestão eficiente de políticas e regras de filtragem;

17.4. Controle necessário sobre o tráfego de rede com base em aplicações, categoria de aplicativos e usuários envolvidos na conexão;

17.5. Disponibilidade de relatórios gerenciais, controles de acesso mais elaborados;

17.6. Aplicação de funcionalidades de segurança na rede de dados;

17.7. Controle de acesso e requisições por camadas de rede e aplicação;

17.8. Melhor desempenho e acessibilidade das informações de todas as camadas do tráfego da rede SEPLAG;

17.9. Integração entre o Sistema de Detecção de Intrusão (IDS) e o Sistema de Prevenção a Intrusão (IPS);

17.10. Possibilidade de inspeção profunda no que tange prevenção de invasão e coleta de dados.

17.11. Reconhecimento de usuários para gestão de liberação ou bloqueio;

17.12. Roteamento e QoS por aplicação;

18.LEGISLAÇÃO APLICADA AO OBJETO

18.1. Lei nº 8.666/93 e alterações – Normas para Licitação e contratos da Administração Pública;

18.2. Decreto Estadual n° 806/2017 – Regimento interno;

18.3. Decreto Estadual n° 840/2017 – Regras para aquisição de bens e serviços da Administração Pública Estadual;

18.4. Decreto Estadual nº 8.199/2006 e nº 8.426/2006 – Critério de Pagamento;

18.5. Decreto Estadual nº 1.349/2018 – Execução orçamentária;

19.DOTAÇÃO ORÇAMENTÁRIA

ÓRGÃO/ ENTIDADE	UNIDADE ORÇAMENTÁRIA	PROJETO/ATIVIDADE	NATUREZA DE DESPESA	FONTE
FUNDESP	11601	2009	449052014	108 E 240

PTA 2020 - Subação 2: Disponibilização do parque computacional e infraestrutura adequados

Cuiabá, 20 de outubro de 2020.

Alison da Silva Ribeiro
Coordenador de Infraestrutura

Marcel Ribeiro Primo de Souza
Superintendente de Tecnologia da Informação Setorial

Prosseguimento:

Eliane Rosa Fernandes de Albuquerque
Secretária Adjunta de Administração Sistêmica

ANEXO I – ESPECIFICAÇÕES TÉCNICA

1. **ESPECIFICAÇÕES GERAIS PARA TODOS OS SWITCHS NEXT GENERATION**

1.1. **Switches de acesso Tipo I – 4 8 portas 10/100/1000 Base-T POE+ + 4 Portas 10Gbe SFP+**

1.1.1. A proposta deverá conter a descrição detalhada com códigos do fabricante de todos os módulos, fontes e acessórios fornecidos.

1.1.2. A solução deve ser composta de um único equipamento, montável em rack 19" devendo este vir acompanhado dos devidos acessórios para tal.

1.1.3. Possuir fonte de alimentação interna que trabalhe em 100V-240V, 50/60 Hz, com detecção automática de tensão e frequência.

1.1.4. Suportar fonte de alimentação redundante externa, montável em rack.

1.1.5. Implementar Power over Ethernet Plus (PoE+) segundo o padrão IEEE 802.3at em todas as portas 1000Base-T, com no mínimo 740W de potência disponível para dispositivos PoE através de fonte interna.

1.1.6. Suportar Power over Ethernet Plus (PoE+) segundo o padrão IEEE 802.3at em todas as portas 1000Base-T simultaneamente, com no mínimo 1440W de potência disponível para dispositivos PoE através da instalação de fonte externa.

1.1.7. Possuir, no mínimo, 170 Gbps de Switch Fabric.

1.1.8. Possuir capacidade de encaminhamentos de pacotes, de no mínimo 130 Mpps utilizando pacotes de 64 bytes.

1.1.9. Detecção automática MDI/MDIX em todas as portas 10/100/1000BASE-T RJ-45.

1.1.10. Possuir porta de console com conector RJ-45 ou DB9 macho.

1.1.11. Possuir leds indicativos de funcionamento da fonte de alimentação, ventiladores e status das portas.

1.1.12. Possuir 48 portas 10/100/1000BASE-T ativas simultaneamente, com conector RJ-45.

1.1.13. Possuir 4 (quatro) portas 10GBASE-X ativas simultaneamente, baseadas em SFP+, devendo um mesmo slot suportar interfaces 10 Gigabit Ethernet 10GBASE-SR, 10GBASE-LR, 10GBASE-ER e 10GBASE-ZR. Não é permitida a utilização de conversores externos.

1.1.14. O equipamento deve possuir além das portas acima citadas uma porta adicional 10/100 ou 10/100/1000 com conector RJ-45 para gerência out-of-band do equipamento.

1.1.15. Implementar empilhamento de no mínimo oito equipamentos e gerência através de um único endereço IP.

1.1.16. O equipamento deve suportar o agrupamento lógico (gerência por um único IP) de unidades remotamente instaladas (no mínimo a distância de 40km).

1.1.17. O empilhamento deve possuir arquitetura de anel para prover resiliência.

1.1.18. O empilhamento deve ter capacidade de path fast recover, ou seja, com a falha de um dos elementos da pilha os fluxos devem ser reestabelecidos no tempo máximo de 50ms.

1.1.19. Possuir indicação visual no painel frontal do equipamento que permita identificar a posição lógica do equipamento da pilha.

1.1.20. O empilhamento deve permitir a criação de grupos de links agregados entre diferentes membros da pilha, segundo 802.3ad.

1.1.21. O empilhamento deve suportar espelhamento de tráfego entre diferentes unidades da pilha.

1.1.22. Deve ser possível mesclar em uma mesma pilha equipamentos com que não implementem PoE.

1.1.23. A Memória Flash instalada deve ser suficiente para comportar no mínimo duas imagens do Sistema Operacional simultaneamente, permitindo que seja feito um upgrade de Software e a imagem anterior seja mantida.

1.1.24. Todas as interfaces ofertadas devem ser non-blocking.
1.1.25. Possuir altura máxima de 1U (1,75").
1.1.26. Deve armazenar, no mínimo, 16.000 (dezesseis mil) endereços MAC.
1.1.27. Implementar agregação de links conforme padrão IEEE 802.3ad
1.1.28. Possuir homologação da ANATEL, de acordo com a Resolução número 242.
1.1.29. Implementar agregação de links conforme padrão IEEE 802.3ad com suporte a LACP.
1.1.30. Em conjunto com outro equipamento de mesmo modelo, deverá permitir que um switch conectado aos dois, tenha a possibilidade de agregação de links (IEEE 802.3ad) com suporte a LACP com os mesmos, de forma a simular a existência de apenas um único link lógico entre este equipamento e os dois switches do modelo aqui especificado (Multi-Chassis Trunking, por exemplo). O único link lógico entre as camadas deve eliminar convergência do Spanning Tree, possibilitando o tráfego simultâneo por mais de uma conexão.
1.1.31. Implementar jumbo frames em todas as portas ofertadas, com suporte a pacotes de até 9216 Bytes.
1.1.32. Implementar Proxy-ARP (RFC 1027).
1.1.33. Implementar IGMP v1, v2 e v3 Snooping.
1.1.34. Implementar IGMPv1 (RFC 1112), IGMP v2 (RFC 2236) e IGMPv3 (RFC 3376).
1.1.35. Implementar MVR (Multicast VLAN Registration).
1.1.36. Implementar DHCP/Bootp relay configurável por VLAN para IPv4 e IPv6.
1.1.37. Implementar servidor DHCP interno que permita a configuração de um intervalo de endereços IP a serem atribuídos os clientes DHCP e possibilite ainda a atribuição de, no mínimo, default-gateway, servidor DNS e servidor WINS.
1.1.38. Implementar DHCP Option 82, de acordo com a RFC 3046, com identificação de porta e VLAN, configurável por VLAN.
1.1.39. Implementar DHCP Client para IPv4 e IPv6.
1.1.40. Implementar RFC 3021 - Using 31-Bit Prefixes on IPv4 Point-to-Point Links
1.1.41. Implementar Spanning-Tree (IEEE 802.1d), Rapid Spanning Tree (IEEE 802.1w), Multiple Instance STP (802.1s) e PVST+.
1.1.42. Implementar a configuração de Multiple Spanning Tree Protocol, com suporte a, pelo menos, 32 domínios.
1.1.43. Implementar funcionalidade vinculada ao Spanning-tree onde é possível designar portas de acesso (por exemplo onde estações estão conectadas) que não sofram o processo de Listening-Learning, passando direto para o estado de Forwarding. No entanto, as portas configuradas com esta funcionalidade devem detectar loops na rede normalmente.
1.1.44. Implementar funcionalidade vinculada ao Spanning-tree que evite a eleição de outros switches da rede como Root.
1.1.45. Implementar funcionalidade vinculada ao Spanning-tree que permita desabilitar uma porta de acesso assim que a mesma receba uma BPDU.
1.1.46. Implementar 4000 VLANs por porta, ativas simultaneamente, através do protocolo 802.1Q.
1.1.47. Deverá permitir a criação, remoção, gerenciamento e distribuição de VLANs de forma dinâmica através de portas configuradas como tronco IEEE 802.1Q utilizando o protocolo MVRP segundo o padrão IEEE802.1ak.
1.1.48. Possibilitar a coleta de estatísticas de tráfego baseada em VLANs IEEE 802.1Q e double-tagged VLANs IEEE 802.1ad.
1.1.49. Implementar MAC Based VLAN.
1.1.50. Implementar VLAN Translation.

1.1.51. Implementar VLAN Aggregation ou funcionalidade que permita o compartilhamento de uma mesma subnet e de um mesmo endereço IPv4 utilizado como default-gateway por hosts de diferentes VLANs.
1.1.52. Implementar Private VLANs.
1.1.53. Implementar Port Isolation ou funcionalidade que permita isolamento de portas específicas do switch. As portas isoladas não devem se comunicar entre si, porém podem se comunicar com qualquer outra porta no equipamento que não esteja isolada.
1.1.54. Implementar IEEE 802.1ad com a possibilidade de associar CVIDs específicos para diferentes SVIDs (selective Q-in-Q ou 802.1ad CEP). A implementação deverá permitir a tradução do CVID.
1.1.55. Implementar IEEE 802.1ag (Connectivity Fault Management).
1.1.56. Implementar IEEE 802.3ah Ethernet OAM – Unidirectional Link Fault Management.
1.1.57. Implementar funcionalidade baseada na recomendação do ITU-T Y.1731 com medição de, no mínimo, Frame Delay.
1.1.58. Implementar o protocolo ITU-T G.8032 ERPS.
1.1.59. Implementar protocolo de resiliência em camada 2, específico para topologias em anel, que permita tempo de convergência inferior a 200 ms.
1.1.60. Implementar IEEE 802.1ab Link Layer Discovery Protocol (LLDP).
1.1.61. Implementar LLDP-MED (Media Endpoint Discovery).
1.1.62. Implementar roteamento estático com suporte a, no mínimo, 480 rotas.
1.1.63. Implementar, no mínimo, 500 interfaces IP (IPv4 ou IPv6).
1.1.64. Implementar os protocolos de roteamento IP: RFC 1058 – RIP v1 e RFC 2453 – RIP v2.
1.1.65. Suportar o protocolo de roteamento OSPFv2, incluindo autenticação MD5.
1.1.66. Suportar o protocolo de roteamento OSPFv2 (RFC 2328), incluindo autenticação MD5.
1.1.67. Implementar PIM Snooping.
1.1.68. Suportar protocolo de multicast PIM-SM para IPv4 e IPv6.
1.1.69. Suportar PIM-SSM segundo a RFC 3569.
1.1.70. Suportar VRRPv3 (RFC 5798).
1.1.71. "Deve implementar Dual Stack, ou seja, IPv6 e IPv4, com suporte as seguintes funcionalidades/RFCs:
1.1.71.1. RFC 1981, Path MTU Discovery for IPv6, August 1996 - Host Requirements
1.1.71.2. RFC 5095, Internet Protocol, Version 6 (IPv6) Specification
1.1.71.3. RFC 4861, Neighbor Discovery for IP Version 6, (IPv6)
1.1.71.4. RFC 2462, IPv6 Stateless Address Auto configuration - Host Requirements
1.1.71.5. RFC 2463, Internet Control Message Protocol (ICMPv6) for the IPv6 Specification
1.1.71.6. RFC 2464, Transmission of IPv6 Packets over Ethernet Networks
1.1.71.7. RFC 2465, IPv6 MIB, General Group and Textual Conventions
1.1.71.8. RFC 2466, MIB for ICMPv6
1.1.71.9. RFC 3513, Internet Protocol Version 6 (IPv6) Addressing Architecture
1.1.71.10. RFC 3587, Global Unicast Address Format"
1.1.71.11. Implementar os seguintes protocolos em IPv6: Ping, Traceroute, Telnet, SSHv2, SNMP, Syslog, SNTP e DNS.
1.1.72. "Deve implementar IPv6 de acordo com as seguintes RFCs:
1.1.72.1. RFC 1981, Path MTU Discovery for IPv6, August 1996 - Router Requirements
1.1.72.2. RFC 2462, IPv6 Stateless Address Auto configuration - Router Requirements
1.1.72.3. RFC 2080, RIPng
1.1.72.4. RFC 2462, IPv6 Stateless Address Auto configuration - Router Requirements
1.1.72.5. RFC 2710, IPv6 Multicast Listener Discovery v1 (MLDv1) Protocol

1.1.72.6. RFC 3810, IPv6 Multicast Listener Discovery v2 (MLDv2) Protocol
1.1.72.7. RFC 6106, IPv6 Router Advertisement Options for DNS Configuration
1.1.72.8. Suportar OSPFv3.
1.1.72.9. Implementar OSPFv3 Graceful Restart conforme RFC 5187.
1.1.72.10. A implementação de OSPFv3 e rotas estáticas para IPv6 deve incluir ECMP (Equal Cost Multi Path).
1.1.72.11. Implementar BFD (Bidirectional Forwarding Detection).
1.1.74.12. Implementar Policy Based Routing.
1.1.73. Implementar upload e download de configuração em formato ASCII ou XML, permitindo a edição do arquivo de configuração e, posteriormente, o download do arquivo editado para o equipamento.
1.1.74. Implementar TACACS+ segundo a RFC 1492.
1.1.75. "Implementar autenticação RADIUS com suporte a:
1.1.78.1. RFC 2865 RADIUS Authentication
1.1.78.2. RFC 2866 RADIUS Accounting
1.1.78.3. RFC 3579 RADIUS EAP support for 802.1X"
1.1.76. A implementação de RADIUS deve suportar alteração dinâmica de parâmetros de autorização de uma sessão que já esteja ativa.
1.1.77. A implementação de RADIUS e TACACS+ deve estar disponível para autenticação de usuários via Telnet e Console serial.
1.1.78. Implementar per-command authorization para RADIUS e TACACS+.
1.1.79. Possuir DNS Client para IPv4 segundo a RFC 1591 e DNS Client para IPv6.
1.1.80. Possuir Telnet client and server segundo a RFC 854.
1.1.81. Implementar os seguintes grupos de RMON através da RFC 1757:
1.1.82. History, Statistics, Alarms e Events.
1.1.83. Deve implementar RMON2-probe configuration segundo a RFC 2021, podendo ser implementada internamente no switch ou externamente, por meio de probe em hardware utilizando uma porta 1000BaseTX.
1.1.84. Implementar sFlow ou Netflow, em hardware.
1.1.85. Implementar a atualização de imagens de software e configuração através de um servidor TFTP.
1.1.86. Suportar múltiplos servidores Syslog.
1.1.87. Implementar ajuste de clock do equipamento utilizando NTP com autenticação MD5 e SNTP.
1.1.88. Implementar Port Mirroring, permitindo espelhar até 128 portas físicas ou 16 VLANs para até 16 portas de destino (portas de análise). Deve ser possível configurar mais de uma sessão de espelhamento simultânea.
1.1.89. Implementar RSPAN (Remote Mirroring), permitindo espelhar o tráfego de uma porta ou VLAN de um switch remoto para uma porta de um switch local (porta de análise).
1.1.90. Implementar gerenciamento através de SNMPv1 (RFC 1157), v2c (RFCs 1901 a 1908), v3 (RFCs 3410 a 3415) e SNMP para IPv6.
1.1.91. Implementar SMON de acordo com a RFC 2613.
1.1.92. Implementar cliente e servidor SSHv2.
1.1.93. Implementar cliente e servidor SCP e servidor SFTP.
1.1.94. Implementar gerenciamento via web com suporte a HTTP e HTTPS/SSL, permitindo visualização gráfica da utilização (em percentual, bytes e pacotes) das portas.

1.1.95. A interface gráfica deve permitir visualização de informações do sistema (VLAN, Portas, Fonte e Fans), monitoramento de Log, utilização de portas, QoS e configuração de portas, VLANs e ACLs.
1.1.96. O equipamento ofertado deve possuir um sistema operacional modular.
1.1.97. O sistema operacional deve possuir função grep/pipe para filtrar a saída de determinado comando.
1.1.98. O sistema operacional deve possuir comandos para visualização e monitoração de cada processo, sendo possível verificar por processo qual o consumo de cpu, process-id e qual o consumo de memória por processo.
1.1.99. O sistema operacional deve possuir comandos para que processos sejam terminados ou reiniciados sem que seja necessário a reinicialização do equipamento. Esta funcionalidade deve estar disponível pelo menos para Telnet, TFTP, HTTP e LLDP na versão atual.
1.1.100. Implementar linguagem de scripting baseada em Python, permitindo a automatização de tarefas. A linguagem deve implementar estruturas de controle como loops e execução condicional e permitir a definição de variáveis.
1.1.101. Implementar protocolo de monitoramento de status de comunicação entre dois switches, que possibilite que uma porta seja desabilitada caso seja detectada uma falha de comunicação entre os dois peers.
1.1.102. Implementar funcionalidade que permita sua auto-configuração através dos protocolos DHCP e TFTP, permitindo o provisionamento em massa com o mínimo de intervenção humana.
1.1.103. Deve disponibilizar API (Aplication Programming Interface) aberta para integração com aplicações.
1.1.104. Implementar Rate limiting de entrada em todas as portas. A granularidade deve ser configurável em intervalos de 64Kbps para portas de até 1Gbps. Caso o equipamento ofertado possua suporte a portas 10Gbps, a granularidade para este tipo de interface deve ser configurável em intervalos de 1Mbps. A implementação de Rate Limiting deve permitir a classificação do tráfego utilizando-se ACLs e parâmetros, MAC origem e destino (simultaneamente) IP origem e destino (simultaneamente), portas TCP, portas UDP e campo 802.1p.
1.1.105. Implementar Rate Shaping de saída em todas as portas. A granularidade deve ser configurável em intervalos de 64Kbps para portas de até 1Gbps. Caso o equipamento ofertado possua suporte a portas 10Gbps, a granularidade para este tipo de interface deve ser configurável em intervalos de 1Mbps.
1.1.106. A funcionalidade de Rate Shaping deve permitir a configuração de CIR (Commited Rate), banda máxima, banda mínima e peak rate.
1.1.107. Implementar a leitura, classificação e remarcação de QoS (802.1p e DSCP).
1.1.108. Implementar remarcação de prioridade de pacotes Layer 3, remarcando o campo DiffServ para grupos de tráfego classificados segundo portas TCP e UDP, endereço/subrede IP, VLAN e MAC origem e destino.
1.1.109. Implementar 8 filas de prioridade em hardware por porta.
1.1.110. Implementar os algoritmos de gerenciamento de filas WRR (Weighted Round Robin), WDRR (Weighted Deficit Round Robin) e SP (Strict Priority).
1.1.111. Deve implementar, ao menos dois dos algoritimos acima, simultaneamente em uma mesma porta.
1.1.112. "Implementar as seguintes RFCs:
1.1.117.1. RFC 2474 DiffServ Precedence

1.1.117.2. RFC 2598 DiffServ Expedited Forwarding (EF)
1.1.117.3. RFC 2597 DiffServ Assured Forwarding (AF)
1.1.117.4. RFC 2475 DiffServ Core and Edge Router Functions"

1.1.113. Implementar classificação de tráfego para QoS em Layer1-4 (Policy-Based Mapping) baseado em MAC origem e destino, IP origem e destino, TCP/UDP port, Diffserv e 802.1p.

1.1.114. Implementar detecção de oscilação (flap) de links, permitindo desabilitar uma porta caso a porta oscile acima de um limiar configurado.

1.1.115. Implementar funcionalidade que permita que somente endereços designados por um servidor DHCP tenham acesso à rede.

1.1.116. Implementar funcionalidade que permita que somente servidores DHCP autorizados atribuam configuração IP aos clientes DHCP (Trusted DHCP Server).

1.1.117. Implementar Gratuitous ARP Protection.

1.1.118. Implementar detecção e proteção contra ataques Denial of Service (DoS) direcionados a CPU do equipamento por meio da criação dinâmica e automática de regras para o bloqueio do tráfego suspeito.

1.1.119. Implementar limitação de número de endereços MAC aprendidos por uma porta, para uma determinada VLAN.

1.1.120. Implementar travamento de endereços MAC, permitindo a adição estática de endereços para uma determinada porta ou utilizando os endereços existentes na tabela MAC. O acesso de qualquer outro endereço que não esteja previamente autorizado deve ser negado.

1.1.121. Implementar login de rede baseado no protocolo IEEE 802.1x, permitindo que a porta do switch seja associada a VLAN definida para o usuário no servidor RADIUS.

1.1.122. A implementação do IEEE 802.1x deve incluir suporte a Guest VLAN, encaminhando o usuário para esta VLAN caso este não possua suplicante 802.1x ativo, em caso de falha de autenticação e no caso de indisponibilidade do servidor AAA.

1.1.123. Implementar múltiplos suplicantes por porta, onde cada dispositivo deve ser autenticado de forma independente, podendo ser encaminhados a VLANs distintas. As múltiplas autenticações devem ser realizadas através de IEEE 802.1x.

1.1.124. Implementar autenticação baseada em web, com suporte a SSL, através de RADIUS ou através da base local do switch.

1.1.125. Implementar autenticação baseada em endereço MAC, através de RADIUS ou através da base local do switch.

1.1.126. Implementar ACLs de entrada (ingress ACLs) em hardware, baseadas em critérios da camada 2 (MAC origem e destino e campo 802.1p), camada 3 (IP origem e destino) e camada 4 (portas TCP e UDP), em todas as interfaces e VLANs, com suporte a endereços IPv6.

1.1.127. As ACLs devem ser configuradas para permitir, negar, aplicar QoS, espelhar o tráfego para uma porta de análise, criar entrada de log e incrementar contador.

1.1.128. Implementar funcionalidade que permita a execução de ACLs em um determinado horário do dia (time-based ACLs).

1.1.129. Implementar políticas por usuário, permitindo que as configurações de ACL, QoS sejam aplicadas na porta utilizada para a conexão à rede, após a autenticação.

1.1.130. Implementar a configuração de telefones IP de forma automática, permitindo a detecção do aparelho através do protocolo LLDP e a configuração de VLAN e QoS para a porta.

1.1.131. Implementar a configuração de telefones IP de forma automática, permitindo a detecção do aparelho através do protocolo LLDP e repasse de configuração de VLAN e QoS para o telefone através do protocolo LLDP-MED.

1.1.132. Implementar Policy Based Switching, ou seja, possibilitar que o tráfego classificado por uma ACL seja redirecionado para uma porta física específica.
1.1.133. Implementar funcionalidade que permita o mapeamento de usuários identificados via Kerberos (com a credencial de usuário no domínio), IEEE 802.1x e LLDP, provendo informações como endereço MAC, VLAN e porta física. Estas informações devem estar disponíveis na linha de comando (CLI) do equipamento.
1.1.134. O equipamento ofertado deve permitir que o mesmo faça parte de uma malha ethernet (Fabric Ethernet) descrito nos Switches Core de Rede Tipo I, II e III com as seguintes funcionalidades:
1.1.135. O equipamento ofertado deve permitir a configuração como elemento anexo à malha ethernet;
1.1.136. O equipamento ofertado deve permitir a criação de VLANS mapeadas a serviços virtuais de rede, de que forma os serviços sejam criados automaticamente no elemento de borda da malha e propagados de maneira automática nos demais equipamentos que compõem a malha ethernet
1.1.137. Deve permitir o gerenciamento do equipamento através de software de gerência do Fabric;

1.2. **Switches de acesso Tipo II - 48 portas 10/100/1000 Base-T + 4 Portas 10Gbe SFP+**
1.2.1. A proposta deverá conter a descrição detalhada com códigos do fabricante de todos os módulos, fontes e acessórios fornecidos.
1.2.2. A solução deve ser composta de um único equipamento, montável em rack 19" devendo este vir acompanhado dos devidos acessórios para tal.
1.2.3. Possuir fonte de alimentação interna que trabalhe em 100V-240V, 50/60 Hz, com detecção automática de tensão e frequência.
1.2.4. Suportar fonte de alimentação redundante externa, montável em rack.
1.2.5. Possuir, no mínimo, 170 Gbps de Switch Fabric.
1.2.6. Possuir capacidade de encaminhamento de pacotes, de no mínimo 130 Mpps utilizando pacotes de 64 bytes.
1.2.7. Detecção automática MDI/MDIX em todas as portas 10/100/1000BASE-T RJ-45.
1.2.8. Possuir porta de console com conector RJ-45 ou DB9 macho.
1.2.9. Possuir leds indicativos de funcionamento da fonte de alimentação, ventiladores e status das portas.
1.2.10. Possuir 48 portas 10/100/1000BASE-T ativas simultaneamente, com conector RJ-45.
1.2.11. Possuir 4 (quatro) portas 10GBASE-X ativas simultaneamente, baseadas em SFP+, devendo um mesmo slot suportar interfaces 10 Gigabit Ethernet 10GBASE-SR, 10GBASE-LR, 10GBASE-ER e 10GBASE-ZR. Não é permitida a utilização de conversores externos.
1.2.12. O equipamento deve possuir além das portas acima citadas uma porta adicional 10/100 ou 10/100/1000 com conector RJ-45 para gerência out-of-band do equipamento.
1.2.13. Implementar empilhamento de no mínimo oito equipamentos e gerência através de um único endereço IP.
1.2.14. O equipamento deve suportar o agrupamento lógico (gerência por um único IP) de unidades remotamente instaladas.
1.2.15. O empilhamento deve possuir arquitetura de anel para prover resiliência.
1.2.16. O empilhamento deve ter capacidade de path fast recover, ou seja, com a falha de um dos elementos da pilha os fluxos devem ser reestabelecidos no tempo máximo de 50ms.
1.2.17. Possuir indicação visual no painel frontal do equipamento que permita identificar a posição lógica do equipamento da pilha.

1.2.18. O empilhamento deve permitir a criação de grupos de links agregados entre diferentes membros da pilha, segundo 802.3ad.
1.2.19. O empilhamento deve suportar espelhamento de tráfego entre diferentes unidades da pilha.
1.2.20. Deve ser possível mesclar em uma mesma pilha equipamentos que implementem PoE.
1.2.21. A Memória Flash instalada deve ser suficiente para comportar no mínimo duas imagens do Sistema Operacional simultaneamente, permitindo que seja feito um upgrade de Software e a imagem anterior seja mantida.
1.2.22. Todas as interfaces ofertadas devem ser non-blocking.
1.2.23. Possuir altura máxima de 1U (1,75").
1.2.24. Deve armazenar, no mínimo, 16.000 (dezesseis mil) endereços MAC.
1.2.25. Implementar agregação de links conforme padrão IEEE 802.3ad
1.2.26. Possuir homologação da ANATEL, de acordo com a Resolução número 242.
1.2.27. Implementar agregação de links conforme padrão IEEE 802.3ad com suporte a LACP.
1.2.28. Em conjunto com outro equipamento de mesmo modelo, deverá permitir que um switch conectado aos dois, tenha a possibilidade de agregação de links (IEEE 802.3ad) com suporte a LACP com os mesmos, de forma a simular a existência de apenas um único link lógico entre este equipamento e os dois switches do modelo aqui especificado (Multi-Chassis Trunking, por exemplo). O único link lógico entre as camadas deve eliminar convergência do Spanning Tree, possibilitando o tráfego simultâneo por mais de uma conexão.
1.2.29. Implementar jumbo frames em todas as portas ofertadas, com suporte a pacotes de até 9216 Bytes.
1.2.30. Implementar Proxy-ARP (RFC 1027).
1.2.31. Implementar IGMP v1, v2 e v3 Snooping.
1.2.32. Implementar IGMPv1 (RFC 1112), IGMP v2 (RFC 2236) e IGMPv3 (RFC 3376).
1.2.33. Implementar MVR (Multicast VLAN Registration).
1.2.34. Implementar DHCP/Bootp relay configurável por VLAN para IPv4 e IPv6.
1.2.35. Implementar servidor DHCP interno que permita a configuração de um intervalo de endereços IP a serem atribuídos os clientes DHCP e possibilite ainda a atribuição de, no mínimo, default-gateway, servidor DNS e servidor WINS.
1.2.36. Implementar DHCP Option 82, de acordo com a RFC 3046, com identificação de porta e VLAN, configurável por VLAN.
1.2.37. Implementar DHCP Client para IPv4 e IPv6.
1.2.38. Implementar RFC 3021 - Using 31-Bit Prefixes on IPv4 Point-to-Point Links
1.2.39. Implementar Spanning-Tree (IEEE 802.1d), Rapid Spanning Tree (IEEE 802.1w), Multiple Instance STP (802.1s) e PVST+.
1.2.40. Implementar a configuração de Multiple Spanning Tree Protocol, com suporte a, pelo menos, 32 domínios.
1.2.41. Implementar funcionalidade vinculada ao Spanning-tree onde é possível designar portas de acesso (por exemplo onde estações estão conectadas) que não sofram o processo de Listening-Learning, passando direto para o estado de Forwarding. No entanto, as portas configuradas com esta funcionalidade devem detectar loops na rede normalmente.
1.2.42. Implementar funcionalidade vinculada ao Spanning-tree que evite a eleição de outros switches da rede como Root.
1.2.43. Implementar funcionalidade vinculada ao Spanning-tree que permita desabilitar uma porta de acesso assim que a mesma receba uma BPDU.
1.2.44. Implementar 4000 VLANs por porta, ativas simultaneamente, através do protocolo 802.1Q.
1.2.45. Deverá permitir a criação, remoção, gerenciamento e distribuição de VLANs de forma dinâmica

através de portas configuradas como tronco IEEE 802.1Q utilizando o protocolo MVRP segundo o padrão IEEE802.1ak.
1.2.46. Possibilitar a coleta de estatísticas de tráfego baseada em VLANs IEEE 802.1Q e double-tagged VLANs IEEE 802.1ad.
1.2.47. Implementar MAC Based VLAN.
1.2.48. Implementar VLAN Translation.
1.2.49. Implementar VLAN Aggregation ou funcionalidade que permita o compartilhamento de uma mesma subnet e de um mesmo endereço IPv4 utilizado como default-gateway por hosts de diferentes VLANs.
1.2.50. Implementar Private VLANs.
1.2.51. Implementar Port Isolation ou funcionalidade que permita isolamento de portas específicas do switch. As portas isoladas não devem se comunicar entre si, porém podem se comunicar com qualquer outra porta no equipamento que não esteja isolada.
1.2.52. Implementar IEEE 802.1ad com a possibilidade de associar CVIDs específicos para diferentes SVIDs (selective Q-in-Q ou 802.1ad CEP). A implementação deverá permitir a tradução do CVID.
1.2.53. Implementar IEEE 802.1ag (Connectivity Fault Management).
1.2.54. Implementar IEEE 802.3ah Ethernet OAM – Unidirectional Link Fault Management.
1.2.55. Implementar funcionalidade baseada na recomendação do ITU-T Y.1731 com medição de, no mínimo, Frame Delay.
1.2.56. Implementar o protocolo ITU-T G.8032 ERPS.
1.2.57. Implementar protocolo de resiliência em camada 2, específico para topologias em anel, que permita tempo de convergência inferior a 200 ms.
1.2.58. Implementar IEEE 802.1ab Link Layer Discovery Protocol (LLDP).
1.2.59. Implementar LLDP-MED (Media Endpoint Discovery).
1.2.60. Implementar roteamento estático com suporte a, no mínimo, 480 rotas.
1.2.61. Implementar, no mínimo, 500 interfaces IP (IPv4 ou IPv6).
1.2.62. Implementar os protocolos de roteamento IP: RFC 1058 – RIP v1 e RFC 2453 – RIP v2.
1.2.63. Suportar o protocolo de roteamento OSPFv2, incluindo autenticação MD5.
1.2.64. Suportar o protocolo de roteamento OSPFv2 (RFC 2328), incluindo autenticação MD5.
1.2.65. Implementar PIM Snooping.
1.2.66. Suportar protocolo de multicast PIM-SM para IPv4 e IPv6.
1.2.67. Suportar PIM-SSM segundo a RFC 3569.
1.2.68. Suportar VRRPv3 (RFC 5798).
1.2.69. "Deve implementar Dual Stack, ou seja, IPv6 e IPv4, com suporte as seguintes funcionalidades/RFCs:
1.2.69.1. RFC 1981, Path MTU Discovery for IPv6, August 1996 - Host Requirements
1.2.69.2. RFC 5095, Internet Protocol, Version 6 (IPv6) Specification
1.2.69.3. RFC 4861, Neighbor Discovery for IP Version 6, (IPv6)
1.2.69.4. RFC 2462, IPv6 Stateless Address Auto configuration - Host Requirements
1.2.69.5. RFC 2463, Internet Control Message Protocol (ICMPv6) for the IPv6 Specification
1.2.69.6. RFC 2464, Transmission of IPv6 Packets over Ethernet Networks
1.2.69.7. RFC 2465, IPv6 MIB, General Group and Textual Conventions
1.2.69.8. RFC 2466, MIB for ICMPv6
1.2.69.9. RFC 3513, Internet Protocol Version 6 (IPv6) Addressing Architecture
1.2.69.10. RFC 3587, Global Unicast Address Format"
1.2.70. Implementar os seguintes protocolos em IPv6: Ping, Traceroute, Telnet, SSHv2, SNMP, Syslog, SNTP e DNS.

1.2.71. "Deve implementar IPv6 de acordo com as seguintes RFCs:
1.2.71.1. RFC 1981, Path MTU Discovery for IPv6, August 1996 - Router Requirements
1.2.71.2. RFC 2462, IPv6 Stateless Address Auto configuration - Router Requirements
1.2.71.3. RFC 2080, RIPng
1.2.71.4. RFC 2462, IPv6 Stateless Address Auto configuration - Router Requirements
1.2.71.5. RFC 2710, IPv6 Multicast Listener Discovery v1 (MLDv1) Protocol
1.2.71.6. RFC 3810, IPv6 Multicast Listener Discovery v2 (MLDv2) Protocol
1.2.71.7. RFC 6106, IPv6 Router Advertisement Options for DNS Configuration
1.2.72. Suportar OSPFv3
1.2.73. Implementar OSPFv3 Graceful Restart conforme RFC 5187.
1.2.74. A implementação de OSPFv3 e rotas estáticas para IPv6 deve incluir ECMP (Equal Cost Multi Path).
1.2.75. Implementar BFD (Bidirectional Forwarding Detection).
1.2.76. Implementar Policy Based Routing.
1.2.77. Implementar upload e download de configuração em formato ASCII ou XML, permitindo a edição do arquivo de configuração e, posteriormente, o download do arquivo editado para o equipamento.
1.2.78. Implementar TACACS+ segundo a RFC 1492.
1.2.79. "Implementar autenticação RADIUS com suporte a:
1.2.79.1. RFC 2865 RADIUS Authentication
1.2.79.2. RFC 2866 RADIUS Accounting
1.2.79.3. RFC 3579 RADIUS EAP support for 802.1X"
1.2.80. A implementação de RADIUS deve suportar alteração dinâmica de parâmetros de autorização de uma sessão que já esteja ativa.
1.2.81. A implementação de RADIUS e TACACS+ deve estar disponível para autenticação de usuários via Telnet e Console serial.
1.2.82. Implementar per-command authorization para RADIUS e TACACS+.
1.2.83. Possuir DNS Client para IPv4 segundo a RFC 1591 e DNS Client para IPv6.
1.2.84. Possuir Telnet client and server segundo a RFC 854.
1.2.85. Implementar os seguintes grupos de RMON através da RFC 1757: History, Statistics, Alarms e Events.
1.2.86. Deve implementar RMON2-probe configuration segundo a RFC 2021, podendo ser implementada internamente no switch ou externamente, por meio de probe em hardware utilizando uma porta 1000BaseTX.
1.2.87. Implementar sFlow ou Netflow, em hardware.
1.2.88. Implementar a atualização de imagens de software e configuração através de um servidor TFTP.
1.2.89. Suportar múltiplos servidores Syslog.
1.2.90. Implementar ajuste de clock do equipamento utilizando NTP com autenticação MD5 e SNTP.
1.2.91. Implementar Port Mirroring, permitindo espelhar até 128 portas físicas ou 16 VLANs para até 16 portas de destino (portas de análise). Deve ser possível configurar mais de uma sessão de espelhamento simultânea.
1.2.92. Implementar RSPAN (Remote Mirroring), permitindo espelhar o tráfego de uma porta ou VLAN de um switch remoto para uma porta de um switch local (porta de análise).
1.2.93. Implementar gerenciamento através de SNMPv1 (RFC 1157), v2c (RFCs 1901 a 1908), v3 (RFCs 3410 a 3415) e SNMP para IPv6.
1.2.94. Implementar SMON de acordo com a RFC 2613.

1.2.95. Implementar cliente e servidor SSHv2.
1.2.96. Implementar cliente e servidor SCP e servidor SFTP.
1.2.97. Implementar gerenciamento via web com suporte a HTTP e HTTPS/SSL, permitindo visualização gráfica da utilização (em percentual, bytes e pacotes) das portas.
1.2.98. A interface gráfica deve permitir visualização de informações do sistema (VLAN, Portas, Fonte e Fans), monitoramento de Log, utilização de portas, QoS e configuração de portas, VLANs e ACLs.
1.2.99. O equipamento ofertado deve possuir um sistema operacional modular.
1.2.100. O sistema operacional deve possuir função grep/pipe para filtrar a saída de determinado comando.
1.2.101. O sistema operacional deve possuir comandos para visualização e monitoração de cada processo, sendo possível verificar por processo qual o consumo de cpu, process-id e qual o consumo de memória por processo.
1.2.102. O sistema operacional deve possuir comandos para que processos sejam terminados ou reiniciados sem que seja necessário a reinicialização do equipamento. Esta funcionalidade deve estar disponível pelo menos para Telnet, TFTP, HTTP e LLDP na versão atual.
1.2.103. Implementar linguagem de scripting baseada em Python, permitindo a automatização de tarefas. A linguagem deve implementar estruturas de controle como loops e execução condicional e permitir a definição de variáveis.
1.2.104. Implementar protocolo de monitoramento de status de comunicação entre dois switches, que possibilite que uma porta seja desabilitada caso seja detectada uma falha de comunicação entre os dois peers.
1.2.105. Implementar funcionalidade que permita sua auto-configuração através dos protocolos DHCP e TFTP, permitindo o provisionamento em massa com o mínimo de intervenção humana.
1.2.106. Deve disponibilizar API (Aplication Programming Interface) aberta para integração com aplicações.
1.2.107. Implementar Rate limiting de entrada em todas as portas. A granularidade deve ser configurável em intervalos de 64Kbps para portas de até 1Gbps. Caso o equipamento ofertado possua suporte a portas 10Gbps, a granularidade para este tipo de interface deve ser configurável em intervalos de 1Mbps. A implementação de Rate Limiting deve permitir a classificação do tráfego utilizando-se ACLs e parâmetros, MAC origem e destino (simultaneamente) IP origem e destino (simultaneamente), portas TCP, portas UDP e campo 802.1p.
1.2.108. Implementar Rate Shaping de saída em todas as portas. A granularidade deve ser configurável em intervalos de 64Kbps para portas de até 1Gbps. Caso o equipamento ofertado possua suporte a portas 10Gbps, a granularidade para este tipo de interface deve ser configurável em intervalos de 1Mbps.
1.2.109. A funcionalidade de Rate Shaping deve permitir a configuração de CIR (Commited Rate), banda máxima, banda mínima e peak rate.
1.2.110. Implementar a leitura, classificação e remarcação de QoS (802.1p e DSCP).
1.2.111. Implementar remarcação de prioridade de pacotes Layer 3, remarcando o campo DiffServ para grupos de tráfego classificados segundo portas TCP e UDP, endereço/subrede IP, VLAN e MAC origem e destino.
1.2.112. Implementar 8 filas de prioridade em hardware por porta.
1.2.113. Implementar os algoritmos de gerenciamento de filas WRR (Weighted Round Robin), WDRR (Weighted Deficit Round Robin) e SP (Strict Priority).
1.2.114. Deve implementar, ao menos dois dos algoritimos acima, simultaneamente em uma mesma porta.
1.2.115. "Implementar as seguintes RFCs:

1.2.115.1. RFC 2474 DiffServ Precedence
1.2.115.2. RFC 2598 DiffServ Expedited Forwarding (EF)
1.2.115.3. RFC 2597 DiffServ Assured Forwarding (AF)
1.2.115.4. RFC 2475 DiffServ Core and Edge Router Functions"
1.2.116. Implementar classificação de tráfego para QoS em Layer1-4 (Policy-Based Mapping) baseado em MAC origem e destino, IP origem e destino, TCP/UDP port, Diffserv e 802.1p.
1.2.117. Implementar detecção de oscilação (flap) de links, permitindo desabilitar uma porta caso a porta oscile acima de um limiar configurado.
1.2.118. Implementar funcionalidade que permita que somente endereços designados por um servidor DHCP tenham acesso à rede.
1.2.119. Implementar funcionalidade que permita que somente servidores DHCP autorizados atribuam configuração IP aos clientes DHCP (Trusted DHCP Server).
1.2.120. Implementar Gratuitous ARP Protection.
1.2.121. Implementar detecção e proteção contra ataques Denial of Service (DoS) direcionados a CPU do equipamento por meio da criação dinâmica e automática de regras para o bloqueio do tráfego suspeito.
1.2.122. Implementar limitação de número de endereços MAC aprendidos por uma porta, para uma determinada VLAN.
1.2.123. Implementar travamento de endereços MAC, permitindo a adição estática de endereços para uma determinada porta ou utilizando os endereços existentes na tabela MAC. O acesso de qualquer outro endereço que não esteja previamente autorizado deve ser negado.
1.2.124. Implementar login de rede baseado no protocolo IEEE 802.1x, permitindo que a porta do switch seja associada a VLAN definida para o usuário no servidor RADIUS.
1.2.125. A implementação do IEEE 802.1x deve incluir suporte a Guest VLAN, encaminhando o usuário para esta VLAN caso este não possua suplicante 802.1x ativo, em caso de falha de autenticação e no caso de indisponibilidade do servidor AAA.
1.2.126. Implementar múltiplos suplicantes por porta, onde cada dispositivo deve ser autenticado de forma independente, podendo ser encaminhados a VLANs distintas. As múltiplas autenticações devem ser realizadas através de IEEE 802.1x.
1.2.127. Implementar autenticação baseada em web, com suporte a SSL, através de RADIUS ou através da base local do switch.
1.2.128. Implementar autenticação baseada em endereço MAC, através de RADIUS ou através da base local do switch.
1.2.129. Implementar ACLs de entrada (ingress ACLs) em hardware, baseadas em critérios da camada 2 (MAC origem e destino e campo 802.1p), camada 3 (IP origem e destino) e camada 4 (portas TCP e UDP), em todas as interfaces e VLANs, com suporte a endereços IPv6.
1.2.130. As ACLs devem ser configuradas para permitir, negar, aplicar QoS, espelhar o tráfego para uma porta de análise, criar entrada de log e incrementar contador.
1.2.131. Implementar funcionalidade que permita a execução de ACLs em um determinado horário do dia (time-based ACLs).
1.2.132. Implementar políticas por usuário, permitindo que as configurações de ACL, QoS sejam aplicadas na porta utilizada para a conexão à rede, após a autenticação.
1.2.133. Implementar a configuração de telefones IP de forma automática, permitindo a detecção do aparelho através do protocolo LLDP e a configuração de VLAN e QoS para a porta.
1.2.134. Implementar a configuração de telefones IP de forma automática, permitindo a detecção do aparelho através do protocolo LLDP e repasse de configuração de VLAN e QoS para o telefone através do protocolo LLDP-MED.

1.2.135. Implementar Policy Based Switching, ou seja, possibilitar que o tráfego classificado por uma ACL seja redirecionado para uma porta física específica.
1.2.136. Implementar funcionalidade que permita o mapeamento de usuários identificados via Kerberos (com a credencial de usuário no domínio), IEEE 802.1x e LLDP, provendo informações como endereço MAC, VLAN e porta física. Estas informações devem estar disponíveis na linha de comando (CLI) do equipamento.
1.2.137. O equipamento ofertado deve permitir que o mesmo faça parte de uma malha ethernet (Fabric Ethernet) descrito nos Switches Core de Rede Tipo I, II e III com as seguintes funcionalidades:
1.2.138. O equipamento ofertado deve permitir a configuração como elemento anexo à malha ethernet;
1.2.139. O equipamento ofertado deve permitir a criação de VLANS mapeadas a serviços virtuais de rede, de que forma os serviços sejam criados automaticamente no elemento de borda da malha e propagados de maneira automática nos demais equipamentos que compõem a malha ethernet
1.2.140. Deve permitir o gerenciamento do equipamento através de software de gerência do Fabric;

1.3. **Switches de acesso Tipo III - 24 portas 10/100/1000 Base-T POE+ + 4 Portas 10Gbe SFP+**
1.3.1. A proposta deverá conter a descrição detalhada com códigos do fabricante de todos os módulos, fontes e acessórios fornecidos.
1.3.2. A solução deve ser composta de um único equipamento, montável em rack 19" devendo este vir acompanhado dos devidos acessórios para tal.
1.3.3. Possuir fonte de alimentação interna que trabalhe em 100V-240V, 50/60 Hz, com detecção automática de tensão e frequência.
1.3.4. Suportar fonte de alimentação redundante externa, montável em rack.
1.3.5. Implementar Power over Ethernet Plus (PoE+) segundo o padrão IEEE 802.3at em todas as portas 1000Base-T, com no mínimo 380W de potência disponível para dispositivos PoE através de fonte interna.
1.3.6. Possuir, no mínimo, 120 Gbps de Switch Fabric.
1.3.7. Possuir capacidade de encaminhamentos de pacotes, de no mínimo 90 Mpps utilizando pacotes de 64 bytes.
1.3.8. Detecção automática MDI/MDIX em todas as portas 10/100/1000BASE-T RJ-45.
1.3.9. Possuir porta de console com conector RJ-45 ou DB9 macho.
1.3.10. Possuir leds indicativos de funcionamento da fonte de alimentação, ventiladores e status das portas.
1.3.11. Possuir 24 portas 10/100/1000BASE-T ativas simultaneamente, com conector RJ-45.
1.3.12. Possuir 4 (quatro) portas 10GBASE-X ativas simultaneamente, baseadas em SFP+, devendo um mesmo slot suportar interfaces 10 Gigabit Ethernet 10GBASE-SR, 10GBASE-LR, 10GBASE-ER e 10GBASE-ZR. Não é permitida a utilização de conversores externos.
1.3.13. O equipamento deve possuir além das portas acima citadas uma porta adicional 10/100 ou 10/100/1000 com conector RJ-45 para gerência out-of-band do equipamento.
1.3.14. Implementar empilhamento de no mínimo oito equipamentos e gerência através de um único endereço IP.
1.3.15. O equipamento deve suportar o agrupamento lógico (gerência por um único IP) de unidades remotamente instaladas (no mínimo a distância de 40km).
1.3.16. O empilhamento deve possuir arquitetura de anel para prover resiliência.
1.3.17. O empilhamento deve ter capacidade de path fast recover, ou seja, com a falha de um dos elementos da pilha os fluxos devem ser reestabelecidos no tempo máximo de 50ms.

1.3.18. Possuir indicação visual no painel frontal do equipamento que permita identificar a posição lógica do equipamento da pilha.
1.3.19. O empilhamento deve permitir a criação de grupos de links agregados entre diferentes membros da pilha, segundo 802.3ad.
1.3.20. O empilhamento deve suportar espelhamento de tráfego entre diferentes unidades da pilha.
1.3.21. Deve ser possível mesclar em uma mesma pilha equipamentos com que não implementem PoE.
1.3.22. A Memória Flash instalada deve ser suficiente para comportar no mínimo duas imagens do Sistema Operacional simultaneamente, permitindo que seja feito um upgrade de Software e a imagem anterior seja mantida.
1.3.23. Todas as interfaces ofertadas devem ser non-blocking.
1.3.24. Possuir altura máxima de 1U (1,75").
1.3.25. Deve armazenar, no mínimo, 16.000 (dezesseis mil) endereços MAC.
1.3.26. Implementar agregação de links conforme padrão IEEE 802.3ad
1.3.27. Possuir homologação da ANATEL, de acordo com a Resolução número 242.
1.3.28. Implementar agregação de links conforme padrão IEEE 802.3ad com suporte a LACP.
1.3.29. Em conjunto com outro equipamento de mesmo modelo, deverá permitir que um switch conectado aos dois, tenha a possibilidade de agregação de links (IEEE 802.3ad) com suporte a LACP com os mesmos, de forma a simular a existência de apenas um único link lógico entre este equipamento e os dois switches do modelo aqui especificado (Multi-Chassis Trunking, por exemplo). O único link lógico entre as camadas deve eliminar convergência do Spanning Tree, possibilitando o tráfego simultâneo por mais de uma conexão.
1.3.30. Implementar jumbo frames em todas as portas ofertadas, com suporte a pacotes de até 9216 Bytes.
1.3.31. Implementar Proxy-ARP (RFC 1027).
1.3.32. Implementar IGMP v1, v2 e v3 Snooping.
1.3.33. Implementar IGMPv1 (RFC 1112), IGMP v2 (RFC 2236) e IGMPv3 (RFC 3376).
1.3.34. Implementar MVR (Multicast VLAN Registration).
1.3.35. Implementar DHCP/Bootp relay configurável por VLAN para IPv4 e IPv6.
1.3.36. Implementar servidor DHCP interno que permita a configuração de um intervalo de endereços IP a serem atribuídos os clientes DHCP e possibilite ainda a atribuição de, no mínimo, default-gateway, servidor DNS e servidor WINS.
1.3.37. Implementar DHCP Option 82, de acordo com a RFC 3046, com identificação de porta e VLAN, configurável por VLAN.
1.3.38. Implementar DHCP Client para IPv4 e IPv6.
1.3.39. Implementar RFC 3021 - Using 31-Bit Prefixes on IPv4 Point-to-Point Links
1.3.40. Implementar Spanning-Tree (IEEE 802.1d), Rapid Spanning Tree (IEEE 802.1w), Multiple Instance STP (802.1s) e PVST+.
1.3.41. Implementar a configuração de Multiple Spanning Tree Protocol, com suporte a, pelo menos, 32 domínios.
1.3.42. Implementar funcionalidade vinculada ao Spanning-tree onde é possível designar portas de acesso (por exemplo onde estações estão conectadas) que não sofram o processo de Listening-Learning, passando direto para o estado de Forwarding. No entanto, as portas configuradas com esta funcionalidade devem detectar loops na rede normalmente.
1.3.43. Implementar funcionalidade vinculada ao Spanning-tree que evite a eleição de outros switches da rede como Root.

1.3.44. Implementar funcionalidade vinculada ao Spanning-tree que permita desabilitar uma porta de acesso assim que a mesma receba uma BPDU.
1.3.45. Implementar 4000 VLANs por porta, ativas simultaneamente, através do protocolo 802.1Q.
1.3.46. Deverá permitir a criação, remoção, gerenciamento e distribuição de VLANs de forma dinâmica através de portas configuradas como tronco IEEE 802.1Q utilizando o protocolo MVRP segundo o padrão IEEE802.1ak.
1.3.47. Possibilitar a coleta de estatísticas de tráfego baseada em VLANs IEEE 802.1Q e double-tagged VLANs IEEE 802.1ad.
1.3.48. Implementar MAC Based VLAN.
1.3.49. Implementar VLAN Translation.
1.3.50. Implementar VLAN Aggregation ou funcionalidade que permita o compartilhamento de uma mesma subnet e de um mesmo endereço IPv4 utilizado como default-gateway por hosts de diferentes VLANs.
1.3.51. Implementar Private VLANs.
1.3.52. Implementar Port Isolation ou funcionalidade que permita isolamento de portas específicas do switch. As portas isoladas não devem se comunicar entre si, porém podem se comunicar com qualquer outra porta no equipamento que não esteja isolada.
1.3.53. Implementar IEEE 802.1ad com a possibilidade de associar CVIDs específicos para diferentes SVIDs (selective Q-in-Q ou 802.1ad CEP). A implementação deverá permitir a tradução do CVID.
1.3.54. Implementar IEEE 802.1ag (Connectivity Fault Management).
1.3.55. Implementar IEEE 802.3ah Ethernet OAM – Unidirectional Link Fault Management.
1.3.56. Implementar funcionalidade baseada na recomendação do ITU-T Y.1731 com medição de, no mínimo, Frame Delay.
1.3.57. Implementar o protocolo ITU-T G.8032 ERPS.
1.3.58. Implementar protocolo de resiliência em camada 2, específico para topologias em anel, que permita tempo de convergência inferior a 200 ms.
1.3.59. Implementar IEEE 802.1ab Link Layer Discovery Protocol (LLDP).
1.3.60. Implementar LLDP-MED (Media Endpoint Discovery).
1.3.61. Implementar roteamento estático com suporte a, no mínimo, 480 rotas.
1.3.62. Implementar, no mínimo, 500 interfaces IP (IPv4 ou IPv6).
1.3.63. Implementar os protocolos de roteamento IP: RFC 1058 – RIP v1 e RFC 2453 – RIP v2.
1.3.64. Suportar o protocolo de roteamento OSPFv2, incluindo autenticação MD5.
1.3.65. Implementar o protocolo de roteamento OSPFv2, incluindo autenticação MD5.
1.3.66. Implementar o protocolo de roteamento OSPFv2 (RFC 2328), incluindo autenticação MD5.
1.3.67. Implementar PIM Snooping.
1.3.68. Suportar protocolo de multicast PIM-SM para IPv4 e IPv6.
1.3.69. Suportar PIM-SSM segundo a RFC 3569.
1.3.70. Suportar VRRPv3 (RFC 5798).
1.3.71. "Deve implementar Dual Stack, ou seja, IPv6 e IPv4, com suporte as seguintes funcionalidades/RFCs:
1.3.71.1. RFC 1981, Path MTU Discovery for IPv6, August 1996 - Host Requirements
1.3.71.2. RFC 5095, Internet Protocol, Version 6 (IPv6) Specification
1.3.71.3. RFC 4861, Neighbor Discovery for IP Version 6, (IPv6)
1.3.71.4. RFC 2462, IPv6 Stateless Address Auto configuration - Host Requirements
1.3.71.5. RFC 2463, Internet Control Message Protocol (ICMPv6) for the IPv6 Specification
1.3.71.6. RFC 2464, Transmission of IPv6 Packets over Ethernet Networks
1.3.71.7. RFC 2465, IPv6 MIB, General Group and Textual Conventions

1.3.71.8. RFC 2466, MIB for ICMPv6
1.3.71.9. RFC 3513, Internet Protocol Version 6 (IPv6) Addressing Architecture
1.3.71.10. RFC 3587, Global Unicast Address Format"
1.3.72. Implementar os seguintes protocolos em IPv6: Ping, Traceroute, Telnet, SSHv2, SNMP, Syslog, SNTP e DNS.
1.3.73. "Deve implementar IPv6 de acordo com as seguintes RFCs:
1.3.73.1. RFC 1981, Path MTU Discovery for IPv6, August 1996 - Router Requirements
1.3.73.2. RFC 2462, IPv6 Stateless Address Auto configuration - Router Requirements
1.3.73.3. RFC 2080, RIPng
1.3.73.4. RFC 2462, IPv6 Stateless Address Auto configuration - Router Requirements
1.3.73.5. RFC 2710, IPv6 Multicast Listener Discovery v1 (MLDv1) Protocol
1.3.73.6. RFC 3810, IPv6 Multicast Listener Discovery v2 (MLDv2) Protocol
1.3.73.7. RFC 6106, IPv6 Router Advertisement Options for DNS Configuration
1.3.73.8. Suportar OSPFv3.
1.3.73.9. Implementar OSPFv3 Graceful Restart conforme RFC 5187.
1.3.73.10. A implementação de OSPFv3 e rotas estáticas para IPv6 deve incluir ECMP (Equal Cost Multi Path).
1.3.73.11. Implementar BFD (Bidirectional Forwarding Detection).
1.3.74. Implementar Policy Based Routing.
1.3.75. Implementar upload e download de configuração em formato ASCII ou XML, permitindo a edição do arquivo de configuração e, posteriormente, o download do arquivo editado para o equipamento.
1.3.76. Implementar TACACS+ segundo a RFC 1492.
1.3.77. "Implementar autenticação RADIUS com suporte a:
1.3.77.1. RFC 2865 RADIUS Authentication
1.3.77.2. RFC 2866 RADIUS Accounting
1.3.77.3. RFC 3579 RADIUS EAP support for 802.1X"
1.3.78. A implementação de RADIUS deve suportar alteração dinâmica de parâmetros de autorização de uma sessão que já esteja ativa.
1.3.79. A implementação de RADIUS e TACACS+ deve estar disponível para autenticação de usuários via Telnet e Console serial.
1.3.80. Implementar per-command authorization para RADIUS e TACACS+.
1.3.81. Possuir DNS Client para IPv4 segundo a RFC 1591 e DNS Client para IPv6.
1.3.82. Possuir Telnet client and server segundo a RFC 854.
1.3.83. Implementar os seguintes grupos de RMON através da RFC 1757: History, Statistics, Alarms e Events.
1.3.84. Deve implementar RMON2-probe configuration segundo a RFC 2021, podendo ser implementada internamente no switch ou externamente, por meio de probe em hardware utilizando uma porta 1000BaseTX.
1.3.85. Implementar sFlow ou Netflow, em hardware.
1.3.86. Implementar a atualização de imagens de software e configuração através de um servidor TFTP.
1.3.87. Suportar múltiplos servidores Syslog.
1.3.88. Implementar ajuste de clock do equipamento utilizando NTP com autenticação MD5 e SNTP.
1.3.89. Implementar Port Mirroring, permitindo espelhar até 128 portas físicas ou 16 VLANs para até 16 portas de destino (portas de análise). Deve ser possível configurar mais de uma sessão de espelhamento simultânea.

1.3.90. Implementar RSPAN (Remote Mirroring), permitindo espelhar o tráfego de uma porta ou VLAN de um switch remoto para uma porta de um switch local (porta de análise).
1.3.91. Implementar gerenciamento através de SNMPv1 (RFC 1157), v2c (RFCs 1901 a 1908), v3 (RFCs 3410 a 3415) e SNMP para IPv6.
1.3.92. Implementar SMON de acordo com a RFC 2613.
1.3.93. Implementar cliente e servidor SSHv2.
1.3.94. Implementar cliente e servidor SCP e servidor SFTP.
1.3.95. Implementar gerenciamento via web com suporte a HTTP e HTTPS/SSL, permitindo visualização gráfica da utilização (em percentual, bytes e pacotes) das portas.
1.3.96. A interface gráfica deve permitir visualização de informações do sistema (VLAN, Portas, Fonte e Fans), monitoramento de Log, utilização de portas, QoS e configuração de portas, VLANs e ACLs.
1.3.97. O equipamento ofertado deve possuir um sistema operacional modular.
1.3.98. O sistema operacional deve possuir função grep/pipe para filtrar a saída de determinado comando.
1.3.99. O sistema operacional deve possuir comandos para visualização e monitoração de cada processo, sendo possível verificar por processo qual o consumo de cpu, process-id e qual o consumo de memória por processo.
1.3.100. O sistema operacional deve possuir comandos para que processos sejam terminados ou reiniciados sem que seja necessário a reinicialização do equipamento. Esta funcionalidade deve estar disponível pelo menos para Telnet, TFTP, HTTP e LLDP na versão atual.
1.3.101. Implementar linguagem de scripting baseada em Python, permitindo a automatização de tarefas. A linguagem deve implementar estruturas de controle como loops e execução condicional e permitir a definição de variáveis.
1.3.102. Implementar protocolo de monitoramento de status de comunicação entre dois switches, que possibilite que uma porta seja desabilitada caso seja detectada uma falha de comunicação entre os dois peers.
1.3.103. Implementar funcionalidade que permita sua auto-configuração através dos protocolos DHCP e TFTP, permitindo o provisionamento em massa com o mínimo de intervenção humana.
1.3.104. Deve disponibilizar API (Aplication Programming Interface) aberta para integração com aplicações.
1.3.105. Implementar Rate limiting de entrada em todas as portas. A granularidade deve ser configurável em intervalos de 64Kbps para portas de até 1Gbps. Caso o equipamento ofertado possua suporte a portas 10Gbps, a granularidade para este tipo de interface deve ser configurável em intervalos de 1Mbps. A implementação de Rate Limiting deve permitir a classificação do tráfego utilizando-se ACLs e parâmetros, MAC origem e destino (simultaneamente) IP origem e destino (simultaneamente), portas TCP, portas UDP e campo 802.1p.
1.3.106. Implementar Rate Shaping de saída em todas as portas. A granularidade deve ser configurável em intervalos de 64Kbps para portas de até 1Gbps. Caso o equipamento ofertado possua suporte a portas 10Gbps, a granularidade para este tipo de interface deve ser configurável em intervalos de 1Mbps.
1.3.107. A funcionalidade de Rate Shaping deve permitir a configuração de CIR (Commited Rate), banda máxima, banda mínima e peak rate.
1.3.108. Implementar a leitura, classificação e remarcação de QoS (802.1p e DSCP).
1.3.109. Implementar remarcação de prioridade de pacotes Layer 3, remarcando o campo DiffServ para grupos de tráfego classificados segundo portas TCP e UDP, endereço/subrede IP, VLAN e MAC origem e destino.
1.3.110. Implementar 8 filas de prioridade em hardware por porta.

1.3.111. Implementar os algoritmos de gerenciamento de filas WRR (Weighted Round Robin), WDRR (Weighted Deficit Round Robin) e SP (Strict Priority).
1.3.112. Deve implementar, ao menos dois dos algoritimos acima, simultaneamente em uma mesma porta.
1.3.113. "Implementar as seguintes RFCs:
1.3.113.1. RFC 2474 DiffServ Precedence
1.3.113.2. RFC 2598 DiffServ Expedited Forwarding (EF)
1.3.113.3. RFC 2597 DiffServ Assured Forwarding (AF)
1.3.113.4. RFC 2475 DiffServ Core and Edge Router Functions"
1.3.114. Implementar classificação de tráfego para QoS em Layer1-4 (Policy-Based Mapping) baseado em MAC origem e destino, IP origem e destino, TCP/UDP port, Diffserv e 802.1p.
1.3.115. Implementar detecção de oscilação (flap) de links, permitindo desabilitar uma porta caso a porta oscile acima de um limiar configurado.
1.3.116. Implementar funcionalidade que permita que somente endereços designados por um servidor DHCP tenham acesso à rede.
1.3.117. Implementar funcionalidade que permita que somente servidores DHCP autorizados atribuam configuração IP aos clientes DHCP (Trusted DHCP Server).
1.3.118. Implementar Gratuitous ARP Protection.
1.3.119. Implementar detecção e proteção contra ataques Denial of Service (DoS) direcionados a CPU do equipamento por meio da criação dinâmica e automática de regras para o bloqueio do tráfego suspeito.
1.3.120. Implementar limitação de número de endereços MAC aprendidos por uma porta, para uma determinada VLAN.
1.3.121. Implementar travamento de endereços MAC, permitindo a adição estática de endereços para uma determinada porta ou utilizando os endereços existentes na tabela MAC. O acesso de qualquer outro endereço que não esteja previamente autorizado deve ser negado.
1.3.122. Implementar login de rede baseado no protocolo IEEE 802.1x, permitindo que a porta do switch seja associada a VLAN definida para o usuário no servidor RADIUS.
1.3.123. A implementação do IEEE 802.1x deve incluir suporte a Guest VLAN, encaminhando o usuário para esta VLAN caso este não possua suplicante 802.1x ativo, em caso de falha de autenticação e no caso de indisponibilidade do servidor AAA.
1.3.124. Implementar múltiplos suplicantes por porta, onde cada dispositivo deve ser autenticado de forma independente, podendo ser encaminhados a VLANs distintas. As múltiplas autenticações devem ser realizadas através de IEEE 802.1x.
1.3.125. Implementar autenticação baseada em web, com suporte a SSL, através de RADIUS ou através da base local do switch.
1.3.126. Implementar autenticação baseada em endereço MAC, através de RADIUS ou através da base local do switch.
1.3.127. Implementar ACLs de entrada (ingress ACLs) em hardware, baseadas em critérios da camada 2 (MAC origem e destino e campo 802.1p), camada 3 (IP origem e destino) e camada 4 (portas TCP e UDP), em todas as interfaces e VLANs, com suporte a endereços IPv6.
1.3.128. As ACLs devem ser configuradas para permitir, negar, aplicar QoS, espelhar o tráfego para uma porta de análise, criar entrada de log e incrementar contador.
1.3.129. Implementar funcionalidade que permita a execução de ACLs em um determinado horário do dia (time-based ACLs).
1.3.130. Implementar políticas por usuário, permitindo que as configurações de ACL, QoS sejam aplicadas na porta utilizada para a conexão à rede, após a autenticação.

1.3.131. Implementar a configuração de telefones IP de forma automática, permitindo a detecção do aparelho através do protocolo LLDP e a configuração de VLAN e QoS para a porta.
1.3.132. Implementar a configuração de telefones IP de forma automática, permitindo a detecção do aparelho através do protocolo LLDP e repasse de configuração de VLAN e QoS para o telefone através do protocolo LLDP-MED.
1.3.133. Implementar Policy Based Switching, ou seja, possibilitar que o tráfego classificado por uma ACL seja redirecionado para uma porta física específica.
1.3.134. Implementar funcionalidade que permita o mapeamento de usuários identificados via Kerberos (com a credencial de usuário no domínio), IEEE 802.1x e LLDP, provendo informações como endereço MAC, VLAN e porta física. Estas informações devem estar disponíveis na linha de comando (CLI) do equipamento.
1.3.135. O equipamento ofertado deve permitir que o mesmo faça parte de um malha ethernet (Fabric Ethernet) descrito nos Switches Core de Rede Tipo I, II e III com as seguintes funcionalidades:
1.3.136. O equipamento ofertado deve permitir a configuração como elemento anexo à malha ethernet;
1.3.137. O equipamento ofertado deve permitir a criação de VLANS mapeadas a serviços virtuais de rede, de que forma os serviços sejam criados automaticamente no elemento de borda da malha e propagados de maneira automática nos demais equipamentos que compõem a malha ethernet
1.3.138. Deve permitir o gerenciamento do equipamento através de software de gerência do Fabric;

1.4. **Switches de acesso Tipo IV - 24 portas 10/100/1000 Base-T + 4 Portas 10Gbe SFP+**
1.4.1. A proposta deverá conter a descrição detalhada com códigos do fabricante de todos os módulos, fontes e acessórios fornecidos.
1.4.2. A solução deve ser composta de um único equipamento, montável em rack 19" devendo este vir acompanhado dos devidos acessórios para tal.
1.4.3. Possuir fonte de alimentação interna que trabalhe em 100V-240V, 50/60 Hz, com detecção automática de tensão e frequência.
1.4.4. Suportar fonte de alimentação redundante externa, montável em rack.
1.4.5. Possuir, no mínimo, 120 Gbps de Switch Fabric.
1.4.6. Possuir capacidade de encaminhamento de pacotes, de no mínimo 90 Mpps utilizando pacotes de 64 bytes.
1.4.7. Detecção automática MDI/MDIX em todas as portas 10/100/1000BASE-T RJ-45.
1.4.8. Possuir porta de console com conector RJ-45 ou DB9 macho.
1.4.9. Possuir leds indicativos de funcionamento da fonte de alimentação, ventiladores e status das portas.
1.4.10. Possuir 24 portas 10/100/1000BASE-T ativas simultaneamente, com conector RJ-45.
1.4.11. Possuir 4 (quatro) portas 10GBASE-X ativas simultaneamente, baseadas em SFP+, devendo um mesmo slot suportar interfaces 10 Gigabit Ethernet 10GBASE-SR, 10GBASE-LR, 10GBASE-ER e 10GBASE-ZR. Não é permitida a utilização de conversores externos.
1.4.12. O equipamento deve possuir além das portas acima citadas uma porta adicional 10/100 ou 10/100/1000 com conector RJ-45 para gerência out-of-band do equipamento.
1.4.13. Implementar empilhamento de no mínimo oito equipamentos e gerência através de um único endereço IP.
1.4.14. O equipamento deve suportar o agrupamento lógico (gerência por um único IP) de unidades remotamente instaladas.
1.4.15. O empilhamento deve possuir arquitetura de anel para prover resiliência.
1.4.16. O empilhamento deve ter capacidade de path fast recover, ou seja, com a falha de um dos

elementos da pilha os fluxos devem ser reestabelecidos no tempo máximo de 50ms.
1.4.17. Possuir indicação visual no painel frontal do equipamento que permita identificar a posição lógica do equipamento da pilha.
1.4.18. O empilhamento deve permitir a criação de grupos de links agregados entre diferentes membros da pilha, segundo 802.3ad.
1.4.19. O empilhamento deve suportar espelhamento de tráfego entre diferentes unidades da pilha.
1.4.20. Deve ser possível mesclar em uma mesma pilha equipamentos que não implementem PoE.
1.4.21. A Memória Flash instalada deve ser suficiente para comportar no mínimo duas imagens do Sistema Operacional simultaneamente, permitindo que seja feito um upgrade de Software e a imagem anterior seja mantida.
1.4.22. Todas as interfaces ofertadas devem ser non-blocking.
1.4.23. Possuir altura máxima de 1U (1,75").
1.4.24. Deve armazenar, no mínimo, 16.000 (dezesseis mil) endereços MAC.
1.4.25. Implementar agregação de links conforme padrão IEEE 802.3ad
1.4.26. Possuir homologação da ANATEL, de acordo com a Resolução número 242.
1.4.27. Implementar agregação de links conforme padrão IEEE 802.3ad com suporte a LACP.
1.4.28. Em conjunto com outro equipamento de mesmo modelo, deverá permitir que um switch conectado aos dois, tenha a possibilidade de agregação de links (IEEE 802.3ad) com suporte a LACP com os mesmos, de forma a simular a existência de apenas um único link lógico entre este equipamento e os dois switches do modelo aqui especificado (Multi-Chassis Trunking, por exemplo). O único link lógico entre as camadas deve eliminar convergência do Spanning Tree, possibilitando o tráfego simultâneo por mais de uma conexão.
1.4.29. Implementar jumbo frames em todas as portas ofertadas, com suporte a pacotes de até 9216 Bytes.
1.4.30. Implementar Proxy-ARP (RFC 1027).
1.4.31. Implementar IGMP v1, v2 e v3 Snooping.
1.4.32. Implementar IGMPv1 (RFC 1112), IGMP v2 (RFC 2236) e IGMPv3 (RFC 3376).
1.4.33. Implementar MVR (Multicast VLAN Registration).
1.4.34. Implementar DHCP/Bootp relay configurável por VLAN para IPv4 e IPv6.
1.4.35. Implementar servidor DHCP interno que permita a configuração de um intervalo de endereços IP a serem atribuídos os clientes DHCP e possibilite ainda a atribuição de, no mínimo, default-gateway, servidor DNS e servidor WINS.
1.4.36. Implementar DHCP Option 82, de acordo com a RFC 3046, com identificação de porta e VLAN, configurável por VLAN.
1.4.37. Implementar DHCP Client para IPv4 e IPv6.
1.4.38. Implementar RFC 3021 - Using 31-Bit Prefixes on IPv4 Point-to-Point Links
1.4.39. Implementar Spanning-Tree (IEEE 802.1d), Rapid Spanning Tree (IEEE 802.1w), Multiple Instance STP (802.1s) e PVST+.
1.4.40. Implementar a configuração de Multiple Spanning Tree Protocol, com suporte a, pelo menos, 32 domínios.
1.4.41. Implementar funcionalidade vinculada ao Spanning-tree onde é possível designar portas de acesso (por exemplo onde estações estão conectadas) que não sofram o processo de Listening-Learning, passando direto para o estado de Forwarding. No entanto, as portas configuradas com esta funcionalidade devem detectar loops na rede normalmente.
1.4.42. Implementar funcionalidade vinculada ao Spanning-tree que evite a eleição de outros switches da rede como Root.
1.4.43. Implementar funcionalidade vinculada ao Spanning-tree que permita desabilitar uma porta de

acesso assim que a mesma receba uma BPDU.
1.4.44. Implementar 4000 VLANs por porta, ativas simultaneamente, através do protocolo 802.1Q.
1.4.45. Deverá permitir a criação, remoção, gerenciamento e distribuição de VLANs de forma dinâmica através de portas configuradas como tronco IEEE 802.1Q utilizando o protocolo MVRP segundo o padrão IEEE802.1ak.
1.4.46. Possibilitar a coleta de estatísticas de tráfego baseada em VLANs IEEE 802.1Q e double-tagged VLANs IEEE 802.1ad.
1.4.47. Implementar MAC Based VLAN.
1.4.48. Implementar VLAN Translation.
1.4.49. Implementar VLAN Aggregation ou funcionalidade que permita o compartilhamento de uma mesma subnet e de um mesmo endereço IPv4 utilizado como default-gateway por hosts de diferentes VLANs.
1.4.50. Implementar Private VLANs.
1.4.51. Implementar Port Isolation ou funcionalidade que permita isolamento de portas específicas do switch. As portas isoladas não devem se comunicar entre si, porém podem se comunicar com qualquer outra porta no equipamento que não esteja isolada.
1.4.52. Implementar IEEE 802.1ad com a possibilidade de associar CVIDs específicos para diferentes SVIDs (selective Q-in-Q ou 802.1ad CEP). A implementação deverá permitir a tradução do CVID.
1.4.53. Implementar IEEE 802.1ag (Connectivity Fault Management).
1.4.54. Implementar IEEE 802.3ah Ethernet OAM – Unidirectional Link Fault Management.
1.4.55. Implementar funcionalidade baseada na recomendação do ITU-T Y.1731 com medição de, no mínimo, Frame Delay.
1.4.56. Implementar o protocolo ITU-T G.8032 ERPS.
1.4.57. Implementar protocolo de resiliência em camada 2, específico para topologias em anel, que permita tempo de convergência inferior a 200 ms.
1.4.58. Implementar IEEE 802.1ab Link Layer Discovery Protocol (LLDP).
1.4.59. Implementar LLDP-MED (Media Endpoint Discovery).
1.4.60. Implementar roteamento estático com suporte a, no mínimo, 480 rotas.
1.4.61. Implementar, no mínimo, 500 interfaces IP (IPv4 ou IPv6).
1.4.62. Implementar os protocolos de roteamento IP: RFC 1058 – RIP v1 e RFC 2453 – RIP v2.
1.4.63. Suportar o protocolo de roteamento OSPFv2, incluindo autenticação MD5.
1.4.64. Implementar PIM Snooping.
1.4.65. Suportar protocolo de multicast PIM-SM para IPv4 e IPv6.
1.4.66. Suportar PIM-SSM segundo a RFC 3569.
1.4.67. Suportar VRRPv3 (RFC 5798).
1.4.68. "Deve implementar Dual Stack, ou seja, IPv6 e IPv4, com suporte as seguintes funcionalidades/RFCs:
1.4.68.1. RFC 1981, Path MTU Discovery for IPv6, August 1996 - Host Requirements
1.4.68.2. RFC 5095, Internet Protocol, Version 6 (IPv6) Specification
1.4.68.3. RFC 4861, Neighbor Discovery for IP Version 6, (IPv6)
1.4.68.4. RFC 2462, IPv6 Stateless Address Auto configuration - Host Requirements
1.4.68.5. RFC 2463, Internet Control Message Protocol (ICMPv6) for the IPv6 Specification
1.4.68.6. RFC 2464, Transmission of IPv6 Packets over Ethernet Networks
1.4.68.7. RFC 2465, IPv6 MIB, General Group and Textual Conventions
1.4.68.8. RFC 2466, MIB for ICMPv6
1.4.68.9. RFC 3513, Internet Protocol Version 6 (IPv6) Addressing Architecture
1.4.68.10. RFC 3587, Global Unicast Address Format"

1.4.69. Implementar os seguintes protocolos em IPv6: Ping, Traceroute, Telnet, SSHv2, SNMP, Syslog, SNTP e DNS.
1.4.70. "Deve implementar IPv6 de acordo com as seguintes RFCs:
1.4.70.1. RFC 1981, Path MTU Discovery for IPv6, August 1996 - Router Requirements
1.4.70.2. RFC 2462, IPv6 Stateless Address Auto configuration - Router Requirements
1.4.70.3. RFC 2080, RIPng
1.4.70.4. RFC 2462, IPv6 Stateless Address Auto configuration - Router Requirements
1.4.70.5. RFC 2710, IPv6 Multicast Listener Discovery v1 (MLDv1) Protocol
1.4.70.6. RFC 3810, IPv6 Multicast Listener Discovery v2 (MLDv2) Protocol
1.4.70.7. RFC 6106, IPv6 Router Advertisement Options for DNS Configuration
1.4.70.8. Suportar OSPFv3.
1.4.70.9. Implementar OSPFv3 Graceful Restart conforme RFC 5187.
1.4.70.10. A implementação de OSPFv3 e rotas estáticas para IPv6 deve incluir ECMP (Equal Cost Multi Path).
1.4.70.11. Implementar BFD (Bidirectional Forwarding Detection).
1.4.71. Implementar Policy Based Routing.
1.4.72. Implementar upload e download de configuração em formato ASCII ou XML, permitindo a edição do arquivo de configuração e, posteriormente, o download do arquivo editado para o equipamento.
1.4.73. Implementar TACACS+ segundo a RFC 1492.
1.4.74. "Implementar autenticação RADIUS com suporte a:
1.4.74.1. RFC 2865 RADIUS Authentication
1.4.74.2. RFC 2866 RADIUS Accounting
1.4.74.3. RFC 3579 RADIUS EAP support for 802.1X"
1.4.75. A implementação de RADIUS deve suportar alteração dinâmica de parâmetros de autorização de uma sessão que já esteja ativa.
1.4.76. A implementação de RADIUS e TACACS+ deve estar disponível para autenticação de usuários via Telnet e Console serial.
1.4.77. Implementar per-command authorization para RADIUS e TACACS+.
1.4.78. Possuir DNS Client para IPv4 segundo a RFC 1591 e DNS Client para IPv6.
1.4.79. Possuir Telnet client and server segundo a RFC 854.
1.4.80. Implementar os seguintes grupos de RMON através da RFC 1757: History, Statistics, Alarms e Events.
1.4.81. Deve implementar RMON2-probe configuration segundo a RFC 2021, podendo ser implementada internamente no switch ou externamente, por meio de probe em hardware utilizando uma porta 1000BaseTX.
1.4.82. Implementar sFlow ou Netflow, em hardware.
1.4.83. Implementar a atualização de imagens de software e configuração através de um servidor TFTP.
1.4.84. Suportar múltiplos servidores Syslog.
1.4.85. Implementar ajuste de clock do equipamento utilizando NTP com autenticação MD5 e SNTP.
1.4.86. Implementar Port Mirroring, permitindo espelhar até 128 portas físicas ou 16 VLANs para até 16 portas de destino (portas de análise). Deve ser possível configurar mais de uma sessão de espelhamento simultânea.
1.4.87. Implementar RSPAN (Remote Mirroring), permitindo espelhar o tráfego de uma porta ou VLAN de um switch remoto para uma porta de um switch local (porta de análise).
1.4.88. Implementar gerenciamento através de SNMPv1 (RFC 1157), v2c (RFCs 1901 a 1908), v3 (RFCs

3410 a 3415) e SNMP para IPv6.
1.4.89. Implementar SMON de acordo com a RFC 2613.
1.4.90. Implementar cliente e servidor SSHv2.
1.4.91. Implementar cliente e servidor SCP e servidor SFTP.
1.4.92. Implementar gerenciamento via web com suporte a HTTP e HTTPS/SSL, permitindo visualização gráfica da utilização (em percentual, bytes e pacotes) das portas.
1.4.93. A interface gráfica deve permitir visualização de informações do sistema (VLAN, Portas, Fonte e Fans), monitoramento de Log, utilização de portas, QoS e configuração de portas, VLANs e ACLs.
1.4.94. O equipamento ofertado deve possuir um sistema operacional modular.
1.4.95. O sistema operacional deve possuir função grep/pipe para filtrar a saída de determinado comando.
1.4.96. O sistema operacional deve possuir comandos para visualização e monitoração de cada processo, sendo possível verificar por processo qual o consumo de cpu, process-id e qual o consumo de memória por processo.
1.4.97. O sistema operacional deve possuir comandos para que processos sejam terminados ou reiniciados sem que seja necessário a reinicialização do equipamento. Esta funcionalidade deve estar disponível pelo menos para Telnet, TFTP, HTTP e LLDP na versão atual.
1.4.98. Implementar linguagem de scripting baseada em Python, permitindo a automatização de tarefas. A linguagem deve implementar estruturas de controle como loops e execução condicional e permitir a definição de variáveis.
1.4.99. Implementar protocolo de monitoramento de status de comunicação entre dois switches, que possibilite que uma porta seja desabilitada caso seja detectada uma falha de comunicação entre os dois peers.
1.4.100. Implementar funcionalidade que permita sua auto-configuração através dos protocolos DHCP e TFTP, permitindo o provisionamento em massa com o mínimo de intervenção humana.
1.4.101. Deve disponibilizar API (Aplication Programming Interface) aberta para integração com aplicações.
1.4.102. Implementar Rate limiting de entrada em todas as portas. A granularidade deve ser configurável em intervalos de 64Kbps para portas de até 1Gbps. Caso o equipamento ofertado possua suporte a portas 10Gbps, a granularidade para este tipo de interface deve ser configurável em intervalos de 1Mbps. A implementação de Rate Limiting deve permitir a classificação do tráfego utilizando-se ACLs e parâmetros, MAC origem e destino (simultaneamente) IP origem e destino (simultaneamente), portas TCP, portas UDP e campo 802.1p.
1.4.103. Implementar Rate Shaping de saída em todas as portas. A granularidade deve ser configurável em intervalos de 64Kbps para portas de até 1Gbps. Caso o equipamento ofertado possua suporte a portas 10Gbps, a granularidade para este tipo de interface deve ser configurável em intervalos de 1Mbps.
1.4.104. A funcionalidade de Rate Shaping deve permitir a configuração de CIR (Commited Rate), banda máxima, banda mínima e peak rate.
1.4.105. Implementar a leitura, classificação e remarcação de QoS (802.1p e DSCP).
1.4.106. Implementar remarcação de prioridade de pacotes Layer 3, remarcando o campo DiffServ para grupos de tráfego classificados segundo portas TCP e UDP, endereço/subrede IP, VLAN e MAC origem e destino.
1.4.107. Implementar 8 filas de prioridade em hardware por porta.
1.4.108. Implementar os algoritmos de gerenciamento de filas WRR (Weighted Round Robin), WDRR (Weighted Deficit Round Robin) e SP (Strict Priority).
1.4.109. Deve implementar, ao menos dois dos algoritimos acima, simultaneamente em uma mesma

porta.
1.4.110. "Implementar as seguintes RFCs:
1.4.110.1. RFC 2474 DiffServ Precedence
1.4.110.2. RFC 2598 DiffServ Expedited Forwarding (EF)
1.4.110.3. RFC 2597 DiffServ Assured Forwarding (AF)
1.4.110.4. RFC 2475 DiffServ Core and Edge Router Functions"
1.4.111. Implementar classificação de tráfego para QoS em Layer1-4 (Policy-Based Mapping) baseado em MAC origem e destino, IP origem e destino, TCP/UDP port, Diffserv e 802.1p.
1.4.112. Implementar detecção de oscilação (flap) de links, permitindo desabilitar uma porta caso a porta oscile acima de um limiar configurado.
1.4.113. Implementar funcionalidade que permita que somente endereços designados por um servidor DHCP tenham acesso à rede.
1.4.114. Implementar funcionalidade que permita que somente servidores DHCP autorizados atribuam configuração IP aos clientes DHCP (Trusted DHCP Server).
1.4.115. Implementar Gratuitous ARP Protection.
1.4.116. Implementar detecção e proteção contra ataques Denial of Service (DoS) direcionados a CPU do equipamento por meio da criação dinâmica e automática de regras para o bloqueio do tráfego suspeito.
1.4.117. Implementar limitação de número de endereços MAC aprendidos por uma porta, para uma determinada VLAN.
1.4.118. Implementar travamento de endereços MAC, permitindo a adição estática de endereços para uma determinada porta ou utilizando os endereços existentes na tabela MAC. O acesso de qualquer outro endereço que não esteja previamente autorizado deve ser negado.
1.4.119. Implementar login de rede baseado no protocolo IEEE 802.1x, permitindo que a porta do switch seja associada a VLAN definida para o usuário no servidor RADIUS.
1.4.120. A implementação do IEEE 802.1x deve incluir suporte a Guest VLAN, encaminhando o usuário para esta VLAN caso este não possua suplicante 802.1x ativo, em caso de falha de autenticação e no caso de indisponibilidade do servidor AAA.
1.4.121. Implementar múltiplos suplicantes por porta, onde cada dispositivo deve ser autenticado de forma independente, podendo ser encaminhados a VLANs distintas. As múltiplas autenticações devem ser realizadas através de IEEE 802.1x.
1.4.122. Implementar autenticação baseada em web, com suporte a SSL, através de RADIUS ou através da base local do switch.
1.4.123. Implementar autenticação baseada em endereço MAC, através de RADIUS ou através da base local do switch.
1.4.124. Implementar ACLs de entrada (ingress ACLs) em hardware, baseadas em critérios da camada 2 (MAC origem e destino e campo 802.1p), camada 3 (IP origem e destino) e camada 4 (portas TCP e UDP), em todas as interfaces e VLANs, com suporte a endereços IPv6.
1.4.125. As ACLs devem ser configuradas para permitir, negar, aplicar QoS, espelhar o tráfego para uma porta de análise, criar entrada de log e incrementar contador.
1.4.126. Implementar funcionalidade que permita a execução de ACLs em um determinado horário do dia (time-based ACLs).
1.4.127. Implementar políticas por usuário, permitindo que as configurações de ACL, QoS sejam aplicadas na porta utilizada para a conexão à rede, após a autenticação.
1.4.128. Implementar a configuração de telefones IP de forma automática, permitindo a detecção do aparelho através do protocolo LLDP e a configuração de VLAN e QoS para a porta.
1.4.129. Implementar a configuração de telefones IP de forma automática, permitindo a detecção do

52
ASR

aparelho através do protocolo LLDP e repasse de configuração de VLAN e QoS para o telefone através do protocolo LLDP-MED.
1.4.130. Implementar Policy Based Switching, ou seja, possibilitar que o tráfego classificado por uma ACL seja redirecionado para uma porta física específica.
1.4.131. Implementar funcionalidade que permita o mapeamento de usuários identificados via Kerberos (com a credencial de usuário no domínio), IEEE 802.1x e LLDP, provendo informações como endereço MAC, VLAN e porta física. Estas informações devem estar disponíveis na linha de comando (CLI) do equipamento.
1.4.132. O equipamento ofertado deve permitir que o mesmo faça parte de uma malha ethernet (Fabric Ethernet) descrito nos Switches Core de Rede Tipo I, II e III com as seguintes funcionalidades:
1.4.133. O equipamento ofertado deve permitir a configuração como elemento anexo à malha ethernet;
1.4.134. O equipamento ofertado deve permitir a criação de VLANS mapeadas a serviços virtuais de rede, de que forma os serviços sejam criados automaticamente no elemento de borda da malha e propagados de maneira automática nos demais equipamentos que compõem a malha ethernet
1.4.135. Deve permitir o gerenciamento do equipamento através de software de gerência do Fabric;

1.5. **Switch Core de Rede Tipo I - 48 portas 10/25 Gbps SFP28 portas, 7 portas QSFP 28**
1.5.1. A proposta deverá conter a descrição detalhada com códigos do fabricante de todos os módulos, fontes e acessórios fornecidos.
1.5.2. A solução deve ser composta de um único equipamento, montável em rack 19" devendo este vir acompanhado dos devidos acessórios para tal.
1.5.3. Possuir fonte de alimentação interna que trabalhe em 110V/220V, 50/60 Hz, com detecção automática de tensão e frequência, hot-swappable.
1.5.4. Possuir fonte de alimentação AC redundante interna, hot-swappable.
1.5.5. Possuir bandeja de ventiladores substituível em campo (field replaceable e hot swappable).
1.5.6. Possuir ventilação "front-to-back", ou seja a saída de ar quente deve acontecer pela traseira do equipamento.
1.5.7. Suportar capacidade agregada de switching de, no mínimo, 4.0 Tbps.
1.5.8. Suportar capacidade de encaminhamento de pacotes, de no mínimo 970 Mpps utilizando pacotes de 64 bytes.
1.5.9. Possuir porta de console com conector RJ-45 ou DB9 macho.
1.5.10. Possuir uma porta Micro-USB para transferência de arquivos.
1.5.11. Possuir leds indicativos de funcionamento da fonte de alimentação, ventiladores e status das portas.
1.5.12. Possuir 48 portas 1/10/25Gb ativas simultaneamente, baseadas em SFP28, devendo um mesmo slot suportar interfaces 25GBASE-SR e 25GBASE-LR.
1.5.13. Possuir 7 portas 40/100Gb ativas simultaneamente, baseadas em QSFP28, devendo um mesmo slot suportar interfaces 100GBASE-SR4 e 100GBASE-LR4.
1.5.14. O equipamento deve possuir, além das portas acima citadas, uma porta adicional 10/100/1000 com conector RJ-45 para gerência out-of-band do equipamento.
1.5.15. A Memória Flash instalada deve ser suficiente para comportar no mínimo duas imagens do Sistema Operacional simultaneamente, permitindo que seja feito um upgrade de Software e a imagem anterior seja mantida.
1.5.16. Possuir altura máxima de 1U (1,75").
1.5.17. Deve suportar o armazenamento de no mínimo 160.000 (cento e sessenta mil) endereços MAC.

53
ASR

1.5.18. Deve suportar o armazenamento de, no mínimo, 16.000 (dezesseis mil) rotas IPv4 em hardware.
1.5.19. Deve suportar o armazenamento de, no mínimo, 7.000 (sete mil) rotas IPv6 em hardware.
1.5.20. Suportar agregação de links conforme padrão IEEE 802.1AX com, no mínimo, 56 grupos, sendo 8 links agregados por grupo.
1.5.21. Implementar, no mínimo, 500 (quinhentas) regras de ACL de entrada (ingress ACLs).
1.5.22. Implementar, no mínimo, 240 (duzentos e quarenta) regras de ACL de saída (egress ACLs).
1.5.23. Possuir, no mínimo, 4 núcleos de processamento, 16GB de memória RAM e 64GB de armazenamento interno.
1.5.24. Possuir, no mínimo, 4 núcleos de processamento, 16GB de memória RAM e 64GB de armazenamento interno, sendo que parte desses recursos permitam a instalação de máquinas virtuais. Caso a solução ofertada não possua recursos que permitam a instalação de máquinas virtuais, deverá ser fornecido servidor adicional para instalação em rack padrão 19", com, no máximo, 1U de altura e possuir, no mínimo, 4 núcleos de processamento, 8GB de memória RAM, 64GB de armazenamento interno e, no mínimo, 1 (um) porta 10G SFP+.
1.5.25. O equipamento deve suportar VRF (Virtual Routing and Forwarding), com, no mínimo, 24 instâncias.
1.5.26. O equipamento deve suportar VRF (Virtual Routing and Forwarding), com, no mínimo, 256 instâncias.
1.5.27. Suportar funcionamento como gateway VXLAN (VTEP).
1.5.28. Implementar funcionamento como gateway VXLAN (VTEP).
1.5.29. Possuir homologação da ANATEL, de acordo com a Resolução número 242.
1.5.30. Deve permitir automação e escalabilidade de rede utilizando protocolo de malha ethernet (fabric ethernet) baseado em TRILL, SPB ou similar.
1.5.31. A malha ethernet deve implementar, nativamente no equipamento ou via software de gerência externo, mecanismo para estabelecimento de serviços virtualizados de redes lógicas em camada 2, de qualquer ponto da malha ethernet para qualquer outro ponto da malha ethernet, sem necessidade de configuração manual dos equipamentos intermediários entre os pontos que terão os serviços configurados.
1.5.32. A malha ethernet deve implementar, nativamente no equipamento ou via software de gerência externo, mecanismo para estabelecimento de serviços virtualizados de redes lógicas em camada 2 e camada 3, de qualquer ponto da malha ethernet para qualquer outro ponto da malha ethernet, sem necessidade de configuração manual dos equipamentos intermediários entre os pontos que terão os serviços configurados.
1.5.33. A malha ethernet deve permitir criação de serviços virtualizados em camada 3, segmentados por VRF, em que um serviço virtualizado não deverá se comunicar com outro. Deve possuir, ainda, mecanismo para permitir que uma VRF se comunique com outra na malha ethernet para os casos em que a comunicação entre essas seja necessária.
1.5.34. A malha ethernet deve implementar mecanismo para tratamento de tráfego Multicast de forma inteligente, permitindo controle de multicast mesmo dentro de serviços virtualizados da malha ethernet, evitando assim flooding desnecessário para portas que não fazem parte de um mesmo grupo multicast.
1.5.35. O mecanismo para estabelecimento de caminhos de serviços virtualizados em camada 2 deverá ser implementado nativamente no equipamento físico ou via software do mesmo fabricante. Caso a solução ofertada necessite de um software adicional, todas as licenças adicionais para a implementação dessa funcionalidade devem ser fornecidas e deverá funcionar de forma redundante para garantir a alta disponibilidade do ambiente.

1.5.36. O mecanismo para estabelecimento de caminhos de serviços virtualizados em camada 2 e camada 3 deverá ser implementado nativamente no equipamento físico ou via software do mesmo fabricante. Caso a solução ofertada necessite de um software adicional, todas as licenças adicionais para a implementação dessa funcionalidade devem ser fornecidas e deverá funcionar de forma redundante para garantir a alta disponibilidade do ambiente.
1.5.37. A malha ethernet deve ser agnóstica à topologia física.
1.5.38. A malha ethernet deve permitir escalabilidade de, no mínimo, 100 (cem) equipamentos;
1.5.39. A malha ethernet deve permitir a adição de equipamentos do tipo FFF (Fixed Form Factor) e equipamentos do tipo chassi.
1.5.40. A malha ethernet deverá permitir alta disponibilidade em caso de falhas de links e deverá permitir a utilização de todos os links da topologia sem gerar loops.
1.5.41. Implementar agregação de links com suporte a LACP.
1.5.42. Em conjunto com outro equipamento de mesmo modelo, deverá permitir que um switch conectado aos dois, tenha a possibilidade de agregação de links com suporte a LACP com os mesmos, de forma a simular a existência de apenas um único link lógico entre este equipamento e os dois switches do modelo aqui especificado (Multi-Chassis Trunking, por exemplo). O único link lógico entre as camadas deve eliminar convergência do Spanning Tree, possibilitando o tráfego simultâneo por mais de uma conexão.
1.5.43. Implementar jumbo frames em todas as portas ofertadas, com suporte a pacotes de até 9200 Bytes.
1.5.44. Implementar Proxy-ARP (RFC 1027).
1.5.45. Implementar IGMPv1 (RFC 1112), IGMP v2 (RFC 2236) e IGMPv3 (RFC 3376).
1.5.46. Implementar DHCP/Bootp relay.
1.5.47. Implementar DHCP Option 82, de acordo com a RFC 3046.
1.5.48. Implementar DHCP Client (RFC 2131).
1.5.49. Implementar Spanning-Tree (IEEE 802.1d), Rapid Spanning Tree (IEEE 802.1w) e Multiple Instance STP (802.1s).
1.5.50. Implementar a configuração de Multiple Spanning Tree Protocol, com suporte a, pelo menos, 64 instâncias.
1.5.51. Implementar funcionalidade vinculada ao Spanning-tree onde é possível designar portas de acesso (por exemplo onde estações estão conectadas) que não sofram o processo de Listening-Learning, passando direto para o estado de Forwarding. No entanto, as portas configuradas com esta funcionalidade devem detectar loops na rede normalmente.
1.5.52. Implementar funcionalidade vinculada ao Spanning-tree que permita desabilitar uma porta de acesso assim que a mesma receba uma BPDU.
1.5.53. Implementar mecanismo de prevenção contra loops, desabilitando a porta de acesso de forma automática em caso de loop.
1.5.54. Implementar 4000 VLANs por porta, ativas simultaneamente, através do protocolo 802.1Q.
1.5.55. Implementar Private VLAN.
1.5.56. Implementar L2 ping e traceroute de acordo com IEEE 802.1ag (Connectivity Fault Management).
1.5.57. Implementar os protocolos de roteamento IP: RFC 1058 – RIP v1 e RFC 2453 – RIP v2.
1.5.58. Implementar o protocolo de roteamento OSPFv2 (RFC 2328).
1.5.59. Implementar RFC 1587 OSPF NSSA Option.
1.5.60. Implementar protocolo de multicast PIM-SM para IPv4 e IPv6.
1.5.61. Implementar PIM-SSM segundo a RFC 3569.
1.5.62. Implementar ECMP (Equal Cost Multi Path) para rotas IPv4 e IPv6.

1.5.63. Implementar VRRPv3 (RFC 5798).
1.5.64. Deve implementar BGPv4.
1.5.65. "Deve implementar Dual Stack, ou seja, IPv6 e IPv4, com suporte as seguintes funcionalidades/RFCs:
1.5.65.1. RFC 1981, Path MTU Discovery for IPv6, August 1996 - Host Requirements
1.5.65.2. RFC 5095, Internet Protocol, Version 6 (IPv6) Specification
1.5.65.3. RFC 4861, Neighbor Discovery for IP Version 6, (IPv6)
1.5.65.4. RFC 2460, IPv6 base stack
1.5.65.5. RFC 2462, IPv6 Stateless Address Auto configuration - Host Requirements
1.5.65.6. RFC 2463, Internet Control Message Protocol (ICMPv6) for the IPv6 Specification
1.5.65.7. RFC 2464, Transmission of IPv6 Packets over Ethernet Networks
1.5.65.8. RFC 2466, MIB for ICMPv6
1.5.65.9. RFC 3513, Internet Protocol Version 6 (IPv6) Addressing Architecture
1.5.65.10. RFC 3587, Global Unicast Address Format"
1.5.66. "Deve implementar IPv6 de acordo com as seguintes RFCs:
1.5.66.1. RFC 2080, RIPng
1.5.66.2. RFC 2710, IPv6 Multicast Listener Discovery v1 (MLDv1) Protocol
1.5.66.3. RFC 3810, IPv6 Multicast Listener Discovery v2 (MLDv2) Protocol"
1.5.67. Implementar OSPFv3 conforme RFC 5340.
1.5.68. A implementação de OSPFv3 e rotas estáticas para IPv6 deve incluir ECMP (Equal Cost Multi Path).
1.5.69. Implementar Policy Based Routing.
1.5.70. "Implementar autenticação RADIUS com suporte a:
1.5.70.1. RFC 2138 RADIUS Authentication
1.5.70.2. RFC 2139 RADIUS Accounting
1.5.70.3. RFC 3579 RADIUS EAP support for 802.1X"
1.5.71. A implementação de RADIUS deve suportar alteração dinâmica de parâmetros de autorização de uma sessão que já esteja ativa.
1.5.72. A implementação de RADIUS e TACACS+ deve estar disponível para autenticação de usuários via Telnet e Console serial.
1.5.73. Implementar per-command authorization para RADIUS ou TACACS+.
1.5.74. Possuir DNS Client para IPv4 segundo a RFC 1591 e para IPv6 segundo a RFC 2874.
1.5.75. Possuir Telnet client and server segundo a RFC 854.
1.5.76. Implementar os seguintes grupos de RMON através da RFC 2819: History, Statistics, Alarms e Events.
1.5.77. Implementar sFlow ou Netflow.
1.5.78. Implementar a atualização de imagens de software e configuração através de um servidor FTP ou TFTP.
1.5.79. Suportar envio de log para múltiplos servidores Syslog.
1.5.80. Implementar ajuste de clock do equipamento utilizando NTP com autenticação MD5.
1.5.81. Implementar Port Mirroring, permitindo espelhar, no mínimo, 30 portas físicas.
1.5.82. Implementar gerenciamento através de SNMPv1 (RFC 1157), v2 (RFC 2576, RFCs 2578 a 2580 e RFCs 3416 e 3417) e v3 (RFCs 3411 a 3415).
1.5.83. Implementar cliente e servidor SSHv2.
1.5.84. Implementar servidor SCP e servidor SFTP.
1.5.85. Implementar gerenciamento via web com suporte a HTTP e HTTPS.
1.5.86. O sistema operacional deve possuir comandos para visualização do consumo de CPU e

memória RAM.
1.5.87. O sistema operacional deve possuir função grep/pipe para filtrar a saída de determinado comando.
1.5.88. Implementar protocolo de monitoramento de status de comunicação entre dois switches, que possibilite que uma porta seja desabilitada caso seja detectada uma falha de comunicação entre os dois peers.
1.5.89. "Implementar as seguintes RFCs:
1.5.89.1. RFC 2474 DiffServ Precedence
1.5.89.2. RFC 2475 DiffServ Core and Edge Router Functions
1.5.89.3. RFC 2597 DiffServ Assured Forwarding (AF)
1.5.89.4. RFC 2598 DiffServ Expedited Forwarding (EF)"
1.5.90. Deve implementar rate shaping de saída.
1.5.91. Implementar a leitura, classificação e remarcação de QoS DSCP.
1.5.92. Implementar 8 filas de prioridade em hardware por porta.
1.5.93. Implementar os algoritmos de gerenciamento de filas WRR (Weighted Round Robin) e SP (Strict Priority).
1.5.94. Implementar detecção de oscilação (flap) de links, permitindo desabilitar uma porta caso a porta oscile acima de um limiar configurado.
1.5.95. Implementar Gratuitous ARP Protection ou Filtering.
1.5.96. Implementar prevenção contra ataques Denial of Service (DoS).
1.5.97. Implementar ACLs de entrada (ingress ACLs) em hardware, baseadas em critérios da camada 2 (MAC origem e destino e campo 802.1p), camada 3 (IP origem e destino) e camada 4 (portas TCP e UDP), em todas as interfaces e VLANs.
1.5.98. As ACLs devem ser configuradas para permitir, negar, aplicar QoS, espelhar o tráfego para uma porta de análise e incrementar contador.

1.6. **Switch Core de Rede Tipo II - 12 portas 1/10 Gbps SFP+ e 12 portas 1/10 Gbps RJ45**
1.6.1. A proposta deverá conter a descrição detalhada com códigos do fabricante de todos os módulos, fontes e acessórios fornecidos.
1.6.2. A solução deve ser composta de um único equipamento, montável em rack 19" devendo este vir acompanhado dos devidos acessórios para tal.
1.6.3. Possuir fonte de alimentação interna que trabalhe em 110V/220V, 50/60 Hz, com detecção automática de tensão e frequência, hot-swappable.
1.6.4. Possuir fonte de alimentação AC redundante interna, hot-swappable.
1.6.5. Possuir bandeja de ventiladores substituível em campo (field replaceable e hot swappable).
1.6.6. Possuir ventilação "front-to-back", ou seja, a saída de ar quente deve acontecer pela traseira do equipamento.
1.6.7. Suportar capacidade agregada de switching de, no mínimo, 650 Gbps.
1.6.8. Suportar capacidade de encaminhamento de pacotes, de no mínimo 505 Mpps utilizando pacotes de 64 bytes.
1.6.9. Possuir porta de console com conector RJ-45 ou DB9 macho.
1.6.10. Possuir uma porta USB Micro B para gerenciamento.
1.6.11. Possuir, no mínimo, uma porta USB para transferência de arquivos.
1.6.12. Possuir leds indicativos de funcionamento da fonte de alimentação, ventiladores e status das portas.
1.6.13. Possuir 12 portas 1/10GBASE-X ativas simultaneamente, baseadas em SFP+, devendo um mesmo slot suportar interfaces 10 Gigabit Ethernet 10GBASE-SR, 10GBASE-LR, 10GBASE-ER e

10GBASE-ZR e interfaces 1 Gigabit Ethernet 1000BASE-SX, 1000BASE-LX. Não é permitida a utilização de conversores externos. Os transceivers deverão ser do mesmo fabricante dos switches.
1.6.14. Possuir 12 portas 1/10GBASE-T ativas simultaneamente, com conector RJ-45.
1.6.15. O equipamento deve possuir, além das portas acima citadas, uma porta adicional 10/100/1000 com conector RJ-45 para gerência out-of-band do equipamento.
1.6.16. A Memória Flash instalada deve ser suficiente para comportar no mínimo duas imagens do Sistema Operacional simultaneamente, permitindo que seja feito um upgrade de Software e a imagem anterior seja mantida.
1.6.17. "O produto deve permitir a instalação de softwares, seja através de acesso ao sistema operacional ou através de máquina virtual disponível diretamente no equipamento, com as seguintes características:
1.6.18. - Possuir sistema operacional Linux disponível para instalação de pacotes de softwares;
1.6.19. - Permitir a captura de pacotes que atravessem o equipamento sem perda de desempenho através de ferramentas de software, tais como, tcpdump ou Wireshark;
1.6.20. - Permitir a comunicação bidirecional entre softwares que possam ser instalados no equipamento com um ou mais segmentos de rede (tagged ou untagged) simultaneamente;
1.6.21. - O acesso ao sistema operacional ou a máquina virtual deve ser feito através da interface de gerência ou de uma interface dedicada para esta função, para que os dados coletados possam ser enviados a um servidor sem interferir na comunicação de de dados da rede de produção. "
1.6.22. Possuir altura máxima de 1U (1,75").
1.6.23. Deve suportar o armazenamento de no mínimo 80.000 (oitenta mil) endereços MAC.
1.6.24. Deve suportar o armazenamento de, no mínimo, 15.000 (quinze mil) rotas IPv4 em hardware.
1.6.25. Deve suportar o armazenamento de, no mínimo, 7.000 (sete mil) rotas IPv6 em hardware.
1.6.26. Suportar agregação de links conforme padrão IEEE 802.1AX com, no mínimo, 24 grupos, sendo 8 links agregados por grupo.
1.6.27. Implementar, no mínimo, 500 (quinhentas) regras de ACL de entrada (ingress ACLs).
1.6.28. Implementar, no mínimo, 120 (cento e vinte) regras de ACL de saída (egress ACLs).
1.6.29. O equipamento deve suportar VRF (Virtual Routing and Forwarding), com, no mínimo, 24 instâncias.
1.6.30. O equipamento deve suportar VRF (Virtual Routing and Forwarding), com, no mínimo, 256 instâncias.
1.6.31. Possuir homologação da ANATEL, de acordo com a Resolução número 242.
1.6.32. Deve permitir automação e escalabilidade de rede utilizando protocolo de malha ethernet (fabric ethernet) baseado em TRILL, SPB ou similar.
1.6.33. A malha ethernet deve implementar, nativamente no equipamento ou via software de gerência externo, mecanismo para estabelecimento de serviços virtualizados de redes lógicas em camada 2 e camada 3, de qualquer ponto da malha ethernet para qualquer outro ponto da malha ethernet, sem necessidade de configuração manual dos equipamentos intermediários entre os pontos que terão os serviços configurados.
1.6.34. A malha ethernet deve permitir criação de serviços virtualizados em camada 3, segmentados por VRF, em que um serviço virtualizado não deverá se comunicar com outro. Deve possuir, ainda, mecanismo para permitir que uma VRF se comunique com outra na malha ethernet para os casos em que a comunicação entre essas seja necessária.
1.6.35. A malha ethernet deve implementar mecanismo para tratamento de tráfego Multicast de forma inteligente, permitindo controle de multicast mesmo dentro de serviços virtualizados da malha ethernet, evitando assim flooding desnecessário para portas que não fazem parte de um mesmo grupo multicast.

1.6.36. O mecanismo para estabelecimento de caminhos de serviços virtualizados em camada 2 e camada 3 deverá ser implementado nativamente no equipamento físico ou via software do mesmo fabricante. Caso a solução ofertada necessite de um software adicional, todas as licenças adicionais para a implementação dessa funcionalidade devem ser fornecidas e deverá funcionar de forma redundante para garantir a alta disponibilidade do ambiente.
1.6.37. A malha ethernet deve ser agnóstica à topologia física.
1.6.38. A malha ethernet deve permitir escalabilidade de, no mínimo, 100 (cem) equipamentos;
1.6.39. A malha ethernet deve permitir a adição de equipamentos do tipo FFF (Fixed Form Factor) e equipamentos do tipo chassi.
1.6.40. A malha ethernet deverá permitir alta disponibilidade em caso de falhas de links e deverá permitir a utilização de todos os links da topologia sem gerar loops.
1.6.41. Implementar agregação de links com suporte a LACP.
1.6.42. Em conjunto com outro equipamento de mesmo modelo, deverá permitir que um switch conectado aos dois, tenha a possibilidade de agregação de links com suporte a LACP com os mesmos, de forma a simular a existência de apenas um único link lógico entre este equipamento e os dois switches do modelo aqui especificado (Multi-Chassis Trunking, por exemplo). O único link lógico entre as camadas deve eliminar convergência do Spanning Tree, possibilitando o tráfego simultâneo por mais de uma conexão.
1.6.43. Implementar jumbo frames em todas as portas ofertadas, com suporte a pacotes de até 9200 Bytes.
1.6.44. Implementar Proxy-ARP (RFC 1027).
1.6.45. Implementar IGMPv1 (RFC 1112), IGMP v2 (RFC 2236) e IGMPv3 (RFC 3376).
1.6.46. Implementar DHCP/Bootp relay.
1.6.47. Implementar DHCP Option 82, de acordo com a RFC 3046.
1.6.48. Implementar DHCP Client (RFC 2131).
1.6.49. Implementar Spanning-Tree (IEEE 802.1d), Rapid Spanning Tree (IEEE 802.1w) e Multiple Instance STP (802.1s).
1.6.50. Implementar a configuração de Multiple Spanning Tree Protocol, com suporte a, pelo menos, 12 instâncias.
1.6.51. Implementar funcionalidade vinculada ao Spanning-tree onde é possível designar portas de acesso (por exemplo onde estações estão conectadas) que não sofram o processo de Listening-Learning, passando direto para o estado de Forwarding. No entanto, as portas configuradas com esta funcionalidade devem detectar loops na rede normalmente.
1.6.52. Implementar funcionalidade vinculada ao Spanning-tree que permita desabilitar uma porta de acesso assim que a mesma receba uma BPDU.
1.6.53. Implementar mecanismo de prevenção contra loops, desabilitando a porta de acesso de forma automática em caso de loop.
1.6.54. Implementar 4000 VLANs por porta, ativas simultaneamente, através do protocolo 802.1Q.
1.6.55. Implementar Private VLAN.
1.6.56. Implementar L2 ping e traceroute de acordo com IEEE 802.1ag (Connectivity Fault Management).
1.6.57. Implementar os protocolos de roteamento IP: RFC 1058 – RIP v1 e RFC 2453 – RIP v2.
1.6.58. Implementar o protocolo de roteamento OSPFv2 (RFC 2328).
1.6.59. Implementar RFC 1587 OSPF NSSA Option.
1.6.60. Implementar protocolo de multicast PIM-SM para IPv4 e IPv6.
1.6.61. Implementar PIM-SSM segundo a RFC 3569.
1.6.62. Implementar ECMP (Equal Cost Multi Path) para rotas IPv4 e IPv6.

1.6.63. Implementar VRRPv3 (RFC 5798).
1.6.64. Deve implementar BGPv4.
1.6.65. "Deve implementar Dual Stack, ou seja, IPv6 e IPv4, com suporte as seguintes funcionalidades/RFCs:
1.6.65.1. RFC 1981, Path MTU Discovery for IPv6, August 1996 - Host Requirements
1.6.65.2. RFC 5095, Internet Protocol, Version 6 (IPv6) Specification
1.6.65.3. RFC 4861, Neighbor Discovery for IP Version 6, (IPv6)
1.6.65.4. RFC 2460, IPv6 base stack
1.6.65.5. RFC 2462, IPv6 Stateless Address Auto configuration - Host Requirements
1.6.65.6. RFC 2463, Internet Control Message Protocol (ICMPv6) for the IPv6 Specification
1.6.65.7. RFC 2464, Transmission of IPv6 Packets over Ethernet Networks
1.6.65.8. RFC 2466, MIB for ICMPv6
1.6.65.9. RFC 3513, Internet Protocol Version 6 (IPv6) Addressing Architecture
1.6.65.10. RFC 3587, Global Unicast Address Format"
1.6.66. "Deve implementar IPv6 de acordo com as seguintes RFCs:
1.6.66.1. RFC 2080, RIPng
1.6.66.2. RFC 2710, IPv6 Multicast Listener Discovery v1 (MLDv1) Protocol
1.6.66.3. RFC 3810, IPv6 Multicast Listener Discovery v2 (MLDv2) Protocol"
1.6.67. Implementar OSPFv3 conforme RFC 5340.
1.6.68. A implementação de OSPFv3 e rotas estáticas para IPv6 deve incluir ECMP (Equal Cost Multi Path).
1.6.69. Implementar Policy Based Routing.
1.6.70. "Implementar autenticação RADIUS com suporte a:
1.6.70.1. RFC 2138 RADIUS Authentication
1.6.70.2. RFC 2139 RADIUS Accounting
1.6.70.3. RFC 3579 RADIUS EAP support for 802.1X"
1.6.71. A implementação de RADIUS deve suportar alteração dinâmica de parâmetros de autorização de uma sessão que já esteja ativa.
1.6.72. A implementação de RADIUS e TACACS+ deve estar disponível para autenticação de usuários via Telnet e Console serial.
1.6.73. Implementar per-command authorization para RADIUS ou TACACS+.
1.6.74. Possuir DNS Client para IPv4 segundo a RFC 1591 e para IPv6 segundo a RFC 2874.
1.6.75. Possuir Telnet client and server segundo a RFC 854.
1.6.76. Implementar os seguintes grupos de RMON através da RFC 2819: History, Statistics, Alarms e Events.
1.6.77. Implementar sFlow ou Netflow.
1.6.78. Implementar a atualização de imagens de software e configuração através de um servidor FTP ou TFTP.
1.6.79. Suportar envio de log para múltiplos servidores Syslog.
1.6.80. Implementar ajuste de clock do equipamento utilizando NTP com autenticação MD5.
1.6.81. Implementar Port Mirroring, permitindo espelhar, no mínimo, 45 portas físicas.
1.6.82. Implementar gerenciamento através de SNMPv1 (RFC 1157), v2 (RFC 2576, RFCs 2578 a 2580 e RFCs 3416 e 3417) e v3 (RFCs 3411 a 3415).
1.6.83. Implementar cliente e servidor SSHv2.
1.6.84. Implementar servidor SCP e servidor SFTP.
1.6.85. Implementar gerenciamento via web com suporte a HTTP e HTTPS.
1.6.86. O sistema operacional deve possuir comandos para visualização do consumo de CPU e

memória RAM.
1.6.87. O sistema operacional deve possuir função grep/pipe para filtrar a saída de determinado comando.
1.6.88. Implementar protocolo de monitoramento de status de comunicação entre dois switches, que possibilite que uma porta seja desabilitada caso seja detectada uma falha de comunicação entre os dois peers.
1.6.89. "Implementar as seguintes RFCs:
1.6.89.1. RFC 2474 DiffServ Precedence
1.6.89.2. RFC 2475 DiffServ Core and Edge Router Functions
1.6.89.3. RFC 2597 DiffServ Assured Forwarding (AF)
1.6.89.4. RFC 2598 DiffServ Expedited Forwarding (EF)"
1.6.90. Deve implementar rate shaping de saída.
1.6.91. Implementar a leitura, classificação e remarcação de QoS DSCP.
1.6.92. Implementar 8 filas de prioridade em hardware por porta.
1.6.93. Implementar os algoritmos de gerenciamento de filas WRR (Weighted Round Robin) e SP (Strict Priority).
1.6.94. Implementar detecção de oscilação (flap) de links, permitindo desabilitar uma porta caso a porta oscile acima de um limiar configurado.
1.6.95. Implementar Gratuitous ARP Protection ou Filtering.
1.6.96. Implementar prevenção contra-ataques Denial of Service (DoS).
1.6.97. Implementar ACLs de entrada (ingress ACLs) em hardware, baseadas em critérios da camada 2 (MAC origem e destino e campo 802.1p), camada 3 (IP origem e destino) e camada 4 (portas TCP e UDP), em todas as interfaces e VLANs.
1.6.98. As ACLs devem ser configuradas para permitir, negar, aplicar QoS, espelhar o tráfego para uma porta de análise e incrementar contador.

1.7. **Switch Core de Rede Tipo III - 48 portas 10/100/1000BASE-T + 2 Portas 25 gigas SPF28**
1.7.1. A proposta deverá conter a descrição detalhada com códigos do fabricante de todos os módulos, fontes e acessórios fornecidos.
1.7.2. A solução deve ser composta de um único equipamento, montável em rack 19" devendo este vir acompanhado dos devidos acessórios para tal.
1.7.3. Possuir fonte de alimentação interna que trabalhe em 110V/220V, 50/60 Hz, com detecção automática de tensão e frequência, hot-swappable.
1.7.4. Suportar/Possuir fonte de alimentação AC redundante interna, hot-swappable.
1.7.5. Possuir bandeja de ventiladores substituível em campo (field replaceable e hot swappable).
1.7.6. Possuir ventilação "front-to-back", ou seja, a saída de ar quente deve acontecer pela traseira do equipamento.
1.7.7. Suportar capacidade agregada de switching de, no mínimo, 190 Gbps.
1.7.8. Suportar capacidade de encaminhamento de pacotes, de no mínimo 145 Mpps utilizando pacotes de 64 bytes.
1.7.9. Possuir porta de console com conector RJ-45 ou DB9 macho.
1.7.10. Possuir uma porta USB Micro B para gerenciamento.
1.7.11. Possuir, no mínimo, uma porta USB para transferência de arquivos.
1.7.12. Possuir leds indicativos de funcionamento da fonte de alimentação, ventiladores e status das portas.
1.7.13. Possuir 48 portas 10/100/1000BASE-T ativas simultaneamente, com conector RJ-45.

1.7.14. Possuir 02 portas 25 Gb SPF28.
1.7.15. A Memória Flash instalada deve ser suficiente para comportar no mínimo duas imagens do Sistema Operacional simultaneamente, permitindo que seja feito um upgrade de Software e a imagem anterior seja mantida.
1.7.16. Possuir altura máxima de 1U (1,75").
1.7.17. Deve suportar o armazenamento de no mínimo 80.000 (oitenta mil) endereços MAC.
1.7.18. Deve suportar o armazenamento de, no mínimo, 15.000 (quinze mil) rotas IPv4 em hardware.
1.7.19. Deve suportar o armazenamento de, no mínimo, 7.000 (sete mil) rotas IPv6 em hardware.
1.7.20. Suportar agregação de links conforme padrão IEEE 802.1AX com, no mínimo, 48 grupos, sendo 8 links agregados por grupo.
1.7.21. Implementar, no mínimo, 500 (quinhentas) regras de ACL de entrada (ingress ACLs).
1.7.22. Implementar, no mínimo, 120 (cento e vinte) regras de ACL de saída (egress ACLs).
1.7.23. O equipamento deve suportar VRF (Virtual Routing and Forwarding), com, no mínimo, 24 instâncias.
1.7.24. O equipamento deve suportar VRF (Virtual Routing and Forwarding), com, no mínimo, 256 instâncias.
1.7.25. Possuir homologação da ANATEL, de acordo com a Resolução número 242.
1.7.26. Deve permitir automação e escalabilidade de rede utilizando protocolo de malha ethernet (fabric ethernet) baseado em TRILL, SPB ou similar.
1.7.27. A malha ethernet deve implementar, nativamente no equipamento ou via software de gerência externo, mecanismo para estabelecimento de serviços virtualizados de redes lógicas em camada 2 e camada 3, de qualquer ponto da malha ethernet para qualquer outro ponto da malha ethernet, sem necessidade de configuração manual dos equipamentos intermediários entre os pontos que terão os serviços configurados.
1.7.28. A malha ethernet deve permitir criação de serviços virtualizados em camada 3, segmentados por VRF, em que um serviço virtualizado não deverá se comunicar com outro. Deve possuir, ainda, mecanismo para permitir que uma VRF se comunique com outra na malha ethernet para os casos em que a comunicação entre essas seja necessária.
1.7.29. A malha ethernet deve implementar mecanismo para tratamento de tráfego Multicast de forma inteligente, permitindo controle de multicast mesmo dentro de serviços virtualizados da malha ethernet, evitando assim flooding desnecessário para portas que não fazem parte de um mesmo grupo multicast.
1.7.30. O mecanismo para estabelecimento de caminhos de serviços virtualizados em camada 2 e camada 3 deverá ser implementado nativamente no equipamento físico ou via software do mesmo fabricante. Caso a solução ofertada necessite de um software adicional, todas as licenças adicionais para a implementação dessa funcionalidade devem ser fornecidas e deverá funcionar de forma redundante para garantir a alta disponibilidade do ambiente.
1.7.31. A malha ethernet deve ser agnóstica à topologia física.
1.7.32. A malha ethernet deve permitir escalabilidade de, no mínimo, 100 (cem) equipamentos;
1.7.33. A malha ethernet deve permitir a adição de equipamentos do tipo FFF (Fixed Form Factor) e equipamentos do tipo chassi.
1.7.34. A malha ethernet deverá permitir alta disponibilidade em caso de falhas de links e deverá permitir a utilização de todos os links da topologia sem gerar loops.
1.7.35. Implementar agregação de links com suporte a LACP.
1.7.36. Em conjunto com outro equipamento de mesmo modelo, deverá permitir que um switch conectado aos dois, tenha a possibilidade de agregação de links com suporte a LACP com os mesmos, de forma a simular a existência de apenas um único link lógico entre este equipamento e os dois

switches do modelo aqui especificado (Multi-Chassis Trunking, por exemplo). O único link lógico entre as camadas deve eliminar convergência do Spanning Tree, possibilitando o tráfego simultâneo por mais de uma conexão.
1.7.37. Implementar jumbo frames em todas as portas ofertadas, com suporte a pacotes de até 9200 Bytes.
1.7.38. Implementar Proxy-ARP (RFC 1027).
1.7.39. Implementar IGMPv1 (RFC 1112), IGMP v2 (RFC 2236) e IGMPv3 (RFC 3376).
1.7.40. Implementar DHCP/Bootp relay.
1.7.41. Implementar DHCP Option 82, de acordo com a RFC 3046.
1.7.42. Implementar DHCP Client (RFC 2131).
1.7.43. Implementar Spanning-Tree (IEEE 802.1d), Rapid Spanning Tree (IEEE 802.1w) e Multiple Instance STP (802.1s).
1.7.44. Implementar a configuração de Multiple Spanning Tree Protocol, com suporte a, pelo menos, 12 instâncias.
1.7.45. Implementar funcionalidade vinculada ao Spanning-tree onde é possível designar portas de acesso (por exemplo onde estações estão conectadas) que não sofram o processo de Listening-Learning, passando direto para o estado de Forwarding. No entanto, as portas configuradas com esta funcionalidade devem detectar loops na rede normalmente.
1.7.46. Implementar funcionalidade vinculada ao Spanning-tree que permita desabilitar uma porta de acesso assim que a mesma receba uma BPDU.
1.7.47. Implementar mecanismo de prevenção contra loops, desabilitando a porta de acesso de forma automática em caso de loop.
1.7.48. Implementar 4000 VLANs por porta, ativas simultaneamente, através do protocolo 802.1Q.
1.7.49. Implementar Private VLAN.
1.7.50. Implementar L2 ping e traceroute de acordo com IEEE 802.1ag (Connectivity Fault Management).
1.7.51. Implementar os protocolos de roteamento IP: RFC 1058 – RIP v1 e RFC 2453 – RIP v2.
1.7.52. Implementar o protocolo de roteamento OSPFv2 (RFC 2328).
1.7.53. Implementar RFC 1587 OSPF NSSA Option.
1.7.54. Implementar protocolo de multicast PIM-SM para IPv4 e IPv6.
1.7.55. Implementar PIM-SSM segundo a RFC 3569.
1.7.56. Implementar ECMP (Equal Cost Multi Path) para rotas IPv4 e IPv6.
1.7.57. Implementar VRRPv3 (RFC 5798).
1.7.58. Deve implementar BGPv4.
1.7.59. "Deve implementar Dual Stack, ou seja, IPv6 e IPv4, com suporte as seguintes funcionalidades/RFCs:
1.7.59.1. RFC 1981, Path MTU Discovery for IPv6, August 1996 - Host Requirements
1.7.59.2. RFC 5095, Internet Protocol, Version 6 (IPv6) Specification
1.7.59.3. RFC 4861, Neighbor Discovery for IP Version 6, (IPv6)
1.7.59.4. RFC 2460, IPv6 base stack
1.7.59.5. RFC 2462, IPv6 Stateless Address Auto configuration - Host Requirements
1.7.59.6. RFC 2463, Internet Control Message Protocol (ICMPv6) for the IPv6 Specification
1.7.59.7. RFC 2464, Transmission of IPv6 Packets over Ethernet Networks
1.7.59.8. RFC 2466, MIB for ICMPv6
1.7.59.9. RFC 3513, Internet Protocol Version 6 (IPv6) Addressing Architecture
1.7.59.10. RFC 3587, Global Unicast Address Format"
1.7.60. "Deve implementar IPv6 de acordo com as seguintes RFCs:

1.7.60.1. RFC 2080, RIPng
1.7.60.2. RFC 2710, IPv6 Multicast Listener Discovery v1 (MLDv1) Protocol
1.7.60.3. RFC 3810, IPv6 Multicast Listener Discovery v2 (MLDv2) Protocol"
1.7.61. Implementar OSPFv3 conforme RFC 5340.
1.7.62. A implementação de OSPFv3 e rotas estáticas para IPv6 deve incluir ECMP (Equal Cost Multi Path).
1.7.63. Implementar Policy Based Routing.
1.7.64. "Implementar autenticação RADIUS com suporte a:
1.7.64.1. RFC 2138 RADIUS Authentication
1.7.64.2. RFC 2139 RADIUS Accounting
1.7.64.3. RFC 3579 RADIUS EAP support for 802.1X"
1.7.65. A implementação de RADIUS deve suportar alteração dinâmica de parâmetros de autorização de uma sessão que já esteja ativa.
1.7.66. A implementação de RADIUS e TACACS+ deve estar disponível para autenticação de usuários via Telnet e Console serial.
1.7.67. Implementar per-command authorization para RADIUS ou TACACS+.
1.7.68. Possuir DNS Client para IPv4 segundo a RFC 1591 e para IPv6 segundo a RFC 2874.
1.7.69. Possuir Telnet client and server segundo a RFC 854.
1.7.70. Implementar os seguintes grupos de RMON através da RFC 2819: History, Statistics, Alarms e Events.
1.7.71. Implementar sFlow ou Netflow.
1.7.72. Implementar a atualização de imagens de software e configuração através de um servidor FTP ou TFTP.
1.7.73. Suportar envio de log para múltiplos servidores Syslog.
1.7.74. Implementar ajuste de clock do equipamento utilizando NTP com autenticação MD5.
1.7.75. Implementar Port Mirroring, permitindo espelhar, no mínimo, 45 portas físicas.
1.7.76. Implementar gerenciamento através de SNMPv1 (RFC 1157), v2 (RFC 2576, RFCs 2578 a 2580 e RFCs 3416 e 3417) e v3 (RFCs 3411 a 3415).
1.7.77. Implementar cliente e servidor SSHv2.
1.7.78. Implementar servidor SCP e servidor SFTP.
1.7.79. Implementar gerenciamento via web com suporte a HTTP e HTTPS.
1.7.80. O sistema operacional deve possuir comandos para visualização do consumo de CPU e memória RAM.
1.7.81. O sistema operacional deve possuir função grep/pipe para filtrar a saída de determinado comando.
1.7.82. Implementar protocolo de monitoramento de status de comunicação entre dois switches, que possibilite que uma porta seja desabilitada caso seja detectada uma falha de comunicação entre os dois peers.
1.7.83. "Implementar as seguintes RFCs:
1.7.83.1. RFC 2474 DiffServ Precedence
1.7.83.2. RFC 2475 DiffServ Core and Edge Router Functions
1.7.83.3. RFC 2597 DiffServ Assured Forwarding (AF)
1.7.83.4. RFC 2598 DiffServ Expedited Forwarding (EF)"
1.7.84. Deve implementar rate shaping de saída.
1.7.85. Implementar a leitura, classificação e remarcação de QoS DSCP.
1.7.86. Implementar 8 filas de prioridade em hardware por porta.
1.7.87. Implementar os algoritmos de gerenciamento de filas WRR (Weighted Round Robin) e SP (Strict

Priority).
1.7.88. Implementar detecção de oscilação (flap) de links, permitindo desabilitar uma porta caso a porta oscile acima de um limiar configurado.
1.7.89. Implementar Gratuitous ARP Protection ou Filtering.
1.7.90. Implementar prevenção contra ataques Denial of Service (DoS).
1.7.91. Implementar ACLs de entrada (ingress ACLs) em hardware, baseadas em critérios da camada 2 (MAC origem e destino e campo 802.1p), camada 3 (IP origem e destino) e camada 4 (portas TCP e UDP), em todas as interfaces e VLANs.
1.7.92. As ACLs devem ser configuradas para permitir, negar, aplicar QoS, espelhar o tráfego para uma porta de análise e incrementar contador

2. **Controladora de Rede Wirelles**
2.1. CARACTERÍSTICAS BÁSICAS EXIGIDAS
2.1.1. Deve ser do mesmo fabricante dos switches dos demais itens;
2.1.2. O controlador wireless poderá ser fornecido como appliance virtual para plataforma VMware compatível com VMware ESXi 6 ou superior ou plataforma Microsoft Hyper-V ou poderá ser fornecido montado em hardware específico ou em chassis que permita a instalação de módulos para a execução das funcionalidades requisitadas;
2.1.3. Caso seja fornecido em hardware específico deve obedecer aos seguintes requisitos mínimos:
2.1.4. Deve suportar fonte de alimentação interna, redundante e com seleção automática de tensão (110-220 VAC);
2.1.5. Permitir ser montado em rack padrão de 19 (dezenove) polegadas, incluindo todos os acessórios necessários;
2.1.6. Deve possuir mais 2 (duas) portas SFP+ para inserção de interfaces 1/10 Gigabit Ethernet;
2.2. CAPACIDADE DE CONTROLE DE ACCESS POINTS
2.2.1. Deve estar licenciado para gerenciar, no mínimo, 60 (sessenta) Access Points (APs) simultaneamente;
2.2.2. Permitir a expansão do número de access points wireless através de licenças de software, sem exigir a troca de hardware ou Host Virtualizado;
2.2.3. Permitir a expansão da capacidade através de licenças de software para, no mínimo, 500 (quinhentos) APs por controlador;
2.2.4. Capacidade de gerenciar no mínimo 8000 (oito mil) usuários simultaneamente por controlador;

2.3. MODO DE OPERAÇÃO
2.3.1. O controlador WLAN poderá estar instalado em qualquer ponto da infraestrutura de rede e deve possuir a capacidade de controlar APs instalados na mesma localidade e em localidade remota através de rede WAN;
2.3.2. Na ocorrência de inoperância de um AP, o controlador WLAN deverá ajustar automaticamente a potência dos APs adjacentes, de modo a prover a cobertura da área não assistida;
2.3.3. Se controlador principal falhar, os APs relacionados no controlador principal devem ser gerenciados pelo controlador redundante sem a necessidade de intervenção ou reconfiguração;
2.3.4. Deve permitir sua configuração em alta disponibilidade (HA) com outro controlador de igual capacidade;
2.3.5. Quando um dos controladores de um par configurado como HA falhar, o controlador que restar deverá ter capacidade de assumir todos os APs do controlador com falha, adicionalmente aos APs adotados por ele e não permitindo que a rede wireless se torne inoperante;

65
ASR

2.3.6. Caso necessite de licença de software ou hardware adicional para a implementação de HA a mesma deve ser fornecida;
2.3.7. Implementar sistema de balanceamento de carga para associação de clientes entre APs próximos para otimizar a performance;
2.3.8. Detectar áreas de sombra de cobertura e efetuar os devidos ajustes para sua correção automaticamente;
2.3.9. Ajustar dinamicamente o nível de potência e canal de rádio dos APs, de modo a otimizar o tamanho da célula de RF, garantindo a performance e escalabilidade;
2.3.10. Implementar Dynamic Radio Management (DRM) ou função semelhante de controle de rádio frequência (Canal e potência);
2.3.11. Implementar modo de operação com encaminhamento de tráfego diretamente no Access Point (AP), ou seja, switching no AP;
2.3.12. Implementar modo de operação tunelado do tráfego wireless diretamente no controlador wireless;
2.3.13. Deve ser possível usar os dois modos (Switching no AP e tráfego tunelado) simultaneamente;

2.4. ROTEAMENTO
2.4.1. Deve possibilitar a configuração de rotas estáticas;
2.4.2. Deve possuir DHCP relay;

2.5. GERENCIAMENTO
2.5.1. Implementar Syslog Client;
2.5.2. Implementar TFTP ou FTP;
2.5.3. Implementar CLI (Command Line Interface);
2.5.4. Permitir a atualização remota do sistema operacional e dos arquivos de configuração utilizados no equipamento;
2.5.5. Permitir a configuração e gerenciamento seguro por meio de browser padrão (HTTPS);
2.5.6. Possuir porta de console para gerenciamento e configuração via linha de comando CLI ou interface Ethernet dedicada ao gerenciamento via CLI do controlador;
2.5.7. Possuir ferramentas de debug e log de eventos para depuração e gerenciamento em primeiro nível;
2.5.8. Possibilitar a obtenção da parâmetros do equipamento através do protocolo SNMP;
2.5.9. Permitir a criação de regras de adoção de Access Points, baseadas em, pelo menos, endereço IP ou subnet, para que o Access Point seja adotado com as configurações de determinado site automaticamente;

2.6. SEGURANÇA e QoS
2.6.1. "Implementar em conjunto com os Access Points:
2.6.2. O padrão IEEE 802.11a;
2.6.3. O padrão IEEE 802.11b;
2.6.4. O padrão IEEE 802.11g;
2.6.5. O padrão IEEE 802.11n;
2.6.6. O padrão IEEE 802.11ac;
2.6.7. O padrão IEEE 802.11ax;
2.6.8. O padrão IEEE 802.11r;
2.6.9. O padrão IEEE 802.11k;
2.6.10. O padrão IEEE 802.11w;"

2.6.11. "Implementar:
2.6.12. RFC 2865 Radius;
2.6.13. RFC 2866 Radius Accounting;
2.6.14. RFC 1213 MIB-II;"
2.6.15. Suportar integração com servidor RADIUS e LDAP externo;
2.6.16. Deve implementar recursos para detecção de rogue AP (Rogue Access Point) nas bandas de 2,4 GHz e 5 GHz.
2.6.17. Deve implementar recursos para detecção de rogue clients nas bandas de 2,4 GHz e 5 GHz.
2.6.18. Deve implementar a detecção de clientes nas proximidades, bem como o SSID/BSSID em que estão conectados, caso a informação esteja disponível nos pacotes de controle que estejam trafegando pelo ar;
2.6.19. Deve implementar a detecção de BSSIDs próximos e suas respectivas potências de sinal;
2.6.20. Deve suportar mitigação de rogue APs;
2.6.21. Deve permitir a captura de pacotes para fins de troubleshooting;
2.6.22. Deve implementar mecanismo do tipo RF Auto-Tuning, ou seja, associar dinamicamente o canal de comunicação e a potência de transmissão dos rádios dos access points e ainda reajustar estes parâmetros de forma automática sempre que for necessário;
2.6.23. Implementar, em conjunto com o Ponto de Acesso, Qualidade de Serviço com suporte a IEEE 802.11e e WMM;
2.6.24. Suportar CAC (CallAdmissionControl);
2.6.25. Possibilitar roaming com integridade de sessão, dando suporte a aplicações em tempo real, tais como, VoWLAN e streaming de vídeo;
2.6.26. Implementar capacidade de economia de energia com o uso do UAPSD (Unscheduled Automatic Power Save Delivery);
2.6.27. Implementar, em conjunto com o AP, fast roaming seguro;
2.6.28. Implementar 802.1Q;
2.6.29. Implementar mapeamento de QoS de pacotes marcados na rede cabeada com ToS/DSCP para a rede wireless através de WMM;
2.6.30. Implementar protocolo de autenticação para controle do acesso administrativo ao equipamento utilizando servidor RADIUS ou TACACS+;
2.6.31. Implementar listas de controle de acesso ou funcionalidade similar de controle;
2.6.32. Implementar filtros de acesso à rede baseados em endereços MAC;
2.6.33. Implementar associação de usuários a políticas de segurança L2, L3 e L7, com base em parâmetros como grupo de usuário do LDAP e RADIUS, tipo de dispositivo (Android, IOS, Windows, entre outros) e localização (SSID);
2.6.34. "Implementar a criação de grupos de tipos de dispositivos (Android, IOS, Windows, entre outros) de forma que o usuário possa receber políticas de segurança de acordo com o tipo de seu dispositivo, durante a etapa de autenticação;"
2.6.35. Implementar associação dinâmica de usuário a VLAN, com base nos parâmetros da etapa de autenticação;
2.6.36. Implementar associação dinâmica de filtros ou ACL e de QoS, com base nos parâmetros da etapa de autenticação;
2.6.37. Implementar a limitação de banda por usuário, com base nos parâmetros da etapa de autenticação;
2.6.38. Implementar regras de acesso até camada 7, com base nos parâmetros da etapa de autenticação;
2.6.39. Deve ser possível o agendamento da disponibilidade (habilitar/desabilitar) de SSIDs,

agendando determinada data e horário que o SSID deve estar disponível. Este agendamento poderá inclusive ter recorrência periódica como diária, semanal ou mensal;
2.6.40. Implementar IEEE 802.1X, para autenticação de clientes wireless, com pelo menos os seguintes métodos EAP: EAP-TTLS, PEAP, EAP-TLS, EAP-SIM, EAP-MD5 e EAP-FAST;
2.6.41. Implementar, em conjunto com o AP, WEP, chaves estáticas e dinâmicas;
2.6.42. Implementar, em conjunto com o AP, WPA com algoritmo de criptografia TKIP;
2.6.43. Implementar, em conjunto com o AP, WPA2 com algoritmo de criptografia AES;
2.6.44. Implementar, em conjunto com o AP, WPA3-SAE e WPA3-Compatibility (SAE ou WPA2 PSK);
2.6.45. Implementar funcionalidade que permita que o AP suprima respostas a probes de clientes que possuam RSS abaixo de um valor mínimo configurado;
2.6.46. Deve possuir localmente no controlador, portal web para autenticação dos usuários visitantes, sendo possível a customização com informações e características visuais (mensagem, logo, banner, etc);
2.6.47. Implementar Captive Portal com suporte a auto registro e auto registro via conta do Facebook, Microsoft e Gmail;
2.6.48. O portal web de autenticação, bem como a ferramenta de administração e gerência devem ser acessadas via web nativo, sem a necessidade de instalação de nenhum software ou plug-in adicional;
2.6.49. Deve suportar o uso de captive portal externo ao controlador.
2.6.50. O controlador wireless deve permitir acessar o Access Point via SSH através de interface gráfica para fins de troubleshooting.
2.6.51. O controlador wireless deverá suportar a instalação de aplicações do mesmo fabricante ou de terceiros, com o conceito de containers ou através de acesso ao sistema operacional do controlador, compartilhando recursos em comum;
2.6.52. Deve ser possível importar planta baixa dos locais nos formatos .jpg, .png ou .svg;
2.6.53. Possuir informação visual e gráfica, nas plantas baixas dos locais inseridas no sistema, para:
2.6.54. - Visualização dos pontos de acesso instalados, com estado de funcionamento;
2.6.55. - Visualização do mapa de calor de RF (Heatmap);
2.6.56. - Visualização dos canais utilizados por AP;
2.6.57. - Visualização da performance da rede baseada na velocidade do link;
2.6.58. - Visualização da performance de rede baseada em parâmetros de qualidade RF;
2.6.59. Deve permitir a customização das plantas baixas importadas criando paredes de diferentes tipos considerando o comportamento de interferência RF de cada material;

2.7. RELATÓRIOS
2.7.1. Deve possuir relatórios por grupo de APs, por AP, por SSID e por usuário que relacionem métricas de utilização da rede;
2.7.2. Deve possuir relatórios por grupo de APs, por AP, por SSID e por usuário que relacionem métricas de qualidade de radiofrequência;
2.7.3. Deve possuir relatórios por grupo de APs, por AP e por SSID que relacionem métricas dos clientes (devices) conectados como sistema operacional, fabricante e etc;
2.7.4. Deve possuir relatórios que relacionem métricas de clientes associados através de captive portal;
2.7.5. Possuir relatórios que relacionem grupos de aplicações em camada 7 e suas utilizações de rede;
2.7.6. Deve possuir relatórios que correlacionem métricas indicando a saúde da rede;
2.7.7. Deve possuir relatório que relacione métricas de troubleshooting como captura de pacotes;
2.7.8. Deve ser possível visualizar os relatórios com dados históricos para análise forense, sendo possível alterar o período;

2.7.9. Possuir certificação/homologação da ANATEL;

3. **Access Point 802.11 ax/ac/abgn 4x4:4 MIMO**
3.1. Especificações:
3.1.1. Deve ser do mesmo fabricante do controlador WLAN
3.1.2. "Access Point (AP) atendendo simultaneamente aos padrões:
3.1.3. IEEE 802.11a;
3.1.4. IEEE 802.11b;
3.1.5. IEEE 802.11g;
3.1.6. IEEE 802.11n;
3.1.7. IEEE 802.11ac (Wave 2);
3.1.8. IEEE 802.11ax;"
3.1.9. "Implementar a conexão simultânea de dispositivos configurados nos padrões:
3.1.10. IEEE 802.11b/g/n;
3.1.11. IEEE 802.11a/n;
3.1.12. IEEE 802.11ac (Wave 2);
3.1.13. IEEE 802.11ax;"
3.1.14. O Access Point deve possuir rádio Bluetooth, conforme padrão BLE;
3.1.15. Implementar funcionamento simultâneo dos rádios 2.4GHz, 5.0 GHz e Bluetooth (BLE);
3.1.16. Deve suportar modo de operação Dual 5GHz;
3.1.17. Implementar todas as seguintes taxas de transmissão e fallback automático:
3.1.18. IEEE 802.11a: 54, 48, 36, 24, 18, 12, 9 e 6 Mbps;
3.1.19. IEEE 802.11b: 11, 5.5, 2 e 1 Mbps;
3.1.20. IEEE 802.11g: 54, 48, 36, 24, 18, 12, 11, 9, 6, 5.5, 2 e 1 Mbps;
3.1.21. IEEE 802.11n: MCS0 à MCS15;
3.1.22. IEEE 802.11ac: MCS0 à MCS9 até 4SS;
3.1.23. IEEE 802.11ax: MCS0 à MCS11 até 4SS;
3.1.24. Deve suportar canais de 20 MHz, 40 MHz, 80 MHz e 160 MHz;
3.1.25. Deve suportar modulação OFDMA;
3.1.26. Deve vir acompanhado dos componentes que permitam sua fixação em teto;
3.1.27. Deve vir acompanhado dos componentes que permitam sua fixação em parede;
3.1.28. Deve ser compatível com a ferramenta de administração wireless;
3.1.29. O Access Point ofertado deve suportar alimentação PoE pelos padrões 802.3af ou 802.3at.
3.1.30. Deve implementar instalação plug and play;
3.1.31. Deve suportar análise de espectro RF;
3.1.32. Deve implementar um modo hibrido de operação que seja capaz de suportar varredura de segurança e atender aos clientes no mesmo rádio;
3.1.33. Deve implementar um modo de operação que seja capaz de fazer a varredura de segurança, trabalhando de forma dedicada, sem a necessidade de módulos de hardware adicionais para este fim.
3.1.34. A potência de cada cadeia de transmissão (transmit chain) deve ser de, no mínimo, 12 dBm em 2.4 GHz e 5 GHz;
3.1.35. Deve implementar associação de policies para clientes, sem depender de segmentação via SSIDs dedicados;
3.1.36. Implementar Stateless Address Auto Configuration (SLAAC);
3.1.37. Implementar LLDP;
3.1.38. Implementar Dynamic DNS para facilitar o acesso remoto aos Access Points;

69
ASR

3.1.39. Implementar cliente DHCP, para configuração automática de rede;
3.1.40. Implementar servidor DHCP;
3.1.41. Suportar Captive portal;
3.1.42. Suportar o armazenamento da página do Captive Portal diretamente no Access Point;
3.1.43. Implementar servidor RADIUS;
3.1.44. Suportar TACACS+;
3.1.45. Suportar o armazenamento de, pelo menos, duas imagens do sistema operacional, podendo alternar entre elas sem a necessidade de reinstalação do sistema operacional;
3.1.46. Deverá suportar operação em modo MESH;
3.1.47. Deverá permitir o desligamento automático do SSID com base em horários pré definidos;
3.1.48. Suportar IPSec;
3.1.49. Suportar integração com servidor LDAP externo;
3.1.50. Suportar rotas estáticas IPv4 e IPv6;
3.1.51. Implementar IGMP Snooping;
3.1.52. Implementar MLD Snooping;

3.2. INTERFACES
3.2.1. Possuir pelo menos 01 (uma) porta Gigabit Ethernet 10/100/1000 Mbps, auto-sensing, com conector RJ-45 Fêmea para dados, não sendo aceito portas de gerência;
3.2.2. Possuir pelo menos 01 (uma) porta Multigigabit Ethernet 100/1000/2500/5000Mbps, auto-sensing, com conector RJ-45 Fêmea para dados, não sendo aceito portas de gerência;
3.2.3. Implementar sua energização, por pelo menos uma das interface de rede descritas no item anterior, através de um único injetor padrão IEEE 802.3af PoE ou IEEE 802.3at PoE+;
3.2.4. O Access Point deve permitir sua operação em capacidade máxima mesmo quando energizado através do injetor PoE+;
3.2.5. Deve suportar redundância de PoE (PoE Failover);
3.2.6. Suportar sua energização através de fonte externa ou interna que opere com tensão de entrada para a fonte em 110/220VAC;
3.2.7. Possuir porta de console para configuração;
3.2.8. Possuir interface USB 3.0;

3.3. LEDS E SINALIZAÇÃO
3.3.1. Possuir LEDs indicativos do estado de operação;

3.4. ANTENAS
3.4.1. Possuir antenas:
3.4.2. Internas ao AP;
3.4.3. Com ganho de, no mínimo, 4dBi para 2.4GHz;
3.4.4. Com ganho de, no mínimo, 5dBi para 5.0GHz;
3.4.5. Com ganho de, no mínimo, 5dBi para Bluetooth;
3.4.6. Que implemente padrão de irradiação omnidirecional;
3.4.7. Que implemente operação simultânea em 4x4:4 MU-MIMO;

3.5. MODO DE OPERAÇÃO
3.5.1. Implementar modo de operação onde o AP possa estar remotamente conectado ao controlador wireless tanto de forma direta em uma rede de camada 2 ou em qualquer ponto de uma rede segmentada em subredes de camada 3;

3.5.2. Deve permitir sua operação através da conexão a um controlador principal e a um controlador secundário;
3.5.3. Deve permitir selecionar automaticamente o canal de transmissão;
3.5.4. Deve permitir ajustar dinamicamente o nível de potência e canal de rádio;
3.5.5. Deve possuir suporte a pelo menos 8 SSIDs para 2.4GHz e 8 SSIDs para 5.0GHz;
3.5.6. Deve permitir habilitar e desabilitar a divulgação do SSID;
3.5.7. Deve implementar Fast Roaming ou funcionalidade similar de forma a garantir o Roaming sem perda de conexão;
3.5.8. Não deve haver licença restringindo o número de usuários por AP;
3.5.9. Implementar a pilha de protocolos TCP/IP;
3.5.10. Implementar VLANs conforme padrão IEEE 802.1Q;
3.5.11. Deve permitir se configurar automaticamente ao ser conectado na rede;
3.5.12. Implementar Packet aggregation A-MPDU, A-MSDU para 802.11ac e 802.11n;

3.6. GERENCIAMENTO
3.6.1. "Deve permitir o agrupamento, em uma única rede Wi-Fi, para operar em
3.6.2. modo distribuído/colaborativo ou modo dependente de controlador central
3.6.3. WLAN, com um total de pelo menos 60 (cinquenta) Pontos de Acesso;"
3.6.4. Permitir via controlador wireless, a atualização remota do sistema operacional;
3.6.5. Permitir via controlador wireless, a atualização remota dos arquivos de configuração utilizados no equipamento;
3.6.6. O AP deverá suportar o funcionamento em modo dependente e independente de controladora

3.7. SEGURANÇA e QoS
3.7.1. Implementar filtros de acesso à rede baseados em aplicação (camada 7);
3.7.2. Implementar redirecionamento HTTP/HTTPS para Captive Portal externo diretamente no AP;
3.7.3. Possuir entrada para dispositivo antifurto do tipo Kensington lock ou similar;
3.7.4. Suportar varredura de Rádio Frequência nas tecnologias 802.11a, 802.11b/g, 802.11n e 802.11ac para identificação de APs não autorizados (rogues);
3.7.5. Suportar varredura de Rádio Frequência nas tecnologias 802.11a, 802.11b/g, 802.11n, 802.11ac para identificação de interferências nos canais na rede WLAN;
3.7.6. Implementar IEEE 802.1X de acesso do próprio AP a rede cabeada;
3.7.7. Implementar autenticação com geração dinâmica de chaves criptográficas por sessão e por usuário;
3.7.8. Implementar Stateful Firewall;
3.7.9. Implementar NAT;
3.7.10. Implementar, em conjunto com o Controlador WLAN, WEP, chaves estáticas e dinâmicas;
3.7.11. Implementar, em conjunto com o Controlador WLAN, WPA com algoritmo de criptografia TKIP e MIC;
3.7.12. Implementar, em conjunto com o Controlador WLAN, WPA2 com algoritmo de criptografia AES;
3.7.13. Implementar, em conjunto com o Controlador WLAN, WPA3-SAE e WPA3-Compatibility (SAE ou WPA2 PSK);
3.7.14. Implementar padrão IEEE 802.11e WMM da Wi-Fi Alliance para priorização de tráfego, suportando aplicações em tempo real, tais como VoIP e vídeo;
3.7.15. Possuir certificação da Wi-Fi Alliance para WiFi 6 e WPA3;
3.7.16. Possuir MTBF (Mean Time Between Failure) de, no mínimo, 320.000 (Trezentos e vinte mil) horas;

3.7.17. Possuir certificação/homologação da ANATEL;

4. **Módulo Transceiver SFP+ 10GBASE-LR para switch de acesso**
4.1. Devem ser compatíveis com os switches objeto deste termo;
4.2. Deve operar em fibras ópticas monomodo;
4.3. Devem ser do tipo SFP, operando no padrão 10GBASE-LR.

5. **Módulo Transceiver SFP+ 10GBASE-LR para switch core**
5.1. Devem ser compatíveis com os switches objeto deste termo;
5.2. Deve operar em fibras ópticas monomodo;
5.3. Devem ser do tipo SFP, operando no padrão 10GBASE-LR.

6. **Cordão Duplex Conectorizado SM**
6.1. Ter tamanho mínimo de 2,0m;
6.2. Possuir conector LC em ambas as extremidades;
6.3. As fibras devem ser do tipo SM – 9/125µm
6.4. Deverá atender as especificações da Norma ANSI/EIA/TIA-568C.
6.5. Deverá ser apresentado certificação ISO 9001 e ISO 14000 do fabricante do produto.
6.6. Apresentar catálogo do Fabricante.

7. **Cordão Duplex Conectorizado MM**
7.1. Ter tamanho mínimo de 2,0m;
7.2. Possuir conector LC em ambas as extremidades;
7.3. As fibras devem ser do tipo MM – 50/125µm mínimo OM3.
7.4. Deverá atender as especificações da Norma ANSI/EIA/TIA-568C.
7.5. Deverá ser apresentado certificação ISO 9001 e ISO 14000 do fabricante do produto.
7.6. Apresentar catálogo do Fabricante.

8. **Cabo de empilhamento 10 G para switch de acesso**
8.1. Devem ser compatíveis com os switches objeto deste termo;
8.2. Dever ter no mínimo 1 metro de comprimento.

9. **Cabo de empilhamento 100 G para switch de core**
9.1. Devem ser compatíveis com os switches objeto deste termo;
9.2. Dever ter no mínimo 1 metro de comprimento.

10. **Cabo de empilhamento 25 G para switch de core**
10.1. Devem ser compatíveis com os switches objeto deste termo;
10.2. Dever ter no mínimo 1 metro de comprimento.

11. **Software de gerenciamento de rede**
11.1. Deve permitir a integração da gerência da rede em uma única ferramenta de gerenciamento, de forma centralizada;
11.2. Deve possuir arquitetura cliente servidor, com interface web ou java podendo ser acessível através de browser web padrão;
11.3. Deve gerenciar, no mínimo, 50 dispositivos/IPs do ambiente;
11.4. Todas as licenças necessárias para o funcionamento da solução devem ser fornecidas;

11.5. Deve permitir que, no mínimo, 50 usuários administrativos acessem esta ferramenta de gerenciamento simultaneamente;
11.6. A ferramenta deve possibilitar a configuração de diferentes perfis de administradores. Deve ser possível ainda criar usuários com perfil de administração e outros de apenas visualização;
11.7. A ferramenta deve permitir autenticação de usuários administrativos via banco de dados interno, RADIUS, TACACS+ e LDAP;
11.8. Deve permitir o gerenciamento de configurações, desempenho e falhas na rede;
11.9. Deve permitir sua instalação em pelo menos uma das plataformas abaixo:
11.10. Windows Server 2012 ou mais recente;
11.11. LINUX: Red Hat Enterprise Linux versão 6 ou mais recente;
11.12. LINUX: Ubuntu versão 16 ou mais recente;
11.13. Appliance virtual VMware ESXi 6 ou mais recente;
11.14. Appliance virtual Hyper-V Server 2012 ou mais recente;
11.15. Deve permitir o descobrimento manual de equipamentos presentes em uma ou mais subredes. A ferramenta deve permitir, ainda, que dispositivos de rede configurados com uma opção de DHCP ou através de um nome conhecido via DNS possam buscar diretamente a ferramenta de forma automática.
11.16. Deve permitir pré-configurar as informações de gerenciamento dos dispositivos de rede com a finalidade de que os mesmos possam ser configurados automaticamente ao buscarem a ferramenta.
11.17. O software de gerenciamento deve suportar o protocolo SNMP de gerenciamento de versão 1, 2 e 3;
11.18. A solução de gerenciamento fornecida deve ser capaz de gerenciar equipamentos de outros fabricantes, pelo menos de forma básica através de MIBs padrões de mercado.
11.19. Deve permitir a criação de múltiplas topologias/mapas da infraestrutura de rede.
11.20. O mapa de topologia deve permitir adição de dispositivos de rede e, através de protocolos de descobrimento como LLDP, CDP ou similar, criar automaticamente os links entre os dispositivos de rede;
11.21. O mapa de topologia deve permitir a identificação de problemas na infraestrutura de rede através de mudança de cores;
11.22. O mapa de topologia deve permitir visualizar as VLANs configuradas em cada equipamento;
11.23. A ferramenta deve permitir a criação e remoção de VLANs nos dispositivos e associação de portas às mesmas;
11.24. A ferramenta deve permitir comparar as VLANs que foram configuradas pelo operador na ferramenta com as VLANs que já existem nos dispositivos e permitir que o operador escolha quais VLANs deverão ser sincronizadas com os dispositivos de rede.
11.25. A ferramenta deve permitir a definição de parâmetros relacionados à configuração inicial da malha ethernet (Fabric ethernet) para que os dispositivos da rede de malha ethernet possam subir a malha de forma centralizada;
11.26. A ferramenta deve permitir o provisionamento de serviços virtualizados em camada 2 e camada 3 nos dispositivos da malha ethernet (Fabric ethernet);
11.27. A ferramenta deve permitir visualização da topologia da malha ethernet (Fabric ethernet);
11.28. A ferramenta deve permitir realizar troubleshooting utilizando ferramentas como ping, traceroute ou similares diretamente no mapa de topologia;
11.29. A ferramenta deve permitir a visualização do caminho da malha ethernet selecionado entre dois determinados dispositivos que implementem a malha ethernet;
11.30. Deve permitir a identificação do status das portas dos dispositivos (up ou down), utilização e velocidade das portas;

11.31. Deve permitir desabilitar e habilitar as portas dos dispositivos da rede;
11.32. Deve permitir retornar dados dos dispositivos da rede via SNMP e permitir alteração desses parâmetros graficamente;
11.33. A ferramenta deve permitir receber logs dos dispositivos da rede via syslog;
11.34. Deve permitir a criação de alarmes customizados baseados em status dos dispositivos da rede, syslog, trap de SNMP, severidade dos eventos reportados, limiares de CPU, memória e banda de rede, entre outros.
11.35. Deve permitir a criação de alarmes com ações customizadas como envio de e-mail, execução de um script ou programa, criar um trap SNMP e enviar um syslog.
11.36. A ferramenta deve permitir a configuração de um servidor SMTP externo para o envio de informações de gerenciamento da ferramenta;
11.37. Deve suportar a localização de um dispositivo da rede baseado nos argumentos endereço IP, endereço MAC, user name e subrede;
11.38. A solução deverá prover recursos de "troubleshooting" capaz de mostrar dados presentes nos switches como processos, status de fontes e ventiladores, módulos, estatísticas de utilização das portas, disponibilidade, entre outros;
11.39. Deve permitir exportar os dados apresentados pela ferramenta em, pelo menos, formato csv;
11.40. Deve suportar a criação e o gerenciamento de políticas de classificação e priorização de tráfego (QoS) nos dispositivos da rede, baseado em perfis de usuários;
11.41. Deve suportar a criação e o gerenciamento de políticas de acesso à rede nos dispositivos da rede, baseado em perfis de usuários;
11.42. Deve suportar a atribuição de regras camada 2 até camada 4 e QoS ao perfil de usuário, de modo que o dispositivo da rede possa assinalar as regras para o usuário, conforme sua autenticação;
11.43. Deve suportar a atribuição de VLANs e identificadores de serviços da malha ethernet ao perfil de usuário, de modo que o dispositivo da rede possa assinalar a VLAN e o serviço da malha ethernet para o usuário, conforme sua autenticação;
11.44. A ferramenta deve permitir a configuração gráfica de rate limit nos dispositivos da rede;
11.45. A ferramenta deve permitir o inventário detalhado de atributos dos dispositivos da rede, atendendo, no mínimo, aos números seriais e versão do sistema operacional;
11.46. A ferramenta deve permitir o armazenamento das configurações dos dispositivos;
11.47. A ferramenta deve permitir o agendamento da função de armazenamento de configuração de determinados elementos da rede;
11.48. A ferramenta deve permitir a comparação da configuração atual do dispositivo com a configuração armazenada na ferramenta;
11.49. Deve permitir o upgrade do sistema operacional dos dispositivos, unitariamente e para um grupo de dispositivos, inclusive podendo agendar um dia e horário para que este upgrade aconteça automaticamente;
11.50. A ferramenta deve permitir restaurar a configuração armazenada;
11.51. A ferramenta deve permitir a criação de scripts baseados, pelo menos, em Python para execução de uma determinada tarefa nos dispositivos de rede;
11.52. A ferramenta deve implementar a criação de fluxos de trabalho baseados em blocos para automação de tarefas complexas que exijam interações que também possam estar fora do contexto do dispositivo de rede;
11.53. Os fluxos de trabalho devem permitir a adição de blocos que permitam executar um comando de CLI, executar um script, executar um comando no dispositivo de rede, realizar interações POST/GET em HTTP, enviar um email, etc;
11.54. Os fluxos de trabalho devem permitir ser executados manualmente pelo operador; em

decorrência de eventos de rede como alarmes; e de forma agendada;
11.55. A ferramenta deve fornecer relatórios gerenciais sobre o funcionamento da rede de forma histórica;
11.56. A ferramenta deve permitir a customização de relatórios utilizando os dados existentes em seu banco de dados;
11.57. A ferramenta deve permitir o envio periódico de relatórios via e-mail em formato pdf;
11.58. A ferramenta deve permitir executar um determinado comando via CLI em diversos dispositivos de rede simultaneamente;
11.59. A ferramenta deve possuir um terminal integrado com a finalidade de gerenciar os dispositivos de rede por linha de comando, via telnet e SSH. Deve ser possível copiar e colar comandos no terminal da ferramenta;
11.60. A ferramenta deve suportar adição de módulos para realização periódica de auditorias com a finalidade de reportar se os dispositivos de rede gerenciados estão em conformidade com GDPR, PCI, HIPAA ou similares.
11.61. Deve fornecer APIs abertas para integração com aplicações de terceiros.

12.**Software de controle de acesso de rede**
12.1. Deverá ser fornecida uma solução de controle de acesso centralizado que combine autenticação, auditoria de vulnerabilidade e serviços de localização para autorizar o acesso à rede e determinar o nível apropriado de serviço para usuários e dispositivos.
12.2. Deve vir com todo hardware, software e licenças necessários para suportar 3.000 dispositivos autenticados, por dia.
12.3. Suportar a configuração de diversas funções, incluindo visitantes e convidados, e permitir políticas de admissão diferentes para cada função.
12.4. Suportar o controle de acesso para redes cabeadas e sem fio.
12.5. Deve ser possível a utilização de appliances em hardware dedicado e virtuais.
12.6. Deve implementar aplicação de políticas de permissão, negação, priorização, limitação de banda, redirecionamento e classificação de tráfego de rede para equipamentos suportados, baseado na identificação do usuário, horário e localização.

13.**ESTRUTURA DE GERENCIAMENTO**
13.1. Deverá vir acompanhado do software de gerenciamento centralizado da solução na quantidade / modelo necessário para atender a solução completa desta solicitação;
13.2. Deverá permitir configuração via interface gráfica.
13.3. Deve prover gerenciamento integrado para controle de acesso de usuários e dispositivos à rede, que se conectem por meio de switches e equipamentos wireless.
13.4. Deve incluir:
13.5. - Dashborad contendo rede cabeada e sem fio com capacidade drill down
13.6. - Informacoes detalhadas sobre acesso e identidade dos usuários
13.7. - Relatorios personalizados com dados em tempo real e históricos
13.8. - Mapas de topologia
13.9. - Visão detalhada dos dispositivos contendo tipo de acesso (AP associado, SSID, BSSID), tipo de dispositivo (fabricante, modelo, sistema operacional (mesmo que virtualizado (tipo e versão))), localização exata no caso de clientes wireless (prédio, sala, andar), horário do dia (conexão e desconexão), aplicações autorizadas e QoS, autenticação (tipo MAC, 802.1x, portal web), autorização (perfil de regras de acesso, pessoa responsável em caso de visitantes)
13.10. - Log de eventos

35
ASR

13.11. - Função para busca de dispositivos e usuários
13.12. Deve implementar o ingresso automático e separação de dispositivos móveis gerenciados em categorias de políticas de segurança de acordo com o perfil definido para o usuário e dispositivo.
13.13. Deve suportar provisionamento de base de política de segurança aos dispositivos móveis e cabeados suportados.
13.14. Deve implementar visibilidade completa de todos os dispositivos móveis gerenciados na infraestrutura.
13.15. Deve suportar integração com plataformas MDM e firewalls de mercado.
13.16. Permitir o backup e a restauração das políticas e configurações via ferramenta de Administração.
13.17. Capacidade de visualização das seguintes informações:
13.18. - Nome do Usuário;
13.19. - Endereço MAC do usuário;
13.20. - Endereço IP do usuário;
13.21. - Perfil do usuário;
13.22. - Sistema Operacional do usuário;
13.23. - Resultado do processo de controle de acesso à rede;
13.24. Deverá implementar dashboards e visualizações detalhadas dos dispositivos autenticados ou tentando se autenticar à rede.
13.25. Deverá implementar a possibilidade de customização de visualização dos dashboards para apresentação da informação no formato preferido.
13.26. Deverá suportar notificações e alarmes via syslog, e-mail ou serviços de web para mudanças de estados de dispositivos e registro de visitantes.
13.27. Deverá suportar a função de Mapeamento IP-para-ID que conecta as informações de Nome de usuário, Endereço IP, Endereço MAC e a porta física de cada dispositivo.
13.28. "Através de interface de administração, permitir ao administrador da solução a criação e manutenção dos seguintes elementos de acesso:
13.29. - Grupos de usuários
13.30. - Grupos de visitantes
13.31. - Grupos de dispositivos fixos
13.32. - Grupos de dispositivos móveis
13.33. - Regras de acesso dos usuários, dos visitantes, e dos dispositivos às redes internas, sejam redes cabeadas ou redes sem fio."
13.34. **AUTENTICAÇÃO**
13.34.1. Deverá implementar autenticação por usuário
13.34.2. Deverá implementar autenticação por endereço MAC
13.34.3. Deverá suportar integração com servidores RADIUS e LDAP para fins de autenticação.
13.34.4. O processo de autenticação deverá seguir o padrão IEEE 802.1X ou método similar que utilize protocolo seguro SSL em conjunto com servidor de políticas, e deverá permitir a alteração da VLAN do usuário conforme o perfil do mesmo.
13.34.5. Capacidade de se integrar e fazer parte de um domínio MS-Active Directory, bem como atender demandas de acesso à rede provenientes de pedidos de autenticação.
13.34.6. Capacidade de autenticar dispositivos que não permitem o processo de validação de usuário (impressoras, telefones, câmeras, etc)
13.34.7. Deverá prover o contexto de quais dispositivos estão na rede e quais as particularidades associadas à esses dispositivos.
13.35. **AUTORIZAÇÃO**

13.35.1. Permitir a associação de políticas conforme o sistema operacional da estação sendo validada ou conforme o domínio de segurança configurado.
13.35.2. Deve suportar aplicação das regras diretamente nos switches de acesso, através de controle de regras de segurança ou VLANs, com suporte ao padrão RFC 3580 (VLAN Authorization).
13.35.3. Deve permitir a configuração de lista de exceções por nome de usuário, endereço MAC, ou grupos de endereço MAC.
13.35.4. Deve ser possível configurar cada exceção para permitir, negar, avaliar, ou colocar em rede distinta por regra de segurança ou VLAN.
13.36. **PORTAIS**
13.36.1. Deve implementar um portal para auto-registro de accesso visitante.
13.36.2. Deve implementar um portal de acesso a convidados através de autorização explícita do funcionário responsável pelo convidado (Sponsorship) sem o envolvimento da equipe de administração da rede.
13.36.3. O portal com a função "Sponsor" habilitada deve fornecer a opção de responsável fixo pelo acesso e também a opção de lista de responsáveis para a escolha do visitante
13.36.4. Deve implementar um portal interno de acesso aos responsáveis (Sponsors) com usuário e senha para visualização da lista de convidados aguardando acesso com opção de liberação ou bloqueio do mesmo à rede.
13.36.5. Deve suportar uma página HTML de convidados para registro de endereços MAC onde os usuários não registrados no servidor de autenticação precisam aceitar política de acesso à rede, preenchendo um "Username" para ser associado ao endereço MAC e aceitando uma política de convidados.
13.36.6. O portal deve permitir auto-registro utilizando mídias sociais como Facebook, Microsoft e LinkedIn.
13.36.7. Deve implementar a importação e exportação da relação de credenciais temporárias através de arquivos txt ou csv;
13.36.8. Deve permitir a criação de validade das credenciais, baseando o início da validade na criação da conta ou no primeiro login da conta;
13.36.9. Deve permitir a customização do formulário de criação de credenciais, a ser preenchido pelo autorizador ou pelo visitante, em caso de autosserviço, especificando quais informações cadastrais dos visitantes são obrigatórias ou opcionais;
13.36.10. Deve permitir a customização do nível de segurança da senha temporária que será gerada ao visitante, especificando a quantidade mínima de caracteres e o uso de letras e números para compor a senha;
13.36.11. Deve exigir que o usuário visitante aceite o "Termo de uso da rede" a cada login ou apenas no primeiro login;
13.36.12. Deve permitir o envio das credenciais aos usuários registrados através de mensagens SMS (Short Message Service), email e/ou impressão local.
13.36.13. Deve implementar funcionalidade de acesso por SSID único, onde o NAC fará o direcionamento para a VLAN ou Política de Segurança.
13.37. **RELATÓRIOS**
13.37.1. Deverá implementar relatórios de estatísticas com visualizações variadas, de conexão dos dispositivos à rede com visualização de aceitos, rejeitados, com erro e desconectados.
13.37.2. Deverá implementar relatórios de alocações de perfil aplicado por usuário.
13.37.3. Deverá implementar Dashboards customizado para relatórios em tela.
13.37.4. Deverá implementar relatórios de identificação e acesso de todos os dispositivos conectados com visualização em tempo real e histórica de conexão e estatísticas com customização de maior para

o menor (Top Down).
13.37.5. Todos os relatórios gráficos (Dashboards) deverão também mostrar listagens detalhadas de sua composição.
13.37.6. Deverá implementar relatórios com visualização de tipos de conexão.
13.37.7. Deverá implementar relatórios de regras aplicadas aos dispositivos.
13.37.8. Deverá implementar relatório de topologia interativo com visualização da estrutura de conexão desde a borda até o recurso utilizado, com opção de localização do usuário.
13.37.9. A visualização da topologia deverá exibir os ícones dos equipamentos e dispositvos com identificação dos mesmos com menus interativos disparados diretamente dos ícones (Drill Down)
13.37.10. Deverá implementar relatório histórico de autenticações dos dispositivos.
13.37.11. Deverá permitir identificação de todos os dispositvos conectados.
13.37.12. Prover relatórios com as seguintes informações:
13.37.12.1. - Atividades de login dos usuários;
13.37.12.2. - Condições de erro;
13.37.12.3. - Dispositivos/usuários autenticados com sucesso;
13.37.12.4. - Dispositivos/usuários não autenticados.
13.37.12.5. - Permitir a exportação de relatórios via HTML, CSV ou pdf;

14.**Software de análise de aplicações.**
14.1. A solução deverá ser do mesmo fabricante e ser capaz de prover análise em camada 7 das aplicações atendendo aos requisitos abaixo.
14.2. Todo hardware que compõe a solução deverá ser instalado em gabinete padrão de 19 polegadas, com fornecimento dos respectivos conjuntos de fixação.
14.3. O dispositivo de análise de aplicações deve ser fornecido em forma de appliances físicos ou virtuais, instalados, configurados e possuindo todos os softwares necessários para prover os requisitos técnicos especificados, inclusive o sistema operacional, sem qualquer ônus adicional.
14.4. No caso de appliances físicos ou servidores, a solução poderá adotar hardwares padrão de mercado, desde que atendam aos requisitos RECOMENDADOS pela última versão do manual de instalação dos softwares utilizados.
14.5. Caso a solução fornecida seja baseada em appliances virtuais, deverá ser possível a instalação da solução em plataforma VMware e MS Hyper-V.
14.6. Todo hardware que compõe a solução deverá possuir alimentação elétrica de 110/240 V, 60 Hz, com chaveamento automático.
14.7. A solução deve ser capaz de visualizar e gerenciar os dados e métricas coletados em múltiplos segmentos monitorados em uma única console, permitindo desta forma integração, maior segurança, escalabilidade, robustez e disponibilidade da solução.
14.8. A solução deve possuir uma interface gráfica e intuitiva com API abertas para simples customização de aplicações e integração com produtos de terceiros.
14.9. Deverá ser capaz de inspecionar todos os pacotes recebidos, a partir de sensores de dados, em nível de aplicação, ou seja, deve ser capaz de identificar cada aplicação/assinatura e correlacionar com sua biblioteca interna.
14.10. A solução de análise de aplicações deve prover visibilidade em camada 7 em toda a rede através da combinação de sensores de dados. Entende-se por sensor de dados equipamentos como switches ou access points ou appliances específicos para de coleta de dados da rede com a finalidade de encaminhar os dados coletados ao appliance de análise de aplicações.
14.11. Deve permitir habilitar, desabilitar e apagar assinaturas de aplicações.
14.12. A solução deverá estar licenciada para suportar a análise de, no mínimo, 3.000 clientes.

14.13. Solução deve ser escalável, permitindo adição horizontal de novos appliances para inspeção em camada 7 do tráfego proveniente dos sensores.
14.14. Deve ser integrável com solução de gerenciamento centralizada.
14.15. A solução deve permitir a configuração de usuários com diferentes níveis de permissão.
14.16. A solução deve suportar a integração com a ferramenta de controle de acesso do mesmo fabricante para correlacionar informações sobre o login do usuário com suas aplicações utilizadas na rede.
14.17. Deve permitir a visualização de relatórios do consumo das aplicações, de maneira histórica, através de dashboards com relatórios do tipo pizza, árvore e bolha.
14.18. Os relatórios devem permitir a visualização de, no mínimo:
14.18.1. - Aplicações mais utilizadas (camada 7);
14.18.2. - Top clientes que mais utilizam determinada aplicação;
14.18.3. - Top aplicações mais utilizadas por determinado cliente;
14.18.4. - Locais (Sites) que mais utilizaram determinada aplicação;
14.18.5. - Quantidade de bytes trafegada por aplicação;
14.18.6. - Tipos de aplicações;
14.18.7. - Quantidade de fluxos;
14.18.8. - Grupos de aplicações;
14.19. - Top servidores de aplicações rastreadas.
14.20. A solução deve permitir que os usuários façam "drill down" à partir de visões de alto nível, orientadas a serviços, até visões técnicas com dados detalhados, que auxiliem na análise da causa raiz do problema.
14.21. A solução deve prover telas nas quais seja possível visualizar graficamente a disponibilidade dos serviços do ambiente de aplicações, incluindo quais serviços estão ultrapassando os limites de tempos de resposta estabelecidos.
14.22. A solução deve permitir a visualização dos serviços individualmente ou unidos em grupos lógicos definidos pelo usuário.
14.23. A solução deve ser capaz de monitorar N segmentos de rede de forma simultânea, permitindo assim a monitoração do tráfego das aplicações multicamadas e/ou distribuídas.
14.24. Deve ser capaz de receber e processar informações de todas camadas da rede, incluindo acesso, distribuição, core e datacenter.
14.25. A solução deve ser capaz de consolidar as métricas de desempenho de múltiplos dispositivos sensores de dados, incluídos appliances, máquinas físicas e virtuais fornecidas pela solução.
14.26. A solução deve prover visão unificada do desempenho das aplicações através de toda a infraestrutura.
14.27. Deve permitir verificar quais aplicações estão consumindo maior largura de banda na rede, assim como a latência de cada aplicação.
14.28. A solução deve prover informações precisas com relação a detecção de aplicações, inclusive aplicações que utilizem portas TCP e UDP.
14.29. Deve ser possível visualizar os fluxos bidirecionais e unidirecionais.
14.30. Deve permitir a visualização destes fluxos permitindo inclusive filtrá-los das seguintes opções:
14.30.1. - Fluxos mais recentes, por dispositivo para análise profunda dos pacotes;
14.30.2. - Maior tempo de resposta por conexões TCP;
14.30.3. - Maior tempo de resposta por aplicação;
14.30.4. - Fluxos por grupos de aplicação.
14.30.5. - Bytes recebidos e/ou enviados;
14.30.6. - Fluxos de entrada e/ou saída;

14.31. Deverá permitir a configuração do tempo de refresh da visualização dos fluxos.
14.32. Deverá permitir filtragem e visualização de fluxos por busca de parâmetros, tais como, endereços IP, grupo de aplicação, tempos de resposta e protocolo.
14.33. Deverá permitir verificar o número de vezes que fluxos se utilizaram de determinadas assinaturas.
14.34. Deverá ser possível a exportação de relatórios em formato csv.
14.35. Deverá permitir a comparação entre tempos de resposta da rede e tempos de resposta das aplicações para fins de resolução de problemas.
14.36. A solução deve permitir rastrear determinadas aplicações, permitindo gerar um alarme, por exemplo, durante alterações no comportamento do tempo de resposta destas, para resolução de problemas de forma pró ativa. Deve permitir, ainda, executar um fluxo de trabalho ou script customizados relacionados ao comportamento adverso da rede.
14.37. Deve permitir também a visualização histórica do tempo de resposta das aplicações rastreadas.
14.38. Deverá permitir a atualização da base de assinaturas das aplicações através de acesso a servidor de assinaturas disponibilizada pelo fabricante da solução, de forma manual (não automática) e automática (com opção de atualização diária e mensal).
14.39. A solução deve prover monitoramento de segmentos de rede e dispositivos ininterruptamente.
14.40. A solução deve permitir uma interface flexível para configuração de alarmes. Os alarmes podem ser compostos por aplicações, sub-redes, endereços IP e URLs.
14.41. A solução deve enviar alerta quando o tempo de resposta de uma requisição ultrapassar o limite definido para o serviço requisitado ou quando o serviço ficar indisponível. Este alertas deverão ser transmitidos através de traps SNMP e e-mails para um ou mais destinatários pré-definidos.
14.42. A solução deve, a partir da base histórica formada pelo conhecimento do comportamento da infraestrutura, permitir estabelecer uma gerência de limites com alertas adaptativos.
14.43. A solução deve permitir a consulta dos alertas enviados em um determinado período, informado pelo usuário no seguinte formato: data/hora inicial e data/hora final.
14.44. A solução deve ser capaz de gerar alarmes nos seguintes formatos: trap snmp, email e na própria console.
14.45. Deverá suportar a captura de pacotes em formato pcap ou similar para uso em ferramentas específicas de análises como Wireshark, por exemplo.
14.46. A solução deverá prover o gerenciamento centralizado dos dispositivos sensores de dados fornecidos.
14.47. Deverá permitir a visualização dos dispositivos sensores de dados.
14.48. Deverá disponibilizar facilidades para adicionar e retirar dispositivos sensores de dados.
14.49. Deverá permitir a coleta de fluxos através de sensores de dados via Netflow ou Sflow ou IPFIX ou similar.
14.50. A solução deverá suportar a conexão a vários sensores de dados operando simultaneamente.

15. **Serviços de interligação de racks por link de fibra óptica ao data center**
15.1. Especificações:
15.1.1. A CONTRATADA deverá fornecer todos materiais necessários para a instalação, configuração e operação, de forma a garantir a capacidade operacional de transmissão de dados de 02 (dois) circuitos duplex (transmissão e recepção simultâneos) para cada rack contemplado com capacidade operar em velocidades de 10Gbps em cada par, nas condições e forma descritas neste Edital e seus anexos.
15.1.2. Os serviços contemplam a interligação de 20 racks (de propriedade do Contratante) ao Data Center, sendo que 9 racks devem ser aproveitando os cabos existentes, 9 racks devem ser passados novos cabos conforme topologia rede.

15.1.3. A CONTRATADA deverá fornecer o DIO com terminais LC;
15.1.4. A CONTRATADA deverá fornecer e instalar todos os equipamentos, materiais, acessórios, fazer o lançamento dos cabos nos postes (quando necessário), fazer a fusão e certificar a infraestrutura de fibras óticas, conforme segue as especificações deste item.
15.1.5. Todos os serviços deverão seguir e estar em completo acordo com as normas e recomendações dos organismos governamentais competentes, ainda que não especificados neste termo, nas versões vigentes quando da apresentação das propostas.
15.1.6. Os links de Comunicação deverão possuir níveis de atenuação e dimensionamento adequados de forma a garantir a transmissão de dados de acordo com a banda de transmissão prevista
15.1.7. A CONTRATADA deverá elaborar e entregar ao CONTRATANTE, em mídia eletrônica e cópias impressas, Projeto Executivo plotado em CAD para todos os serviços descritos neste termo, contendo cronograma de serviços, detalhes técnicos da execução dos serviços e lista de pessoas que trabalharão nas atividades previstas nesse Projeto Executivo;
15.1.8. Elaboração do projeto executivo da instalação dos equipamentos de conectividade existentes. O projeto executivo deverá ser elaborado somente após:
15.1.9. A realização de vistoria dos pontos e locais a serem instalados;
15.1.10. É responsabilidade da CONTRATADA disponibilizar todo cabeamento necessário, desde o Datacenter até o local definido para instalação dos equipamentos ativos, bem como eventuais adaptações nas instalações físicas das Unidades (passagem de cabos, lançamento de fibras ópticas, etc.);
15.1.11. A infraestrutura de fibras ótica deve ser aproveitada as existentes nos locais de instalação quando possível, ficando por conta e providência da CONTRATADA realizar a infraestrutura necessária caso não exista rede física em algum local de instalação.
15.1.12. A empresa CONTRATADA deverá fornecer documentação pertinente a instalação infraestrutura de fibras ótica, "As Built", contendo diagrama de blocos do sistema e subsistema, Lay-Out dos equipamentos, distribuição de equipamentos no Rack, encaminhamento de cabo de fibra óptica.
15.1.13. Os testes deverão ser realizados pela CONTRATADA e acompanhados por profissionais da CONTRATANTE de forma a certificar a correta instalação da solução.
15.1.14. Após a realização de todos os testes, deverá ser apresentado pela CONTRATADA um relatório impresso com o detalhamento de todos os testes realizados, bem como os resultados obtidos.
15.1.15. Para efeito de contrato, os links somente serão considerados ACEITOS (implantados e ativados), quando os testes de conectividade entre os equipamentos de cada localidade ocorrer dentro dos parâmetros de desempenho aceitáveis pela CONTRATANTE.
15.1.16. Segue abaixo planilha de referência de materiais:

PLANILHA REFERÊNCIA DE MATERIAIS			
Item	**Descrição do Material**	**Un**	**Qtde**
1	Eletrocalha lisa sem tampa tipo C 100x50x3000mm	br	9
2	Tampa para eletrocalha 100x3000mm	br	9
3	Conexão para eletrocalha lisa com tampa tipo curva horizontal 90º 100x50mm	pç	2
4	Conexão para eletrocalha lisa com tampa tipo Curva de inversão 90º 100x50mm	pç	1
5	Suspensão vertical 100 x 50	pç	27

6	Mão Francesa Simples 38x38x100mm	pç	27
7	Tala de emenda 80x50mm	pç	18
8	Tirante rosqueado 1/4"x3000mm	pç	6
9	Terminal de fechamento liso 50x50mm	pç	2
10	Parafuso cabeça lentilha auto travante rosca NC 1/4x1/2"	pç	109
11	Arruela lisa 1/4"	pç	109
12	Porca sextava zincada 1/4"	pç	109
13	Distanciador "U" simples	pç	29
14	Chumbador CBA 1/4	pç	29
15	Eletroduto leve zincado Ø (1 1/2")	m	21
16	Luva de aço para eletroduto leve zincado, Ø (1 1/2")	pç	7
17	Abraçadeira tipo D com cunha 1 1/2"	pç	20
18	Eletroduto flexível tipo seal tube Ø (1 1/2")	m	25
19	Saída horizontal p/ eletroduto 1 1/2"	pç	3
20	Unidut Cônico 1.1/2" em alumínio silício	pç	3
21	Unidut Reto 1.1/2" em alumínio silício	pç	3
22	Bucha S-8 para alvenaria	pç	55
23	Parafuso S-8	pç	55
24	Caixa de sobrepor 30x30x10cm	pç	2
25	Distribuidor interno óptico com capacidade para 48 fibras OM3, padrão 19" x 1U	pç	5
26	Distribuidor interno óptico com capacidade para 12 fibras OM3, padrão 19" x 1U	pç	7
27	Distribuidor interno óptico com capacidade para 12 fibras SM, padrão 19" x 1U	pç	2
28	Cabo Optico Indoor/Outdoor 12F MM (50) OM3	m	1750
29	Cabo Optico Indoor/Outdoor 12F SM	m	150
30	Alça Pref. Loop Longo 9,000 a 10,00mm	pç	5
31	Abraçadeira BAP 3 C. Ajust. P/Poste C/Paraf.	pç	5
32	Suporte Reforçado P/ BAP 14mm	pç	5
33	Parafuso M12 X 35mm Frances C/ Porca ZF	pç	5
34	Plaqueta Identificação Cabo Optico Injetado. 3mm	pç	350

Obs.: A Lista de materiais acima é meramente estimativa e será de responsabilidade de cada licitante fazer as verificações necessárias ao realizar a vistoria, pois, não será admitindo posteriormente a alegação da inclusão de novos materiais.

15.1.17. **Especificações Técnicas Mínimas Obrigatórias**

15.1.17.1. Eletrocalhas metálicas

a) Quando utilizadas (mencionadas em projetos ou memorial descritivo) deverão ser em chapa de aço pré-zincada a quente conforme padrões CSN zincadas, atendendo ao estabelecido nas normas NBR-7008, nas dimensões indicadas no Anexo III.
b) As eletrocalhas deverão ser fornecidas com as seguintes chapas:
    i. Chapa #24:
        - Eletrocalha lisa sem tampa tipo C 50x50x3000mm
        - Eletrocalha lisa sem tampa tipo C 75x50x3000mm
        - Eletrocalha lisa sem tampa tipo C 75x75x3000mm
        - Eletrocalha lisa sem tampa tipo C 100x50x3000mm
    ii. Chapa #22:
        - Eletrocalha lisa sem tampa tipo C 100x100x3000mm
        - Eletrocalha lisa sem tampa tipo C 150x50x3000mm
    iii. Chapa #20:
        - Eletrocalha lisa sem tampa tipo C 150x100x3000mm
        - Eletrocalha lisa sem tampa tipo C 200x50x3000mm
        - Eletrocalha lisa sem tampa tipo C 300x75x3000mm
c) Deverão ser dobradas em forma de "U" sem virola proporcionando maior resistência a flexo-torção.
d) Todas as eletrocalhas serão lisas com tampa. Toda a fixação será com os acessórios adequado, pré-fabricados e de mesma linha das eletrocalhas.
e) As curvas e acessórios seguirão as mesmas características construtivas do trecho reto, porém, suas formas geométricas são próprias, atendendo as mais diversas situações de montagem e distribuição.
f) Apresentar catálogo do Fabricante.

15.1.17.2. **Eletroduto corrugado flexível PVC**

a) Fabricado em PVC antichama, deve possuir alta resistência a agressões químicas e baixo coeficiente de atrito;
b) Será utilizado na proteção de condutores elétricos e de telecomunicações;
c) Deve atender a norma ABNT NBR 15465.
d) Apresentar catálogo do Fabricante.

15.1.17.3. **Eletroduto Rígido de Aço Carbono**

a) Eletroduto Rígido de Aço Carbono, com solda longitudinal zincado por imersão a quente, de seção circular, comprimento padrão de 3 metros, rosca em ambas as extremidades, com 1 luva;
b) Os diâmetros dos eletrodutos estão especificados na planilha de materiais;
c) Devem obedecer às prescrições da NBR 5624;
d) Deverão acompanhar todos os acessórios e conexões necessárias à instalação e fixação dos mesmos, tais como: luva, curva, bucha e arruela, entre outros.
e) Utilizado principalmente em instalações prediais e industriais de média e baixa tensões. Pode ser aplicado embutido, aparente ou ao tempo.
f) Apresentar catálogo do Fabricante.

15.1.17.4. **Suporte Dielétrico para Cabo Óptico Aéreo**

a) Conjunto composto por corpo articulado base e tampa, coxim bipartido e parafuso de fechamento, que tem por função a suspensão dos cabos óticos fixados nos postes intermediários de uma seção de ancoragem.
b) O corpo articulado deve ser constituído de material polimérico, reforçado com fibra de vidro e aditivo contra raios ultravioletas, conferindo alta resistência a esforços mecânicos e a intempéries climáticas.
c) O coxim bipartido deve ser feito à base de borracha sintética para minimizar os esforços da compressão radial e absorver esforços angulares de torção e flexão sobre o cabo, possuindo inserto de material termoplástico para garantir a ancoragem do cabo.
d) O parafuso de fechamento, a porca sextavada, as arruelas plana e de pressão deverão ser em aço zincado a fogo e os pinos de articulação da tampa deverão ser em alumínio com tratamento superficial, conferindo ao conjunto especial resistência a ambientes agressivos. Deve ser projetado para suportar esforços longitudinais e transversais de até 80kgf.
e) O fechamento do Suporte Dielétrico deve ser feito com a utilização de uma chave tipo canhão ou com chave de torque.
f) Apresentar catálogo do Fabricante.

15.1.17.5. **Conjunto de Ancoragem com Armadura Pré-Formada para Cabo Óptico**

a) Conjunto composto por corpo articulado (base e tampa), coxim bipartido, armadura pré-formada com antideslizante, parafuso de fechamento, abraçadeira e alça de ancoragem, que tem por função a fixação mecânica do cabo ótico aéreo autosustentado nos extremos de uma seção de ancoragem.
b) O corpo articulado e a abraçadeira devem ser constituídos de material polimérico, reforçado com carga e aditivo contra raios ultravioleta, conferindo alta resistência a esforços mecânicos e a intempéries climáticas. O coxim bipartido deve ser de borracha sintética, absorvendo as vibrações do cabo. A armadura pré-formada deve promover o ancoramento do cabo de forma uniforme, preservando sua integridade nas condições de operação. O parafuso de fechamento, a porca sextavada, as arruelas plana e de pressão, os pinos de rotulação e o cabo de aço da alça de ancoragem devem ser fabricados em aço inoxidável. A armadura pré-formada deve ser confeccionada em aço mola zincada a quente.
c) Apresentar catálogo do Fabricante.
d) Características Técnicas:
e) Resistência ao torque no parafuso: até 1,0 kgf.m
f) Comprimento da Armadura para vãos de 80 m:500 mm
g) Comprimento padrão da Alça: 260 mm

15.1.17.6. Cabo de Fibra óptica MM

a) Cabo óptico tipo tight com 12 fibras tipo multímodo 50/125um;
b) Deverá apresentar atenuação máxima de 3,5dB/Km em 850nm e 1,5 dB/Km em 1300nm;
c) Deverá possuir elemento de tração composto por fibras dielétricas;
d) Possuir máxima tensão de instalação de pelo menos 1,0 X Peso do cabo por Quilometro;
e) Ser fabricada conforme ABNT NBR 14772/2020 / ANATEL: anexo a resolução 299;

f) Deverá ser apresentado certificação ISO 9001 e ISO 14000 do fabricante do produto.
g) Apresentar catálogo do Fabricante.

15.1.17.7. Cabo de Fibra óptica SM

a) Cabo óptico tipo tight com 12 fibras tipo monomodo 9/125um;
b) Deverá apresentar atenuação máxima de 0,5dB/Km em 1310nm e 0,3 dB/Km em 1550nm;
c) Deverá possuir elemento de tração composto por fibras dielétricas;
d) Possuir máxima tensão de instalação de pelo menos 1,0 X Peso do cabo por Quilometro;
e) Ser fabricada conforme ABNT NBR 14772/2020 / ANATEL: anexo a resolução 299;
f) Deverá ser apresentado certificação ISO 9001 e ISO 14000 do fabricante do produto.
g) Apresentar catálogo do Fabricante.

15.1.17.8. Distribuidor Interno Óptico (DIO)

a) Deverá ser padrão 19" em chapa de aço e termoplástico PC na cor RAL 7035, 1U de altura;
b) Os modelos devem apresentar funcionalidade tanto para a terminação direta ou fusão de pig-tail de até 48 fibras;
c) Ter a capacidade de aceitar diversos tipos de conectores óptico;
d) Deve apresentar painel frontal articulável tipo gaveta;
e) Deve apresentar proteção contra corrosão;
f) Deverá ser apresentado certificação ISO 9001 e ISO 14000 do fabricante do produto.
g) Apresentar catálogo do Fabricante.

29.Atualização

29.1. A contratada deverá disponibilizar, na vigência do contrato, todas as atualizações dos softwares e firmwares dos equipamentos, concebidas em data posterior ao seu fornecimento, pelo período especificado no termo de referência, sem qualquer ônus adicional para o contratante;

29.2. As atualizações incluídas devem ser do tipo "minor release" e "major release", permitindo manter os equipamentos atualizados em sua última versão de software/firmware.

30.Padronização

30.1. Conforme disposto no item I do artigo 15 da lei 8;666, de 21 de junho de 1993 (I - Atender ao princípio de padronização, que imponha compatibilidade técnica e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas), estes equipamentos, por questões de compatibilidade, gerência, suporte e garantia, devem ser do mesmo fabricante dos equipamentos deste grupo (lote).

31.Serviços de Instalação, ativação e teste

31.1. A INSTALAÇÃO contempla a desembalagem, a montagem de todos os componentes que integram a especificação, a instalação dos equipamentos montados em rack padrão 19", conforme o caso, a energização do equipamento (não contempla a infraestrutura de energia elétrica, circuitos, tomadas, etc);

31.2. A configuração contempla, a realização dos ajustes de hardware e software necessários ao funcionamento integrado da solução ao ambiente da CONTRATANTE e a instalação da solução de gerenciamento dos equipamentos;

85

31.3. Todas as atualizações de firmware ou qualquer outro software componente dos switches, deverão estar na versão mais atualizada disponível ou a última compatível com as demais soluções deste lote e considerada estável;
31.4. Habilitação de licenças que porventura sejam adquiridas e recursos dos equipamentos que serão utilizados no projeto;
31.5. A CONTRATADA de verá implementas as verificações dos recursos e o seu perfeito funcionamento e integração com os demais, conforme as melhores práticas indicadas pelo fabricante;
31.6. A interconexão do(s) equipamento(s) à rede ethernet da CONTRATANTE;
31.7. A migração de configurações do ambiente atual da CONTRATANTE para o novo ambiente;
31.8. Os funcionários da CONTRATADA deverão possuir todo o ferramental necessário ao exercício das suas atividades;
31.9. Os serviços deverão ser realizados por pessoal técnico experiente e certificado pelo fabricante dos equipamentos. Em momento anterior à instalação, a contratante poderá solicitar os comprovantes da qualificação profissional do(s) técnico(s) que executará(ão) os serviços, sendo direito da mesma a sua aceitação ou exigência de troca de profissional no caso de este não satisfazer às condições supramencionadas;
31.10. A CONTRATADA deve garantir a confidencialidade das informações, dados e senhas compartilhadas da CONTRATANTE;
31.11. Durante as atividades realizadas na prestação do serviço, o técnico da CONTRATADA deve demonstrar à equipe técnica de acompanhamento da CONTRATANTE como instalar e configurar os equipamentos e os softwares fornecidos;
31.12. As atividades deverão ser realizadas dentro do horário comercial;
31.13. O planejamento dos serviços de configuração deve resultar num documento "Projeto Executivo ou Escopo do Trabalho". Neste documento devem conter a relação, descrição e quantidades dos produtos fornecidos, descrição da topologia atual e desejada, detalhamento dos serviços que serão executados, premissas do projeto, locais e horários de execução dos serviços, condições de execução dos serviços, pontos de contato da contratante e contratada, cronograma de execução do projeto em etapas, com responsáveis e data e início e fim (se aplicável), relação da documentação a ser entregue ao final da execução dos serviços, responsabilidade da contratante e contratada, plano de gerenciamento de mudanças, itens excluídos no projeto e termo de aceite. Os serviços não poderão ser iniciados antes da apresentação e assinatura de concordância de ambas as partes;
31.14. Todos os parâmetros a serem configurados deverão ser alinhados entre as partes em reuniões de pré-projeto, devendo a contratada sugerir as configurações de acordo com normas técnicas e boas práticas, cabendo à contratante a sua aceitação expressa ou recusa nos casos de não atendimento das condições estabelecidas;
31.15. Ao término dos serviços deve ser criado um relatório detalhado contendo todos os itens configurados no projeto (relatório as-built), etapas de execução e toda informação pertinente para posterior continuidade e manutenção da solução instalada, como usuários e endereços de acesso, configurações realizadas e o resumo das configurações dos equipamentos. Este relatório deve ser enviado com todas as informações em até 15 dias após a finalização dos serviços;

32.Treinamento

32.1. Os serviços de treinamento deverão contemplar a explanação teórica e prática para no mínimo 4 (quatro) administradores da solução.
32.2. Os serviços de treinamento devem serem realizados nas dependências da CONTRATANTE, com carga horária mínima de 24 horas distribuídas em aulas de 8 horas diárias, em data e horário a ser definido entre as partes.

32.3. A CONTRATANTE disponibilizará sala para o treinamento com infraestrutura e apoio básicos (sala com energia elétrica, ar-condicionado, cadeiras, projetor, tela de projeção, computadores).
32.4. A CONTRATADA deverá fornecer manual da solução em mídia eletrônica.
32.5. Conteúdo programático: Arquitetura de funcionamento; Configuração básica para funcionamento; Configuração de gerenciamento.
32.6. A CONTRATADA disponibilizará à CONTRATANTE o relatório da execução do treinamento.
32.7. Deverá ser fornecido certificado de participação do treinamento.

PROTOCOLO SEPLAG
Fls. 87
Rub.

TERMO DE ANÁLISE, APROVAÇÃO E AUTORIZAÇÃO.

1 – DA ANALISE E APROVAÇÃO:

1.1 Analisamos e aprovamos o Termo de Referência nº 05/2020/SUTIS/SAAS/SEPLAG, PLANILHA e PROCESSO INICIAL, sendo constatada a regularidade legal da proposta.

2 – DA AUTORIZAÇÃO:

2.1 Analisado e aprovado o Termo de Referência nº 05/2020/SUTIS/SAAS/SEPLAG inerente e face aos processos e documentos vinculantes, AUTORIZO os procedimentos legais desta licitação, cujos atos procedimentais e contratação devem obediência às condições e termos previstos no presente Termo de Referência supracitado, processo administrativo inerente e legislação vigente.

Data:_____/_____/2020.

Basílio Bezerra Guimarães dos Santos
Secretário de Estado de Planejamento e Gestão