Governo do Estado do Rio de Janeiro
Centro de Tecnologia da Informação e Comunicação do Estado do Rio de Janeiro
Vice Presidência de Tecnologia

TERMO DE REFERÊNCIA

1. **DO OBJETO:**

1.1. Registro de preços para Aquisição de ativos de rede, composto de hardware, softwares de gerenciamento de redes, abrangendo serviços de instalação, suporte e garantia on-site pelo período de 60 (sessenta) meses, visando atender às demandas do PRODERJ e demais Órgãos da Administração Pública, conforme especificações, quantidades e exigências estabelecidas neste Termo de Referência e seus anexos.

1.2. A tabela abaixo apresenta a descrição e quantidade estimada:

LOTE	ID SIGA	ITEM	DESCRIÇÃO	QTD
ÚNICO	**168141**	1	Switch Core	42
	168142	2	Switch Core - Módulo de Interface Tipo I	34
	168143	3	Switch Core - Módulo de Interface Tipo II	60
	168144	4	Switch Core - Módulo de Interface Tipo III	51
	168145	5	Switch Core - Módulo de Interface Tipo IV	48
	168146	6	Switch de Distribuição - Tipo I	166
	168149	7	Switch de Distribuição - Tipo II	64
	168150	8	Switch de Distribuição - Tipo III	241
	168151	9	Switch de Distribuição - Tipo IV	80
	168152	10	Switch de Acesso - Tipo I	1237
	168153	11	Switch de Acesso - Tipo II	698
	168165	12	Controladora WLAN	66
	168166	13	Ponto de Acesso WLAN	3833
	168167	14	Plataforma de Gerenciamento	23

	168154	15	INTERFACE 100GB QSFP SR	581
	168155	16	INTERFACE 100GB QSFP LR	102
	168156	17	INTERFACE 40GB QSFP SR	840
	168157	18	INTERFACE 40GB QSFP LR	250
	168158	19	INTERFACE 25GB SFP28 SR	558
	168159	20	INTERFACE 25GB SFP28 LR	134
	168160	21	INTERFACE 10GB SFP+ SR	906
	168161	22	INTERFACE 10GB SFP+ LR	552
	168162	23	INTERFACE 1GB SFP SX	283
	168163	24	INTERFACE 1GB SFP LX	93
	168164	25	CONVERSOR QSFP PARA 4 SFP+	686

1.3. As especificações técnicas dos equipamentos e serviços constam do ANEXO I (17696592) - ESPECIFICAÇÕES MÍNIMAS E OBRIGATÓRIAS.

2. **DO OBJETIVO:**

2.1. A contratação objeto deste Termo visa suprir as necessidades do PRODERJ e demais órgãos da Administração Pública, com a aquisição de ativos de rede, considerados essenciais para execução das atividades institucionais dos órgãos e cuja ausência ou indisponibilidade, mesmo que temporária, produzirá um impacto direto no dinamismo corporativo e nos serviços prestados.

2.2. A aquisição desta nova solução prevê atingir os seguintes objetivos específicos:

- Concentrar de forma redundante todo tráfego de diversos sites e andares, garantindo alta disponibilidade para todos as redes.
- Uma estrutura de Switches divididos em Núcleo, Distribuição a Acesso;
- Integrar dados, voz e imagens através da mesma rede, com segurança e performance adequados;
- Prover rede WiFi de alto desempenho para dispositivos moveis;
- Integrar todos os sites e servidores através de redes de fibra ótica de alta velocidade e baixa latência;
- Prover alta disponibilidade para a rede do data center, possibilitando total aproveitamento dos recursos adquiridos;
- Prover um ambiente de rede controlado e monitorado;

3. **DA JUSTIFICATIVA:**

3.1. O atendimento das necessidades do PRODERJ e demais órgãos da Administração Pública quanto aos serviços de TIC requer uma dinâmica aprimorada e confiável, capaz de atender a sazonalidade dos serviços prestados ao cidadão. Nesse sentido, várias ações estão sendo tomadas, porém, algumas das necessidades passam obrigatoriamente pela disponibilidade, qualidade e integridade dos serviços oferecidos. Analisando o crescimento da informatização dos serviços de TIC oferecidos à Adminsitração, cada vez mais se percebe a necessidade de aprimoramento e ampliação de conectividade à Internet e aos sistemas internos de processamento de dados.

3.2. Os Ativos de Redes compõem a infraestrutura necessária para a acesso com e/ou sem fio, que permite que dispositivos se conectem à rede LAN corporativa. Desta forma, o presente estudo visa encontrar a melhor solução para aquisição de ativos de rede contemplando os seguintes equipamentos:

- Switches Core
- Switches de Distribuição
- Switches de Acesso
- Controladora WLAN
- Plataforma de Gerenciamento dos Ativos de Rede
- Access Point WLAN
- Interfaces e Conversores

3.3. A Tecnologia da Informação e Comunicação tem adquirido ao longo das últimas décadas, e, principalmente, dos últimos anos, um papel estratégico para qualquer negócio (público ou privado). Enquanto órgão público, os investimentos em atualizações constantes de TIC deixaram de ser uma opção, para serem mandatórios e estratégicos, pois o uso da TIC passou a ser um distinguidor para a eficiência na gestão e atendimento das necessidades dos cidadãos.

3.4. O PRODERJ, para a concretização de suas atribuições, como representante do nível de Direção Geral do Sistema Estadual de Tecnologia da Informação e Comunicação – SETIC, tem dentre seus objetivos precípuos planejar com inteligência as ações na área de Tecnologia da Informação e Comunicação, alinhando redução de custos com a garantia de maior eficiência para gestão e, por consequência, o atendimento às expectativas da população.

3.5. Diante de tal quadro, aliado à realidade econômica que impõe uma gestão enxuta de recursos públicos para investimento e atualização tecnológica de imediato, destina-se o presente processo à opção de aquisição de soluções de TIC. De forma sucinta, a contratação pleiteada vai gerar os seguintes benefícios:

- Fornecer garantia e assistência técnica por 60 meses;
- Atualizar o parque tecnológico;
- Manter alta disponibilidade dos equipamentos e atualização de versão do software;
- Aumentar a segurança dos dados;
- Reduzir o tempo de resposta às demandas dos usuários;

3.6. Entretanto, o parque de equipamentos que forma a rede de computadores na Adminstração Pública está, em sua maior parte, descontinuada pelos fabricantes e na sua totalidade sem contrato de manutenção e de garantia de funcionamento, o que coloca em risco a continuidade dos serviços de TI disponibilizados pelos órgãos, bem como os serviços prestados pelos mesmos.

3.7. A falta ou indisponibilidade destes recursos, prejudica a continuidade operacional das áreas e gera atrasos na entrega dos projetos de negócio. A inflexibilidade destes recursos certamente traria prejuízos à execução dos serviços administrativos da Administração como um todo, situação que acarretaria transtornos aos cidadãos.

3.8. No presente contexto, convém citarmos o princípio da economicidade cuja meta é a obtenção da melhor relação custo-benefício possível que uma alocação de recursos financeiros, econômicos ou patrimoniais possa alcançar, bem como o princípio da eficiência, que exige o aperfeiçoamento dos serviços e atividades, em busca de melhores resultados e do atendimento ao interesse público com ênfase em maiores índices de adequação, eficácia e satisfação.

3.9. A aquisição dos novos ativos de rede visa assegurar a continuidade da comunicação de dados entre os ativos de tecnologia do PRODERJ e demais órgãos da Administração Pública. Os equipamentos atuais que desempenham tais funções encontram-se em processo de descontinuação do serviço de suporte pelos fabricantes. A qualidade e disponibilidade da rede interna de dados do Estado

serão significativamente comprometidas caso não haja a renovação dos equipamentos de comunicação do núcleo da rede, distribuição e acesso.

3.10. Assim posto, a presente demanda, culmina na necessidade de contratação de pessoa jurídica de direto privado especializada no segmento de redes corporativas para o fornecimento de solução de ativos de rede de comunicação de dados, incluindo instalação, capacitação técnica, garantia e suporte.

3.11. Ademais, cabe ao PRODERJ a realização de compras coletivas, por meio de Registro de Preços para a contratação de bens e serviços relativos à tecnologia da informação e comunicação no Governo do Estado, conforme prevê o §2º do art. 4º do Decreto 46.751/2019.

4. JUSTIFICATIVA PARA O NÃO PARCELAMENTO DO OBJETO

4.1. Todos os equipamentos possuem correlação técnica entre si, pois todos se baseiam de forma macro na tecnologia de ativos de rede do tipo switches Ethernet, com o objetivo de criar uma única solução de infraestrutura de rede de computadores, desde a camada de acesso a rede até os switches que formam a infraestrutura de Datacenter.

4.2. O lote único agrupa todos os itens que possuem o objetivo principal de prover os meios necessários para a implantação de uma solução de infraestrutura de ativos de rede, incluindo switches da camada de acesso, core de rede local, interfaces e cabos necessários a interconexão dos equipamentos. Para toda e qualquer solução ofertada faz necessário a capacitação técnica da CONTRATANTE para que através do conhecimento possa extrair a melhor relação custo benefício da solução adquirida.

4.3. Destaca-se ainda que a licitação por grupo único é mais satisfatória do ponto de vista da eficiência técnica, por manter uma maior qualidade do fornecimento, haja vista que o gerenciamento permanece todo o tempo a uma mesma empresa, além de garantir a compatibilidade dos ativos, fato importante quando se mantém diversos serviços e softwares trafegando na rede, a maior interação entre as diferentes fases do fornecimento, a maior facilidade no cumprimento do cronograma e na observância dos prazos, concentração da responsabilidade pela execução do fornecimento em uma só pessoa jurídica e concentração da garantia dos resultados.

4.4. O fato de utilizarmos uma compra em lote de um mesmo fabricante, irá gerar um quantitativo maior para o fornecedor, disponibilizando uma Economicidade para o Estado.

4.5. A utilização de uma única plataforma de gerenciamento, em uma conttratação não parcelada também irá gerar uma Economicidade pelo fato de não necessitar de múltiplas plataformas em uma eventual contratação parcelada do objeto.

4.6. A Administração Pública, não pode restringir em demasia o objeto do contrato sob pena de frustrar a competitividade, por outro, ela não pode definir o objeto de forma excessivamente ampla, haja vista que, nesse caso, os critérios para julgamento das propostas falecem, em virtude da própria administração admitir propostas díspares, inclusive as que não satisfazem ao interesse público e não atendem a necessidade da Administração.

4.7. Portanto, a definição do objeto da licitação pública e as suas especificidades são eminentemente discricionárias, a qual compete ao agente administrativo avaliar o que o interesse público demanda obter mediante a aquisição.

4.8. Cumpre ponderar que, ao decidir pelo procedimento do julgamento das propostas em licitações, cujos objetos constituem-se bens divisíveis, que podem ser apartados em itens, bem como diversos itens podem ser agrupados num único lote, a Administração lançando-se do poder discricionário que tem, definiu que para o certame objetivado houvesse um vencedor para o lote, contendo os itens agrupados, não descurando do interesse público, que demanda ser otimizado.

4.9. A rigor, o agrupamento de vários itens em um mesmo lote não compromete a competitividade do certame, desde que várias empresas, que atuam no mercado, apresentem condições e aptidão para cotar todos os itens, principalmente levando-se em consideração a modalidade adotada, em que os recursos de tecnologia de informação têm como principal vantagem, aproximar pessoas, encurtar distâncias, resultando em considerável ampliação da competitividade, gerando, consequentemente, inúmeras repercussões positivas num processo de licitação pública, dentre estas, a de aumentar a probabilidade de a Administração Pública firmar contrato mais vantajoso, haja vista que ela recebe mais propostas, beneficiando a eficiência em contratos administrativos.

4.10. A própria Lei Federal n.º 8.666/93 garante a possibilidade de utilizar o menor valor global como critério, nos seguintes termos:

> "Art. 40. O edital conterá no preâmbulo o número de ordem em série anual, o nome da repartição interessada e de seu setor, a modalidade, o regime de execução e o tipo da licitação, a menção de que será regida por esta Lei, o local, dia e hora para recebimento da documentação e proposta, bem como para início da abertura dos envelopes, e indicará, obrigatoriamente, o seguinte:
>
> (...)
>
> VII - critério para julgamento, com disposições claras e parâmetros objetivos;
>
> (...)
>
> X - **o critério de aceitabilidade dos preços unitário e global, conforme o caso**, permitida a fixação de preços máximos e vedados a fixação de preços mínimos, critérios estatísticos ou faixas de variação em relação a preços de referência, ressalvado o disposto nos parágrafos 1º e 2º do art . 48". (Grifo nosso)

4.11. Corroborando o entendimento supramencionado, o Tribunal de Contas da União decidiu pelo indeferimento de pedido de divisão do objeto licitado em itens, por considerar que a reunião do objeto em um único item, desde que devidamente justificada pela área demandante ou pelo pregoeiro, afasta a possibilidade de restrição indevida à competitividade. (Acórdão 1.167/2012 – TC 000.431/2012-5 – TCU – Plenário – Relator: José Jorge).

4.12. Essa mesma Corte se pronunciou ainda através do Acórdão nº 732/2008, no seguinte sentido:

> " ...a questão da viabilidade do fracionamento deve ser decidida com base em cada caso, pois cada obra tem as suas especificidades, devendo o gestor decidir analisando qual a solução mais adequada no caso concreto".

4.13. Dessa forma, verifica-se que o entendimento do Tribunal de Contas tem sido o de que a divisão do objeto em itens distintos deve ser auferida sempre no caso concreto, devendo ser aplicada a opção mais vantajosa para a Administração Pública, desde que não haja restrição à competitividade e que em caso de agrupamento, este último esteja devidamente justificado.

4.14. Este mesmo tribunal publicou a Súmula nº 247 do TCU, que estabeleceu que:

> "É obrigatória a admissão da adjudicação por item e não por preço global, nos editais das licitações para a contratação de obras, serviços, compras e alienações, cujo objeto seja divisível, **desde que não haja prejuízo para o conjunto ou complexo ou perda de economia de escala**, tendo em vista o objetivo de propiciar a ampla participação de licitantes que, embora não dispondo de capacidade para a execução, fornecimento ou aquisição da totalidade do objeto, possam fazê-lo com relação a itens ou unidades autônomas, devendo as exigências de habilitação adequar-se a essa divisibilidade". (Grifo nosso)

4.15. Percebe-se que mesmo quando houve o entendimento do TCU que é obrigatório a admissão da adjudicação por item e não por preço global, esta adjudicação por item só pode ocorrer se não causar prejuízo ao conjunto e se não causar perda de economia de escala.

4.16. O TCU, em outra matéria, já teve a oportunidade de se manifestar no sentido de que, no caso específico, a licitação por lote único seria a mais eficiente à administração:

> "Cabe considerar, porém, que o modelo para a contratação parcelada adotado nesse parecer utilizou uma excessiva pulverização dos serviços. Para cada um de cinco prédios, previram-se vários contratos (ar condicionado, instalações elétricas e eletrônicas, instalações hidrossanitárias, civil). Esta exagerada divisão de objeto pode maximizar a influência de fatores que contribuem para tornar mais dispendiosa a contratação (...) embora as estimativas numéricas não mostrem consistência, não há nos autos nenhuma evidência no sentido oposto, de que o parcelamento seria mais vantajoso para a Administração. Ao contrário, os indícios são coincidentes em considerar a licitação global mais econômica" (Acórdão nº 3140/2006 do TCU).

4.17. Portanto, ao se licitar por lote único, deve o administrador analisar a viabilidade técnica e econômica de dividir-se o objeto licitatório, pois segundo Justen Filho, *"a obrigatoriedade do fracionamento respeita limites de ordem técnica e econômica. Não se admite o fracionamento quando tecnicamente isso não for viável ou, mesmo, recomendável. O fracionamento em lotes deve respeitar a integridade qualitativa do objeto a ser executado. (...) a unidade do objeto a ser executado não pode ser destruída através do fracionamento"*.

4.18. Esclarece-nos Carvalho Carneiro acerca do conceito de viabilidade técnica e econômica, informando que: *"a viabilidade técnica diz respeito à integridade do objeto, não se admitindo o parcelamento quando tal medida implicar na sua desnaturação, onde em risco a satisfação do interesse público em questão. Já a viabilidade econômica significa que o parcelamento deve trazer benefícios para a Administração licitante, proporcionando um aumento da competitividade e uma consequente diminuição dos custos para a execução do objeto. No entanto, para uma real noção da viabilidade econômica do parcelamento, é preciso ter em mente a redução de custos proporcionada pela economia de escala".*

4.19. Sobre o tema, vale ainda citar a obra "Temas Polêmicos sobre Licitações e Contratos", vários autores, da editora Malheiros, na página 74,o seguinte trecho: *"(...) em geral, a economia de escala é instrumento fundamental para diminuição de custos. Quanto maior a quantidade a ser negociada, menor o custo unitário, que em decorrência do barateamento do custo da produção (economia de escala na indústria), quer porque há diminuição da margem de lucro (economia de escala geralmente encontrada no comércio)".*

4.20. Este agrupamento encontra guarita ainda em deliberações do TCU sobre a matéria, tais como a decisão que "A aquisição de itens diversos em lotes *deve estar respaldada em critérios justificantes", adotando o entendimento do acórdão 5260/2011, de 06/07/2011, que decidiu que "Inexiste ilegalidade na realização de pregão com previsão de adjudicação por lotes, e não por itens, desde que os lotes sejam integrados por itens de uma mesma natureza e que guardem correlação entre si "*.

4.21. Assim posto, o agrupamento dos itens em lote único levou em consideração questões técnicas, bem como o ganho de economia em escala, sem prejuízo a ampla competividade, uma vez que existe no mercado várias empresas com capacidade de fornecer os produtos e serviços na forma em que estão agrupados neste ETP.

5. DA MODALIDADE DE LICITAÇÃO:

5.1. O objeto do presente Termo de Referência encontra-se dentro da classificação de fornecimento de produtos e serviços comuns, tendo em vista que são equipamentos que compõem a infraestrutura necessária que permite a conexão de dispositivos à rede de dados corporativa.

5.2. Desta forma, o presente estudo visa encontrar a melhor solução para aquisição de ativos de rede em razão de suas características, quantidades e qualidades, que são passíveis de especificações usuais no mercado, em todo o País. Desta forma, a escolha da modalidade de Pregão Eletrônico pelo **MENOR PREÇO GLOBAL.**

5.3. Ademais, os padrões de desempenho e qualidade estão objetivamente definidos no bojo deste Termo de Referência, por meio de especificações e caraterísticas usuais praticadas no mercado nacional, permitindo a qualquer dos interessados formular proposta de preço, a fim de atender às exigências estabelecidas.

6. DO REGISTRO DE PREÇOS:

6.1. O Governo do Estado do Rio de Janeiro, como toda grande organização, tem gastos volumosos com produtos e serviços de Tecnologia da Informação e Comunicação (TIC) entre os órgãos que o compõe. Os crescentes desafios colocados para o governo acabam induzindo o aumento da máquina administrativa e, consequentemente, dos gastos com seus serviços.

6.2. Parte significativa desses dispêndios pode ser reduzida com processos de contratações eficientes, planejados previamente em conjunto por grupos de Órgãos. Além de melhorar a qualidade técnica dos artefatos de contratação, um planejamento integrado de contratação reduz a duplicidade de esforços entre os órgãos e otimiza o trabalho dos técnicos das áreas de licitações e contratos, ensejando ainda economia processual.

6.3. O grande benefício, entretanto, advém da utilização do poder de compra do governo. Na medida em que aproveita as oportunidades de economia de escala, a Administração Pública pode obter melhores preços junto ao mercado, reduzindo seus custos em benefício do atendimento às demandas sociais.

6.4. Esta é uma inteligência trazida pelo Sistema de Registro de Preços - SRP, utilizado sempre que conveniente à contratação de serviços para atendimento a vários Órgãos, que trabalham de forma integrada suas estimativas de consumo e os aspectos técnicos da contratação.

6.5. Cabe ressaltar que o PRODERJ é o Órgão do Governo do Estado competente para realizar Registro de Preços para a contratação de bens e serviços relativos à tecnologia da informação e comunicação, conforme prevê o §2º, art. 4º do Decreto 46.751/2019, que regulamenta o sistema de registro de preços no Estado do Rio de Janeiro.

> Além disso, o inciso X, art. 2º da Lei nº 4480/2004, dispõe que cabe ao PRODERJ: *"oferecer aos órgãos do Estado a possibilidade de aderir a contratos corporativos para suprir os principais itens relativos à Tecnologia da Informação e Comunicação, englobando licenças de software de uso geral (sistemas operacionais, de bancos de dados, de automação de escritórios, de segurança e de rede), linhas de comunicação de dados, estações de trabalho, servidores e terminais de autoatendimento para acesso à internet, tendo como objetivo a obtenção de ganhos de economia de escala para o Estado, além dos benefícios intrínsecos de padronização e integração."*

6.6. Em suma, elencamos cinco argumentos que justificam a adoção do Sistema de Registro de Preços:

I - Melhoria da qualidade técnica dos documentos preliminares ao certame, tais como: especificações técnicas, alinhamento estratégico com o planejamento dos órgãos e condições jurídicas para a contratação;

II - Redução do esforço administrativo para a realização de diversos processos licitatórios sendo que a execução conjunta culmina em um único certame;

III - Padronização do parque tecnológico na Administração Pública;

IV - Redução de custos de manutenção e melhor eficiência pelo uso racional dos recursos, uma vez que estes foram definidos de forma a atender precisamente as necessidades do usuário;

V - Ganho de economia de escala, pois, ao prospectar grandes volumes licitados, a Administração Pública amplia seu poder de compra junto aos fornecedores e consegue reduções consideráveis de preços, fato que certamente não ocorreria quando do fracionamento de certames.

6.7. Portanto, a utilização do Sistema de Registro de Preços será necessária neste certame, uma vez que atenderá as demandas do PRODERJ e demais órgãos da Administração Pública, podendo o quantitativo ora definido sofrer alterações.

6.8. Após a adjudicação e a homologação do resultado da licitação pela autoridade competente, será efetuado o registro de preços mediante Ata de Registro de Preços, a ser firmada entre a(s) licitante(s) vencedora(s) e o PRODERJ, com efeito de compromisso de fornecimento para futura contratação.

6.9. O prazo de vigência da Ata de Registro de Preços será de 12 (doze) meses, contados da sua assinatura e lançamento no sistema.

6.10. A existência de preços registrados não obriga a Administração a firmar as contratações que deles poderão advir, sem que caiba direito à indenização de qualquer espécie. Fica facultada a utilização de outros meios, respeitada a legislação pertinente às licitações e ao Sistema de Registro de Preços, assegurando-se ao beneficiário do registro preferência em igualdade de condições, de acordo com o Edital.

6.11. Não será admitido o recebimento de equipamento diferente daquele registrado na proposta de preços da licitante ou apostilado a Ata de Registro de Preços, ainda que em caráter de vantagem técnica, sem a observância dos procedimentos disciplinados na forma deste TR.

7. DA DOTAÇÃO ORÇAMENTÁRIA:

7.1. Conforme previsto no §2º do art. 10 do Decreto nº 46.751/2019, que regulamenta o Sistema de Registro de Preços no Estado do Rio de Janeiro, na licitação para registro de preços não é necessário indicar dotação orçamentária.

8. DA ENTREGA E CRITÉRIOS DE ACEITAÇÃO DO OBJETO

8.1. Todo e qualquer fornecimento se dará mediante demanda da CONTRATANTE, situação em que será emitida a OF - Ordem de Fornecimento, conforme ANEXO II (17696892) – MODELO DE ORDEM DE FORNECIMENTO.

8.2. Os serviços serão executados nos locais e endereços descritos nas OFs.

8.3. Os bens e/ou serviços que compõem a solução serão recebidos:

a) Provisoriamente, em até 15 (quinze) dias da data de entrega. Ao término deste recebimento será emitido o Termo de Recebimento Provisório, vide ANEXO III (17697476).

b) Definitivamente, no prazo de 30 (trinta) dias após a emissão do Termo de Recebimento Provisório. Ao término deste recebimento será emitido o Termo de Recebimento Definitivo, vide ANEXO IV (17697748).

8.4. A Administração rejeitará, no todo ou em parte, a entrega dos serviços em desacordo com as especificações técnicas exigidas.

8.5. ***Da Aceitação***

8.5.1. A recusa parcial ou total no atendimento de uma OF - Ordem de Fornecimento emitida, será oficiada à CONTRATADA pela CONTRATANTE, que deverá prontamente prestar o serviço de acordo com o estabelecido na respectiva OF;

8.5.2. A aceitação definitiva dar-se-á após a assinatura do termo de recebimento definitivo, correspondente a cada OF.

9. DO MODELO DE EXECUÇÃO DO CONTRATO

9.1. CONTRATADA deverá elaborar um plano de comunicação em conjunto com a CONTRATANTE de acordo com as seguintes diretrizes:

9.1.1. Disponibilizar um profissional responsável pelo relacionamento com a CONTRATANTE, definindo as formas de integração das equipes.

9.1.2. Prever reuniões, com periodicidade a ser definida pelas partes, para avaliação dos resultados e propor recomendações para a execução dos serviços.

9.1.3. Descrever o processo e os procedimentos para a troca de informações que utilize mecanismos formais de comunicação; tais como: e-mail, ata de reunião ou sistema de informação que contemple formas de registro e acompanhamento dos assuntos tratados nas reuniões periódicas.

9.1.4. A presente contratação seguirá o regime de EMPREITADA POR PREÇO GLOBAL, único lote, onde todos os serviços e produtos serão fornecidos por apenas uma empresa, gerando assim uma maior economia ao Estado, em razão do objeto compor uma única soluação.

10. DO MODELO DE GESTÃO DO CONTRATO

10.1. o CONTRATANTE será responsável pela gestão do contrato e pelo atesto quanto à aderência aos padrões de qualidade exigidos dos produtos e serviços entregues.

10.2. A CONTRATADA será responsável pela execução dos serviços e gestão dos recursos humanos, físicos e tecnológicos inerentes ao escopo da contratação.

10.3. Todos os produtos a serem entregues pela CONTRATADA serão solicitados mediante OF - Ordem de Fornecimento.

10.4. Todos os serviços a serem prestados pela CONTRATADA serão executados mediante OF - Ordem de Fornecimento.

11. ACORDO DE NÍVEL DE SERVIÇO:

11.1. Não se aplica, considerando que trata-se de certame licitatório para aquisição de equipamentos, com instalação, configuração, garantia e suporte on-site, o que diferencia de uma

contratação de empresa para prestação de serviços contínuos, onde estes são medidos a avaliados para fins de glosa.

11.2. Considerando que uma solução de TIC engloba todos os elementos (bens, serviços de TIC e automação) necessários que se integram para o alcance dos resultados pretendidos com a contratação, de modo a atender à necessidade que a desencadeou, pode-se afirmar que a contratação em questão compreende uma solução de tecnologia, uma vez que compreende uma solução integrada e indissolúvel, contemplando hardware, software e serviços de instalação, garantindo as melhores práticas do fabricante para a ativação dos equipamentos, em uma única infraestrutura computacional.

12. QUALIFICAÇÃO TÉCNICA:

12.1. Para fins de comprovação de qualificação técnica, deverá(ão) ser apresentado(s) o(s) atestado(s) fornecido(s) por pessoas jurídicas de direito público ou privado, que comprovem a aptidão de desempenho de atividade pertinente e compatível em características, quantidades e prazos com o objeto da licitação, na forma do artigo 30, § 4º, da Lei Federal nº 8.666/93 que indiquem nome, função, endereço e o telefax de contato do(s) atestador(es), ou qualquer outro meio para eventual contato pelo ÓRGÃO GERENCIADOR.

12.2. Em virtude do mecanismo de compras conjuntas ora adotado pelo PRODERJ e pela quantidade de fornecimento simultâneo a ser executado pelos diversos órgãos da Administração Pública, participantes do certame, exige-se o fornecimento de atestado de capacidade técnica referenciando um quantitativo mínimo de 50% do volume estimado para os lotes, a fim de garantir ao Estado a entrega dos equipamentos, tendo em vista a essencialidade desses bens e os riscos decorrentes da ausência deles para a Administração.

12.2.1. Admitir-se-á a soma de atestados de capacidade técnica para a comprovação do quantitativo especificado.

12.3. A Empresa deverá apresentar certidões negativas de falências e recuperação judicial e extrajudicial expedidas pelos distribuidores da sede da pessoa jurídica, ou de execução patrimonial, expedida no domicílio da pessoa física. Caso não seja sediado na Comarca da Capital do Estado do Rio de Janeiro, as certidões deverão vir acompanhadas de declaração oficial da autoridade judiciária competente, relacionando os distribuidores que, na Comarca de sua sede, tenham atribuição para expedir certidões negativas de falências e recuperação judicial, ou de execução patrimonial.

12.4. A Empresa deve também apresentar os seguintes documentos:

12.4.1. Balanço Patrimonial e Demonstrações Contábeis do último exercício social, desde que já exigíveis e apresentados na forma da lei, incluindo Termo de Abertura e Encerramento do livro contábil, que comprovem a boa situação financeira da empresa. Quando encerrados há mais de três meses da data da apresentação da proposta, admitir- se-á atualização de valores, por índices oficiais, sendo vedada a substituição das demonstrações financeiras por balancetes ou balanços provisórios.

13. PAGAMENTO:

13.1. Os pagamentos serão realizados pelo ÓRGÃO GERENCIADOR, ÓRGÃOS PARTICIPANTES e ÓRGÃOS ADERENTES, de acordo com as contratações realizadas por cada um deles.

13.2. O pagamento será realizado à vista, em até 10 (dez) dias úteis após o recebimento definitivo do objeto.

13.3. Os pagamentos serão efetuados, obrigatoriamente, por meio de crédito em conta corrente da instituição financeira contratada pelo Estado, cujo número e agência deverão ser informados pelo adjudicatário até a assinatura do contrato.

13.4. No caso de a CONTRATADA estar estabelecida em localidade que não possua agência da instituição financeira contratada pelo Estado ou caso verificada pelo CONTRATANTE a impossibilidade de a CONTRATADA, em razão de negativa expressa da instituição financeira contratada pelo Estado, abrir ou manter conta corrente naquela instituição financeira, o pagamento poderá ser feito mediante

crédito em conta corrente de outra instituição financeira. Nesse caso, eventuais ônus financeiros e/ou contratuais adicionais serão suportados exclusivamente pela CONTRATADA.

13.5. O contratado deverá emitir Nota Fiscal Eletrônica – NF-e, consoante o Protocolo ICMS nº 42/2009, com a redação conferida pelo Protocolo ICMS nº 85/2010, e caso seu estabelecimento esteja localizado no Estado do Rio de Janeiro, deverá observar a forma prescrita nas alíneas a, b, c, d, e, do §1º, do art. 2º, da Resolução SEFAZ nº 971/2016.

14. GARANTIA CONTRATUAL:

14.1. Exigir-se-á do fornecedor, no prazo máximo de 10 (dez) dias, contado da data da assinatura do contrato, uma garantia, a ser prestada em qualquer modalidade prevista pelo § 1º, art. 56 da Lei n.º 8.666/93, da ordem de 5 % (cinco por cento) do valor do contrato, a ser restituída após sua execução satisfatória.

14.2. A garantia, qualquer que seja a modalidade apresentada pelo vencedor do certame, deverá contemplar a cobertura para os seguintes eventos:

a) prejuízos advindos do não cumprimento do contrato;

b) multas punitivas aplicadas pela fiscalização à contratada;

c) prejuízos diretos causados à CONTRATANTE decorrentes de culpa ou dolo durante a execução do contrato;

d) obrigações previdenciárias e trabalhistas não honradas pela CONTRATADA.

14.3. A garantia prestada não poderá se vincular a outras contratações, salvo após sua liberação.

14.4. Nos casos em que valores de multa venham a ser descontados da garantia, seu valor original será recomposto no prazo de 48 (quarenta e oito) horas, sob pena de rescisão administrativa do contrato.

15. PROCEDIMENTOS DE GESTÃO E FISCALIZAÇÃO:

15.1. O acompanhamento e a fiscalização da execução do Contrato serão exercidos por meio de uma equipe de fiscalização de servidores da CONTRATANTE, devidamente designados e credenciados pelo Órgão, independentemente de qualquer outra supervisão, assistência ou assessoramento, a seu exclusivo juízo.

15.2. O acompanhamento e a fiscalização da execução do contrato consistem na verificação da conformidade da prestação dos serviços, dos materiais, técnicas e equipamentos empregados, de forma a assegurar o perfeito cumprimento do ajuste, que serão exercidos por um ou mais representantes da Contratante, especialmente designados, na forma dos arts. 67 e 73 da Lei nº 8.666, de 1993.

15.3. O representante da Contratante deverá ter a qualificação necessária para o acompanhamento e controle da execução do objeto e do contrato.

15.4. O descumprimento total ou parcial das obrigações e responsabilidades assumidas pela Contratada, sobretudo quanto às obrigações e encargos sociais e trabalhistas, ensejará a aplicação de sanções administrativas, previstas neste Termo de Referência e na legislação vigente, podendo culminar em rescisão contratual, conforme disposto nos artigos 77 e 87 da Lei nº 8.666, de 1993.

15.5. As atividades de gestão e fiscalização da execução contratual devem ser realizadas de forma preventiva, rotineira e sistemática, podendo ser exercidas por servidores, equipe de fiscalização ou único servidor, desde que, no exercício dessas atribuições, fique assegurada a distinção dessas atividades e, em razão do volume de trabalho, não comprometa o desempenho de todas as ações relacionadas à Gestão do Contrato.

15.6. O fiscal técnico deverá apresentar ao preposto da CONTRATADA a avaliação da execução do objeto ou, se for o caso, a avaliação de desempenho e qualidade da prestação dos serviços realizada.

15.7. A fiscalização de que trata esta cláusula não exclui nem reduz a responsabilidade da CONTRATADA, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios, ou emprego de material inadequado ou de qualidade inferior e,

na ocorrência desta, não implica corresponsabilidade da CONTRATANTE ou de seus agentes, gestores e fiscais, de conformidade com o art. 70 da Lei nº 8.666, de 1993.

16. DAS OBRIGAÇÕES DA CONTRATANTE:

16.1. Exigir o cumprimento de todas as obrigações assumidas pela Contratada, de acordo com as cláusulas contratuais e os termos de sua proposta;

16.2. Nomear Gestor do Contrato, assim como Fiscais Técnico e Requisitante para acompanhar e fiscalizar a execução dos contratos;

16.3. Exercer o acompanhamento e a fiscalização dos serviços, por servidor especialmente designado, anotando em registro próprio as falhas detectadas, indicando dia, mês e ano, bem como o nome dos empregados eventualmente envolvidos, e encaminhando os apontamentos à autoridade competente para as providências cabíveis;

16.4. Notificar a Contratada por escrito da ocorrência de eventuais imperfeições, falhas ou irregularidades constatadas no curso da execução dos serviços, fixando prazo para a sua correção, certificando-se que as soluções por ela propostas sejam as mais adequadas;

16.5. Pagar à Contratada o valor do obejto, no prazo e condições estabelecidas neste Termo de Referência;

16.6. Efetuar as retenções tributárias devidas sobre o valor da Nota Fiscal/Fatura da contratada, no que couber;

16.7. Não praticar atos de ingerência na administração da Contratada, tais como:

a) exercer o poder de mando sobre os empregados da Contratada, devendo reportar-se somente aos prepostos ou responsáveis por ela indicados, exceto quando o objeto da contratação previr o atendimento direto, tais como nos serviços de recepção e apoio ao usuário;

b) direcionar a contratação de pessoas para trabalhar nas empresas Contratadas;

c) considerar os trabalhadores da Contratada como colaboradores eventuais do próprio órgão ou entidade responsável pela contratação, especialmente para efeito de concessão de diárias e passagens.

16.8. Fornecer por escrito as informações necessárias para execução do objeto do contrato.

17. DAS OBRIGAÇÕES DA CONTRATADA:

17.1. Indicar formalmente, caso necessário, preposto apto a representá-la junto à CONTRATANTE, que deverá responder pela fiel execução do contrato;

17.2. Executar os serviços, quando for o caso, conforme especificações deste Termo de Referência e de sua proposta, com a alocação dos empregados necessários ao perfeito cumprimento das cláusulas contratuais, além de fornecer e utilizar os materiais e equipamentos, ferramentas e utensílios necessários, na qualidade e quantidade mínimas especificadas neste Termo de Referência e em sua proposta;

17.3. Reparar, corrigir, remover ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os serviços, caso tenham sido efetuados, em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;

17.4. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, bem como por todo e qualquer dano causado ao Órgão ou Governo do Estado, devendo ressarcir imediatamente a Administração em sua integralidade, ficando a Contratante autorizada a descontar da garantia, caso exigida no edital, ou dos pagamentos devidos à Contratada, o valor correspondente aos danos sofridos;

17.5. Vedar a utilização de empregado que seja familiar de agente público ocupante de cargo em comissão ou função de confiança no órgão Contratante, nos termos do artigo 7° do Decreto n° 7.203, de 2010;

17.6. Responsabilizar-se pelo cumprimento das obrigações previstas em Acordo, Convenção, Dissídio Coletivo de Trabalho ou equivalentes das categorias abrangidas pelo contrato, por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas em legislação específica, cuja inadimplência não transfere a responsabilidade à Contratante;

17.7. Prestar todo esclarecimento ou informação solicitada pela Contratante ou por seus prepostos, quando presente, garantindo-lhes o acesso, a qualquer tempo, ao local dos trabalhos, bem como aos documentos relativos à execução do empreendimento;

17.8. Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;

17.9. Cumprir, durante todo o período de execução do contrato, a reserva de cargos prevista em lei para pessoa com deficiência ou para reabilitado da Previdência Social, bem como as regras de acessibilidade previstas na legislação, quando a contratada houver se beneficiado da preferência estabelecida pela Lei nº 13.146, de 2015.

17.10. Manter sigilo, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto de interesse do CONTRATANTE ou de terceiros de que tomar conhecimento em razão da execução do objeto, devendo assinar Termo de Confidencialidade, cujo modelo está no ANEXO V (17698140) e orientar seus empregados nesse sentido.

17.11. Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, tais como os valores providos com o quantitativo de vale transporte, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto da licitação, exceto quando ocorrer algum dos eventos arrolados nos incisos do § 1º do art. 57 da Lei nº 8.666, de 1993.

18. DA PROPOSTA DE PREÇO:

18.1. A proposta de preço ajustada ao valor do lance da LICITANTE deverá seguir a forma definida neste Termo de Referência e no Edital, devendo conter os seguintes termos:

a) Os termos de prestação da garantia estipulados para cada ITEM;

b) Concordar com todos os termos e condições estabelecidas neste Termo de Referência, incluindo as obrigações da contratante, de entrega, e demonstrar estar ciente das sanções administrativas por descumprimento das demais cláusulas deste Termo de Referência e no Edital.

18.2. Apresentação dos demonstrativos de Preço Total e de Preços Unitários, na forma do ANEXO VI (17698806). Deverá ser anexada descrição do(s) produto(s) com os serviço(s) inclusos que será(ão) fornecido(s).

18.3. O valor apresentado deverá contemplar todos os custos inerentes a contratação e ainda aqueles decorrentes de fretes, seguros, embalagens, fiscais, trabalhistas e demais encargos de contribuições, impostos e taxas estabelecidos na forma da Lei.

18.4. Foram solicitados aos fabricantes líderes e visionários do quadrante mágico 2020 do Gartnet para a categoria de infraestrutura de acesso a LAN com e sem fio (Ativos de Rede), os envios de estimativas orçamentárias dos valores unitários dos ítens listados. O Proderj recebeu 03 estimativas orçamentárias através dos parceiros integradores indicados pelos fabricantes.

19. SUBCONTRATAÇÃO, PARTICIPAÇÃO DE CONSÓRCIO OU COOPERATIVA:

19.1. É vedada a subcontratação total ou parcial do objeto, tendo em vista que no fornecimento dos componentes em cada item, o objeto é único, ou seja, a licitante tem condição de ofertar sem necessidade de subcontratação

19.2. Não será permitida a participação de empresas que estiverem reunidas em consórcio, assim como não será permitida a participação de cooperativas, qualquer que seja sua forma de constituição,

dadas as características específicas dos bens que serão fornecidos, que não pressupõem multiplicidade de atividades empresariais distintas (heterogeneidade de atividades empresariais).

19.3. A ausência de consórcio ou cooperativas não trará prejuízos à competitividade do certame, visto que, em regra, a formação de consórcios 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. Nestes casos, a Administração, com vistas a aumentar o número de participantes, admite a formação de consórcio.

19.4. Tendo em vista que é prerrogativa do Poder Público, na condição de contratante, a escolha da participação, ou não, de empresas constituídas sob a forma de consórcio, com as devidas justificativas, conforme se depreende da literalidade do texto da Lei n o 8.666/93, que em seu artigo 33 que atribui à Administração a prerrogativa de admissão de consórcios em licitações por ela promovidas, pelos motivos já expostos, conclui-se que a vedação de constituição de empresas em consórcio, para o caso concreto, é o que melhor atende o interesse público, por prestigiar os princípios da competitividade, economicidade e moralidade.

19.5. Ademais, essa vedação visa exatamente afastar a restrição à competição, na medida que a reunião de empresas que, individualmente, poderiam prestar os serviços, reduziria o número de licitantes e poderia, eventualmente, proporcionar a formação de conluios/carteis para manipular os preços nas licitações.

20. VIGÊNCIA DO CONTRATO:

20.1. O prazo de vigência do contrato será de 12 (doze) meses, a contar da data da assinatura do contrato.

20.2. Por se tratar de processo de aquisição integrada de hardware, software e serviços de instalação, suporte e garantia de 60 (sessenta) meses, não haverá hipótese de renovação do contrato, considerando-se a obsolescência programada no mercado de tecnologia.

20.3. A CONTRATADA deverá sujeitar-se aos acréscimos e supressões contratuais estabelecidos na forma do Art. 65 da Lei nº 8.666/93.

21. REAJUSTE:

21.1. Os contratos gerados à partir da Ata de Registro de Preços deste certame não sofrerão reajuste, exceto nos casos previstos no art. 18, do Decreto nº 7.892 de 23 de Janeiro de 2013 e nos art. 21 e art. 22, do Decreto 46.751/2019, para a renegociação de preços junto aos fornecedores registrados, nos casos em que os preços praticados na Ata de Registro de Preços se tornarem superiores aos preços de mercado.

22. ANEXOS DO TERMO DE REFERÊNCIA

22.1. São partes integrantes deste Termo de Referência os seguintes Anexos:

I - ESPECIFICAÇÕES MÍNIMAS E OBRIGATÓRIAS (17696592).

II - MODELO DE ORDEM DE FORNECIMENTO (17696892).

III - TERMO DE RECEBIMENTO PROVISÓRIO (17697476).

IV - TERMO DE RECEBIMENTO DEFINITIVO (17697748).

V - MODELO DE TERMO DE COMPROMISSO E SIGILO (17698140).

VI - PLANILHA DE COMPOSIÇÃO DE LANCES (17698806).

23. IDENTIFICAÇÃO DOS RESPONSÁVEIS

ELIO THOMÉ DE SOUZA FILHO

Gerente de Redes e Telecomunicacoes

ID Funcional: 0043475078

DANIEL LUZENTE DE LIMA

Diretor de Insfraestrutura Tecnológica

ID Funcional: 0043498850

Rio de Janeiro, 31 de Maio de 2021.

Documento assinado eletronicamente por **Elio Thomé de Souza Filho**, **Analista de Sistemas**, em 31/05/2021, às 17:32, conforme horário oficial de Brasília, com fundamento nos art. 21º e 22º do Decreto nº 46.730, de 9 de agosto de 2019.

Documento assinado eletronicamente por **Daniel Luzente de Lima**, **Diretor**, em 31/05/2021, às 17:32, conforme horário oficial de Brasília, com fundamento nos art. 21º e 22º do Decreto nº 46.730, de 9 de agosto de 2019.

A autenticidade deste documento pode ser conferida no site http://sei.fazenda.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **17694552** e o código CRC **69B80C57**.

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

Governo do Estado do Rio de Janeiro

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

Vice Presidência de Tecnologia

ANEXO I

ESPECIFICAÇÕES MÍNIMAS E OBRIGATÓRIAS

1. SWITCH CORE

Interfaces:

- Cada equipamento deve suportar, no mínimo, 40 (quarenta) portas 100 GbE (QSFP28) sem bloqueio (non-blocking);
- Cada equipamento deve suportar, no mínimo, 90 (noventa) portas 40 GbE (QSFP+) sem bloqueio (non-blocking);
- Cada equipamento deve suportar, no mínimo, 192 (cento e noventa e dois) portas 1/5/10 GbE (SFP/SFP+) sem bloqueio (non-blocking);
- Possuir porta de console para gerenciamento e configuração via linha de comando. O conector deve ser RJ-45 ou padrão RS-232 (os cabos e eventuais adaptadores necessários para acesso à porta de console devem ser fornecidos);
- Deve possuir no mínimo 1 (uma) porta Ethernet RJ-45 para administração fora de banda (out-of-band management).

Dimensões:

- Permitir ser montado em rack padrão de 19 (dezenove) polegadas, incluindo todos os acessórios necessários.
- Deve possuir no máximo 9 (nove) Rack Unit (RU).

Visualização:

- Possuir LEDs para a indicação do status das portas;
- Possuir LEDs do tipo blue beacon para identificação do switch ou porta a ser acessada, para facilitar a manutenção.

Capacidade e Desempenho:

- Possuir matriz de comutação com capacidade de, pelo menos, 9000 Gbps (Gigabits por segundo);
- Possuir capacidade de processamento de, pelo menos, 3000 Mpps (milhões de pacotes por segundo);
- Possuir capacidade de, no mínimo, 120.000 (cento e vinte mil) endereços MAC;
- Suporte a Jumbo Frames de, no mínimo, 9198 bytes em todas as suas portas;
- Ser fornecido com configuração de CPU e memória (RAM e Flash) suficiente para implementação de todas as funcionalidades descritas nesta especificação.

Fontes de Alimentação:

- Possuir fontes de alimentação redundantes simétricas internas ao equipamento, sendo que cada fonte deverá possuir potência suficiente para manter o equipamento em pleno funcionamento em sua capacidade máxima, ou seja, com todas as portas ocupadas;
- Possuir fontes de alimentação que operem de 100V a 220V com frequência de 50Hz a 60Hz;
- Os cabos de energia deverão ser fornecidos no padrão brasileiro (NBR 14.136);
- As fontes e as unidades de ventilação devem ser capazes de serem trocadas com o equipamento em pleno funcionamento, sem nenhum impacto na performance (hot-swappable).

Alta Disponibilidade:

- Suportar Non-Stop Forwarding e Stateful Switchover (NSF/SSO);
- Suportar upgrade de software em serviço (In Service Software Upgrade – ISSU);
- Deve prover total redundância com outros equipamentos da mesma marca e modelo, devendo atender uma das seguintes formas de alta disponibilidade:

1. Formar um virtual switch, de forma que os dois possam ser vistos como uma entidade única, logicamente. Esta funcionalidade pode ser provida através de:
2. Tecnologias do tipo Virtual ou Multi-Chassis;
3. Tecnologias de Stacking (físico ou virtual), garantindo que a pilha continue a funcionar na eventual falha de um dispositivo, sendo a pilha gerenciada como uma entidade única;
4. Tecnologias do tipo Multi-LAG (Multi Link Aggregation) permitindo a redundância de link's entre switches distintos.
5. Em caso de empilhamento ou Multi-LAG, deverão ser fornecidos todos os componentes necessários para garantia da alta disponibilidade, incluindo todos os módulos e/ou cabos/transceivers para interconexão dos equipamentos, bem como as licenças necessárias, caso aplicável;

- Cada switch deve ser fornecido com fontes e ventiladores redundantes e hot-swappable;
- Possuir fontes de alimentação redundantes que operem no modo N+1 ou N+N de forma a garantir o pleno funcionamento do equipamento conforme configuração solicitada, em caso de falha de pelo menos uma das fontes de alimentação.

Funcionalidades de Camada 2:

- Implementar até 4.000 VLAN IDs simultâneas conforme definições do padrão IEEE 802.1Q;
- Deve suportar VLANs dinâmicas. Deve permitir a criação, remoção e distribuição de VLANs de forma dinâmica através de portas configuradas como tronco IEEE 802.1Q;
- Implementar "VLAN Trunking" conforme padrão IEEE 802.1Q nas portas Fast Ethernet e Gigabit Ethernet. Deve ser possível estabelecer quais VLANs serão permitidas em cada um dos troncos 802.1Q configurados;
- Deve implementar Private VLANs;
- Implementar a funcionalidade de "Link Aggregation" (LAGs) conforme padrão IEEE 802.3ad, com no mínimo 8 (oito) portas por LAG (IEEE 802.3ad);
- Deve implementar o padrão IEEE 802.1d ("Spanning Tree Protocol"), IEEE 802.1s ("Multiple Spanning Tree") e IEEE 802.1w ("Rapid Spanning Tree");
- Deve implementar no mínimo 64 (sessenta e quatro) múltiplas Instâncias de Spanning Tree;
- Implementar mecanismo de proteção da "root bridge" do algoritmo Spanning-Tree para prover defesa contra ataques do tipo "Denial of Service" no ambiente de camada 2;
- Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo "fast forwarding" (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente;

- Deve implementar o protocolo IEEE 802.1AB Link Layer Discovery Protocol (LLDP), permitindo a descoberta dos elementos de rede vizinhos;
- Deve suportar exportação de fluxos (IPFIX ou Netflow) para análise do tráfego da rede;
- Deverá ter contadores de entrada e saída de pacotes por porta;
- Deverá suportar NTP.

Funcionalidades de Camada 3:

- Possuir roteamento nível 3 entre VLANs;
- Suportar roteamento de pacotes IPv4 e IPv6;
- Suporte a, pelo menos, 250.000 (duzentos e cinquenta mil) rotas IPv4 dinâmicas;
- Suporte a, pelo menos, 250.000 (duzentos e cinquenta mil) rotas IPv6 dinâmicas;
- Implementar roteamento estático e dinâmico;
- Implementar protocolo de roteamento dinâmico OSPF v2 e v3;
- Implementar protocolo de roteamento dinâmico BGPv4;
- Deve trabalhar simultaneamente com protocolos IPv4 e IPv6;
- Implementar o protocolo IGMP v2, v3;
- Implementar o protocolo VRRP (Virtual Router Redundancy Protocol);
- Implementar roteamento multicast PIM (Protocol Independent Multicast) em modo “sparse-mode”, PIMv2 e PIM-SSM (Source-Specific Multicast);
- Implementar Policy Based Routing;
- IPv6 Management support (Telnet, FTP, SNMP, SSH, NTP).

Segurança:

- Implementar listas de controle de acesso (ACLs) baseadas em endereço IPv4, IPv6 MAC e portas de origem e destino;
- Suportar autenticação via RADIUS e TACACS;
- Possuir suporte a protocolo de autenticação para controle do acesso administrativo ao equipamento;
- Deverá permitir criação de ACL para VLANs (VACL’s);
- Deverá permitir criação de ACL para acesso de terminais (VTY) para TELNET e SSH;
- Implementar mecanismo de autenticação para acesso local ou remoto ao equipamento baseada em um Servidor de Autenticação/Autorização do tipo RADIUS;
- Implementar filtragem de pacotes (ACL - Access Control List), com definições de parâmetros camada 2, 3 e 4;
- Permitir visualização das estatísticas de filtragem das listas de controle de acesso aplicadas;
- Proteger a interface de comando do equipamento através de senha;
- Implementar o protocolo SSH V2 para acesso à interface de linha de comando.
- Permitir a criação de listas de acesso baseadas em endereço IP para limitar o acesso ao switch via Telnet e SSH. Deve ser possível definir os endereços IP de origem das sessões Telnet e SSH;
- Implementar mecanismos de AAA (Authentication, Authorization e Accounting) com garantia de entrega;
- Implementar a criptografia de todos os pacotes enviados ao servidor de controle de acesso e não só os pacotes referentes à senha.
- Permitir controlar quais comandos os usuários ou grupos de usuários podem emitir em determinados elementos de rede.

- Possuir suporte a mecanismo de proteção da “Root Bridge” do algoritmo “Spanning-Tree” para defesa contra ataques do tipo “Denial of Service” no ambiente nível 2.
- Possuir suporte à suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta do switch esteja colocada no modo “Fast Forwarding” (conforme previsto no padrão IEEE 802.1w).
- Deve implementar o padrão IEEE 802.1AE para autenticação e encriptação MACSEc através dos algoritimo 256-bit Advanced Encryption Standard (AES) em todas as portas e velocidades.

Facilidades:

- Implementar Telnet e SSH para acesso à interface de linha de comando.
- Permitir a atualização remota do sistema operacional e arquivos de configuração utilizados no equipamento via interfaces ethernet .
- Ser configurável e gerenciável via GUI (graphical user interface), CLI (command line interface), SNMP, Telnet, SSH, HTTP e HTTPS com, no mínimo, 5 sessões simultâneas e independentes.
- Deve permitir a atualização de sistema operacional através do protocolo TFTP ou FTP.
- Deve permitir a transferência segura de arquivos para o equipamento através do protocolo SCP (Secure Copy) utilizando um cliente padrão ou SFTP (Secure FTP).
- Suportar protocolo SSH para gerenciamento remoto, implementando pelo menos o algoritmo de encriptação de dados 3DES.
- Permitir que a sua configuração seja feita através de terminal assíncrono.
- Permitir a gravação de log externo (syslog). Deve ser possível definir o endereço IP de origem dos pacotes Syslog gerados pelo switch.
- Permitir o armazenamento de sua configuração em memória não volátil, podendo, numa queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior à queda de alimentação.
- Possuir ferramentas para depuração e gerenciamento em primeiro nível, tais como debug, trace, log de eventos.
- Permitir o espelhamento da totalidade do tráfego de uma porta, de um grupo de portas e de VLANs para outra porta localizada no mesmo switch e em outro switch do mesmo tipo conectado à mesma rede local. Deve ser possível definir o sentido do tráfego a ser espelhado: somente tráfego de entrada, somente tráfego de saída e ambos simultaneamente.
- Devem ser suportadas pelo menos duas sessões simultâneas de espelhamento.
- Permitir a adição manual de endereços MAC multicast na tabela de comutação, sem restrição à quantidade de portas a serem associadas.
- Deve ser fornecido com documentação técnica e manuais que contenham informações suficientes para possibilitar a instalação, configuração e operacionalização do equipamento.
- Deve permitir a criação de subgrupos dentro de uma mesma VLAN com conceito de portas isoladas e portas compartilhadas (“promíscuas”), onde portas isoladas não se comunicam com outras portas isoladas, mas apenas com as portas compartilhadas (“promíscuas”) de uma dada VLAN.
- Deve permitir a criação, remoção, gerenciamento e distribuição de VLANs de forma dinâmica através de portas configuradas como tronco IEEE 802.1Q.
- Deverá suportar funcionalidade que permita responder a pacotes para teste da implementação dos níveis de serviço especificados (SLA). Deveram ser suportadas no mínimo as seguintes operações de teste:

1. ICMP echo;
2. TCP connect (em qualquer porta TCP do intervalo 1-50000 que o administrador especifique).
3. UDP echo (em qualquer porta UDP do intervalo 1-50000 que o administrador especifique).
4. O switch deve suportar pelo menos 5 (cinco) destas operações de testes simultaneamente.

- Suportar facilidades de programabilidade através de NETCONF/YANG;
- Suportar scripts de configuração em Python;

Qualidade de Serviço (QoS):

- Possuir a facilidade de priorização de tráfego através do protocolo IEEE 802.1p.
- Possuir suporte a uma fila com prioridade estrita (prioridade absoluta em relação às demais classes dentro do limite de banda que lhe foi atribuído) para tratamento do tráfego “real-time” (voz e vídeo).
- Classificação e Reclassificação baseadas em endereço IP de origem/destino, portas TCP e UDP de origem e destino, endereços MAC de origem e destino.
- Classificação, Marcação e Remarcação baseadas em CoS ("Class of Service" - nivel 2) e DSCP ("Differentiated Services Code Poin\"- nivel 3), conforme definições do IETF (Internet Engineering Task Force).
- Suportar funcionalidades de QoS de “Traffic Shaping” e “Traffic Policing”.
- Deve ser possível a especificação de banda por classe de serviço.
- Para os pacotes que excederem a especificação, deve ser possível configurar ações tais como: transmissão do pacote sem modificação, transmissão com remarcação do valor de DSCP, descarte do pacote.
- Suportar mapeamento de prioridades nível 2, definidas pelo padrão IEEE 802.1p, em prioridades nível 3 (IETF DSCP – Differentiated Services Code Point definido pela Internet Engineering Task Force) e vice-versa.
- Suportar diferenciação de QoS por VLAN.
- Suporte aos mecanismos de QoS WRR (Weighted Round Robin) ou SRR (Shaped Round Robin).
- Suporte aos mecanismos de QoS WRED (Weighted Random Early Detection) ou WTD (Weighted Tail Drop)
- Implementar pelo menos oito filas por porta de saída (egress port).

Gerenciamento:

- O equipamento a ser ofertado deve ser totalmente compatível, e ser fornecido com todas as licenças necessárias para a integração com a PLATAFORMA DE GERENCIAMENTO descrito nesta Especificação Técnica.
- O equipamento a ser ofertado deve implementar gerenciamento orientado a modelo para as funcionalidades de configuração, telemetria, chamadas remotas de procedimentos (RPC) e notificações de eventos de acordo com o padrão YANG (RFC 6020 - YANG - A Data Modeling Language for NETCONF);
- Os Modelos YANG deste equipamento devem estar atualizados para a mesma versão do sistema operacional adotada para a comprovação dos demais requisitos desta especificação. Estes modelos devem estar hospedados em site público que possuam informações de controle de suas versões
- O equipamento a ser ofertado deve implementar, no mínimo, os protocolos de gerenciamento de redes NETCONF (RFC 6241 - Network Configuration Protocol) e gRPC (https://grpc.io/);
- O equipamento a ser ofertado deve implementar, no mínimo, as codificações de dados nos formatos XML (eXtensible Markup Language) e JSON (JavaScript Object Notation);
- O equipamento a ser ofertado deve implementar o método de transporte SSH para o protocolo NETCONF (RFC 4742 ou 6242 - Using the NETCONF Protocol over Secure Shell);
- O equipamento a ser ofertado deve implementar API (Application Programming Interface) modeladas de acordo com o padrão YANG e que implemente os protocolos e as codificações suportadas pela plataforma;
- O equipamento a ser ofertado deve implementar as operações CRUD (Create, Read, Update e Delete) para chamadas via API para modelos YANG abertos e nativos;

- Gerenciável via SSHv2;
- Deve ser gerenciável via SNMP (v1, v2 e v3);
- Implementar o protocolo Syslog para funções de "logging" de eventos;
- Implementar os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps;
- Possuir suporte a MIB II;
- Possibilitar a obtenção da configuração do equipamento através do protocolo SNMP;
- Possibilitar a obtenção via SNMP de informações de capacidade e desempenho da CPU, memória e portas;
- Permitir o controle da geração de traps por porta, possibilitando restringir a geração de traps a portas específicas;
- Implementar nativamente 2 grupos RMON (Alarms e Events);
- Suporte a gerenciamento via CLI, GUI através de interface Web ou da ferramenta de gerenciamento;

2. SWITCH CORE – MODULO DE INTERFACE TIPO I

Características Técnicas

- Deve possuir no mínimo 12 portas de 100GbE utilizando transceptores do tipo QSFP28;
- O modulo de interface deve ser do tipo sem bloqueio (non-blocking);
- Deve permitir a utilização de transceptores do tipo "Short range" (SR4);
- Deve permitir a utilização de transceptores do tipo "Long range" (LR4);
- Deve permitir a utilização de cabos do tipo "break-out" no formato par trançado metálico;
- Deve suportar o padrão IEEE 802.1AE para autenticação e encriptação MACSEc através dos algoritimo 256-bit Advanced Encryption Standard (AES) em todas as portas;
- Deve ser totalmente compatível com o SWITCH CORE descrito nesta Especificação Técnica. Caso sejam necessários a utilização de acessórios, licenças e/ou atualizações de software. Os mesmos devem ser fornecidos;
- Deve permitir sua instalação e remoção sem a necessidade de desligamento do SWITCH CORE.

3. SWITCH CORE – MODULO DE INTERFACE TIPO II

Características Técnicas

- Deve possuir no mínimo 24 portas de 40GbE utilizando transceptores do tipo QSFP+;
- O modulo de interface deve ser do tipo sem bloqueio (non-blocking);
- Deve permitir a utilização de transceptores do tipo "Short range" (SR4);
- Deve permitir a utilização de transceptores do tipo "Long range" (LR4);
- Deve permitir a utilização de cabos do tipo "break-out" tanto em formato par trançado metálico quanto ótico;
- Deve suportar o padrão IEEE 802.1AE para autenticação e encriptação MACSEc através dos algoritimo 256-bit Advanced Encryption Standard (AES) em todas as portas;
- Deve ser totalmente compatível com o SWITCH CORE descrito nesta Especificação Técnica. Caso sejam necessários a utilização de acessórios, licenças e/ou atualizações de software. Os mesmos devem ser fornecidos;
- Deve permitir sua instalação e remoção sem a necessidade de desligamento do SWITCH CORE.

4. SWITCH CORE – MODULO DE INTERFACE TIPO III

Características Técnicas

- Deve possuir no mínimo 48 portas de 1GE, 10GE e 15GE utilizando transceptores do tipo SFP, SFP+ ou QSFP+.
- O modulo de interface deve ser do tipo sem bloqueio (non-blocking);
- Deve permitir a utilização de transceptores do tipo “Short range” (SR4);
- Deve permitir a utilização de transceptores do tipo “Long range” (LR4);
- Deve permitir a utilização de cabos do tipo “TWINAX”;
- Deve suportar o padrão IEEE 802.1AE para autenticação e encriptação MACSEc através dos algoritimo 256-bit Advanced Encryption Standard (AES) em todas as portas;
- Deve ser totalmente compatível com o SWITCH CORE descrito nesta Especificação Técnica. Caso sejam necessários a utilização de acessórios, licenças e/ou atualizações de software. Os mesmos devem ser fornecidos;
- Deve permitir sua instalação e remoção sem a necessidade de desligamento do SWITCH CORE descrito nesta Especificação Técnica.

5. SWITCH CORE – MODULO DE INTERFACE TIPO IV

Características Técnicas

- Deve possuir no mínimo 48 portas 10GE, 5GE, 2.5GE, 1GE, 100Mbps e 10Mbps utilizando conectores RJ-45;
- O modulo de interface deve ser do tipo sem bloqueio (non-blocking);
- Deve suportar o padrão IEEE 802.1AE para autenticação e encriptação MACSEc através dos algoritimo 256-bit Advanced Encryption Standard (AES) em todas as portas;
- Deve ser totalmente compatível com o SWITCH CORE descrito nesta Especificação Técnica. Caso sejam necessários a utilização de acessórios, licenças e/ou atualizações de software. Os mesmos devem ser fornecidos;
- Deve permitir sua instalação e remoção sem a necessidade de desligamento do SWITCH CORE.

6. SWITCH DE DISTRIBUIÇÃO – TIPO I

Interfaces:

- Cada equipamento deve possuir, no mínimo, 24 (vinte e quatro) portas 40GbE (QSFP+) sem bloqueio (non-blocking);
- Possuir porta de console para gerenciamento e configuração via linha de comando. O conector deve ser RJ-45 ou padrão RS-232 (os cabos e eventuais adaptadores necessários para acesso à porta de console devem ser fornecidos);
- Deve possuir no mínimo 1 (uma) porta Ethernet RJ-45 para administração fora de banda (out-of-band management).

Dimensões:

- Permitir ser montado em rack padrão de 19 (dezenove) polegadas, incluindo todos os acessórios necessários.
- Deve possuir no máximo 1 Rack Unit (RU).

Visualização:

- Possuir LEDs para a indicação do status das portas;
- Possuir LEDs do tipo blue beacon para identificação do switch ou porta a ser acessada, para facilitar a manutenção.

Capacidade e Desempenho:

- Possuir matriz de comutação com capacidade de, pelo menos, 1920 Gbps (Gigabits por segundo);
- Possuir capacidade de processamento de, pelo menos, 1440 Mpps (milhões de pacotes por segundo);
- Possuir capacidade de, no mínimo, 64.000 endereços MAC;
- Suporte a Jumbo Frames de, no mínimo, 9198 bytes em todas as suas portas;
- Ser fornecido com configuração de CPU e memória (RAM e Flash) suficiente para implementação de todas as funcionalidades descritas nesta especificação.

Fontes de Alimentação:

- Possuir fontes de alimentação redundantes simétricas internas ao equipamento, sendo que cada fonte deverá possuir potência suficiente para manter o equipamento em pleno funcionamento em sua capacidade máxima, ou seja, com todas as portas ocupadas;
- Possuir fontes de alimentação que operem de 100V a 220V com frequência de 50Hz a 60Hz;
- Os cabos de energia deverão ser fornecidos no padrão brasileiro (NBR 14.136);
- As fontes e as unidades de ventilação devem ser capazes de serem trocadas com o equipamento em pleno funcionamento, sem nenhum impacto na performance (hot-swappable).

Alta Disponibilidade:

- Suportar Non-Stop Forwarding e Stateful Switchover (NSF/SSO);
- Suportar upgrade de software em serviço (In Service Software Upgrade – ISSU);
- Deve prover total redundância com outros equipamentos da mesma marca e modelo, devendo atender uma das seguintes formas de alta disponibilidade:

Formar um virtual switch, de forma que os dois possam ser vistos como uma entidade única, logicamente. Esta funcionalidade pode ser provida através de:

Tecnologias do tipo Virtual ou Multi-Chassis;

Tecnologias de Stacking (físico ou virtual), garantindo que a pilha continue a funcionar na eventual falha de um dispositivo, sendo a pilha gerenciada como uma entidade única;

Tecnologias do tipo Multi-LAG (Multi Link Aggregation) permitindo a redundância de link's entre switches distintos.

Em caso de empilhamento ou Multi-LAG, deverão ser fornecidos todos os componentes necessários para garantia da alta disponibilidade, incluindo todos os módulos e/ou cabos/transceivers para interconexão dos equipamentos, bem como as licenças necessárias, caso aplicável;

Cada switch deve ser fornecido com fontes e ventiladores redundantes e hot-swappable;

- Possuir fontes de alimentação redundantes que operem no modo N+1 ou N+N de forma a garantir o pleno funcionamento do equipamento conforme configuração solicitada, em caso de falha de pelo menos uma das fontes de alimentação.

Funcionalidades de Camada 2:

- Implementar até 4.000 VLAN IDs simultâneas conforme definições do padrão IEEE 802.1Q;

- Deve suportar VLANs dinâmicas. Deve permitir a criação, remoção e distribuição de VLANs de forma dinâmica através de portas configuradas como tronco IEEE 802.1Q;
- Implementar "VLAN Trunking" conforme padrão IEEE 802.1Q nas portas Fast Ethernet e Gigabit Ethernet. Deve ser possível estabelecer quais VLANs serão permitidas em cada um dos troncos 802.1Q configurados;
- Deve implementar Private VLANs;
- Implementar a funcionalidade de "Link Aggregation" (LAGs) conforme padrão IEEE 802.3ad, com no mínimo 8 (oito) portas por LAG (IEEE 802.3ad);
- Deve implementar o padrão IEEE 802.1d ("Spanning Tree Protocol"), IEEE 802.1s ("Multiple Spanning Tree") e IEEE 802.1w ("Rapid Spanning Tree");
- Deve implementar no mínimo 64 (sessenta e quatro) múltiplas Instâncias de Spanning Tree;
- Implementar mecanismo de proteção da "root bridge" do algoritmo Spanning-Tree para prover defesa contra ataques do tipo "Denial of Service" no ambiente de camada 2;
- Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo "fast forwarding" (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente;
- Deve implementar o protocolo IEEE 802.1AB Link Layer Discovery Protocol (LLDP), permitindo a descoberta dos elementos de rede vizinhos;
- Deve suportar exportação de fluxos (IPFIX ou Netflow) para análise do tráfego da rede;
- Deverá ter contadores de entrada e saída de pacotes por porta;
- Deverá suportar NTP.

Funcionalidades de Camada 3:

- Possuir roteamento nível 3 entre VLANs;
- Suportar roteamento de pacotes IPv4 e IPv6;
- Suporte a, pelo menos, 64.000 (sessenta e quatro mil) rotas IPv4 dinâmicas;
- Suporte a, pelo menos, 32.000 (trinta e duas mil) rotas IPv6 dinâmicas;
- Implementar roteamento estático e dinâmico;
- Implementar protocolo de roteamento dinâmico OSPF v2 e v3;
- Implementar protocolo de roteamento dinâmico BGPv4;
- Deve trabalhar simultaneamente com protocolos IPv4 e IPv6;
- Implementar o protocolo IGMP v2, v3;
- Implementar o protocolo VRRP (Virtual Router Redundancy Protocol);
- Implementar roteamento multicast PIM (Protocol Independent Multicast) em modo "sparse-mode", PIMv2 e PIM-SSM (Source-Specific Multicast);
- Implementar Policy Based Routing;
- IPv6 Management support (Telnet, FTP, SNMP, SSH, NTP).

Segurança:

- Implementar listas de controle de acesso (ACLs) baseadas em endereço IPv4, IPv6 MAC e portas de origem e destino;
- Suportar autenticação via RADIUS e TACACS;
- Possuir suporte a protocolo de autenticação para controle do acesso administrativo ao equipamento;
- Deverá permitir criação de ACL para VLANs (VACL's);

- Deverá permitir criação de ACL para acesso de terminais (VTY) para TELNET e SSH;
- Implementar mecanismo de autenticação para acesso local ou remoto ao equipamento baseada em um Servidor de Autenticação/Autorização do tipo RADIUS;
- Implementar filtragem de pacotes (ACL - Access Control List), com definições de parâmetros camada 2, 3 e 4;
- Permitir visualização das estatísticas de filtragem das listas de controle de acesso aplicadas;
- Proteger a interface de comando do equipamento através de senha;
- Implementar o protocolo SSH V2 para acesso à interface de linha de comando.
- Permitir a criação de listas de acesso baseadas em endereço IP para limitar o acesso ao switch via Telnet e SSH. Deve ser possível definir os endereços IP de origem das sessões Telnet e SSH;
- Implementar mecanismos de AAA (Authentication, Authorization e Accounting) com garantia de entrega;
- Implementar a criptografia de todos os pacotes enviados ao servidor de controle de acesso e não só os pacotes referentes à senha.
- Permitir controlar quais comandos os usuários ou grupos de usuários podem emitir em determinados elementos de rede.
- Possuir suporte a mecanismo de proteção da “Root Bridge” do algoritmo “Spanning-Tree” para defesa contra ataques do tipo “Denial of Service” no ambiente nível 2.
- Possuir suporte à suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta do switch esteja colocada no modo “Fast Forwarding” (conforme previsto no padrão IEEE 802.1w).
- Deve implementar o padrão IEEE 802.1AE para autenticação e encriptação MACSEc através dos algoritimo 256-bit Advanced Encryption Standard (AES) em todas as portas e velocidades.

Facilidades:

- Implementar Telnet e SSH para acesso à interface de linha de comando.
- Permitir a atualização remota do sistema operacional e arquivos de configuração utilizados no equipamento via interfaces ethernet .
- Ser configurável e gerenciável via GUI (graphical user interface), CLI (command line interface), SNMP, Telnet, SSH, HTTP e HTTPS com, no mínimo, 5 sessões simultâneas e independentes.
- Deve permitir a atualização de sistema operacional através do protocolo TFTP ou FTP.
- Deve permitir a transferência segura de arquivos para o equipamento através do protocolo SCP (Secure Copy) utilizando um cliente padrão ou SFTP (Secure FTP).
- Suportar protocolo SSH para gerenciamento remoto, implementando pelo menos o algoritmo de encriptação de dados 3DES.
- Permitir que a sua configuração seja feita através de terminal assíncrono.
- Permitir a gravação de log externo (syslog). Deve ser possível definir o endereço IP de origem dos pacotes Syslog gerados pelo switch.
- Permitir o armazenamento de sua configuração em memória não volátil, podendo, numa queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior à queda de alimentação.
- Possuir ferramentas para depuração e gerenciamento em primeiro nível, tais como debug, trace, log de eventos.
- Permitir o espelhamento da totalidade do tráfego de uma porta, de um grupo de portas e de VLANs para outra porta localizada no mesmo switch e em outro switch do mesmo tipo conectado à mesma rede local. Deve ser possível definir o sentido do tráfego a ser espelhado: somente tráfego de entrada, somente tráfego de saída e ambos simultaneamente.
- Devem ser suportadas pelo menos duas sessões simultâneas de espelhamento.

- Permitir a adição manual de endereços MAC multicast na tabela de comutação, sem restrição à quantidade de portas a serem associadas.
- Deve ser fornecido com documentação técnica e manuais que contenham informações suficientes para possibilitar a instalação, configuração e operacionalização do equipamento.
- Deve permitir a criação de subgrupos dentro de uma mesma VLAN com conceito de portas isoladas e portas compartilhadas (“promíscuas”), onde portas isoladas não se comunicam com outras portas isoladas, mas apenas com as portas compartilhadas (“promíscuas”) de uma dada VLAN.
- Deve permitir a criação, remoção, gerenciamento e distribuição de VLANs de forma dinâmica através de portas configuradas como tronco IEEE 802.1Q.
- Deverá suportar funcionalidade que permita responder a pacotes para teste da implementação dos níveis de serviço especificados (SLA). Deveram ser suportadas no mínimo as seguintes operações de teste:

1. ICMP echo;
2. TCP connect (em qualquer porta TCP do intervalo 1-50000 que o administrador especifique).
3. UDP echo (em qualquer porta UDP do intervalo 1-50000 que o administrador especifique).
4. O switch deve suportar pelo menos 5 (cinco) destas operações de testes simultaneamente.
5. Suportar facilidades de programabilidade através de NETCONF/YANG;
6. Suportar scripts de configuração em Python;

Qualidade de Serviço (QoS):

- Possuir a facilidade de priorização de tráfego através do protocolo IEEE 802.1p.
- Possuir suporte a uma fila com prioridade estrita (prioridade absoluta em relação às demais classes dentro do limite de banda que lhe foi atribuído) para tratamento do tráfego “real-time” (voz e vídeo).
- Classificação e Reclassificação baseadas em endereço IP de origem/destino, portas TCP e UDP de origem e destino, endereços MAC de origem e destino.
- Classificação, Marcação e Remarcação baseadas em CoS ("Class of Service" - nivel 2) e DSCP ("Differentiated Services Code Poin\"- nivel 3), conforme definições do IETF (Internet Engineering Task Force).
- Suportar funcionalidades de QoS de “Traffic Shaping” e “Traffic Policing”.
- Deve ser possível a especificação de banda por classe de serviço.
- Para os pacotes que excederem a especificação, deve ser possível configurar ações tais como : transmissão do pacote sem modificação, transmissão com remarcação do valor de DSCP, descarte do pacote.
- Suportar mapeamento de prioridades nível 2, definidas pelo padrão IEEE 802.1p, em prioridades nível 3 (IETF DSCP – Differentiated Services Code Point definido pela Internet Engineering Task Force) e vice-versa.
- Suportar diferenciação de QoS por VLAN.
- Suporte aos mecanismos de QoS WRR (Weighted Round Robin) ou SRR (Shaped Round Robin).
- Suporte aos mecanismos de QoS WRED (Weighted Random Early Detection) ou WTD (Weighted Tail Drop)
- Implementar pelo menos oito filas por porta de saída (egress port).

Gerenciamento:

- O equipamento a ser ofertado deve ser totalmente compatível, e ser fornecido com todas as licenças necessárias para a integração com a PLATAFORMA DE GERENCIAMENTO descrito nesta Especificação Técnica.

- O equipamento a ser ofertado deve implementar gerenciamento orientado a modelo para as funcionalidades de configuração, telemetria, chamadas remotas de procedimentos (RPC) e notificações de eventos de acordo com o padrão YANG (RFC 6020 - YANG - A Data Modeling Language for NETCONF);
- Os Modelos YANG deste equipamento devem estar atualizados para a mesma versão do sistema operacional adotada para a comprovação dos demais requisitos desta especificação. Estes modelos devem estar hospedados em site público que possuam informações de controle de suas versões
- O equipamento a ser ofertado deve implementar, no mínimo, os protocolos de gerenciamento de redes NETCONF (RFC 6241 - Network Configuration Protocol) e gRPC (https://grpc.io/);
- O equipamento a ser ofertado deve implementar, no mínimo, as codificações de dados nos formatos XML (eXtensible Markup Language) e JSON (JavaScript Object Notation);
- O equipamento a ser ofertado deve implementar o método de transporte SSH para o protocolo NETCONF (RFC 4742 ou 6242 - Using the NETCONF Protocol over Secure Shell);
- O equipamento a ser ofertado deve implementar API (Application Programming Interface) modeladas de acordo com o padrão YANG e que implemente os protocolos e as codificações suportadas pela plataforma;
- O equipamento a ser ofertado deve implementar as operações CRUD (Create, Read, Update e Delete) para chamadas via API para modelos YANG abertos e nativos;
- Gerenciável via SSHv2;
- Deve ser gerenciável via SNMP (v1, v2 e v3);
- Implementar o protocolo Syslog para funções de “logging” de eventos;
- Implementar os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps;
- Possuir suporte a MIB II;
- Possibilitar a obtenção da configuração do equipamento através do protocolo SNMP;
- Possibilitar a obtenção via SNMP de informações de capacidade e desempenho da CPU, memória e portas;
- Permitir o controle da geração de traps por porta, possibilitando restringir a geração de traps a portas específicas;
- Implementar nativamente 2 grupos RMON (Alarms e Events);
- Suporte a gerenciamento via CLI, GUI através de interface Web ou da ferramenta de gerenciamento;

7. SWITCH DE DISTRIBUIÇÃO – TIPO II

Interfaces:

- Cada equipamento deve possuir, no mínimo, 48 (vinte e quatro) portas 1/10/25 GbE (SFP/SFP+/SFP28) sem bloqueio (non-blocking);
- Cada equipamento deve possuir, no mínimo, 4 (quatro) portas 40/100 GbE (QSFP+/QSFP28) para uplink
- Possuir porta de console para gerenciamento e configuração via linha de comando. O conector deve ser RJ-45 ou padrão RS-232 (os cabos e eventuais adaptadores necessários para acesso à porta de console devem ser fornecidos);
- Deve possuir no mínimo 1 (uma) porta Ethernet RJ-45 para administração fora de banda (out-of-band management).

Dimensões:

- Permitir ser montado em rack padrão de 19 (dezenove) polegadas, incluindo todos os acessórios necessários.
- Deve possuir no máximo 1 Rack Unit (RU).

Visualização:

- Possuir LEDs para a indicação do status das portas;
- Possuir LEDs do tipo blue beacon para identificação do switch ou porta a ser acessada, para facilitar a manutenção.

Capacidade e Desempenho:

- Possuir matriz de comutação com capacidade de, pelo menos, 3200 Gbps (Gigabits por segundo);
- Possuir capacidade de processamento de, pelo menos, 1 Bpps (bilhões de pacotes por segundo);
- Possuir capacidade de, no mínimo, 64.000 endereços MAC;
- Suporte a Jumbo Frames de, no mínimo, 9198 bytes em todas as suas portas;
- Ser fornecido com configuração de CPU e memória (RAM e Flash) suficiente para implementação de todas as funcionalidades descritas nesta especificação.

Fontes de Alimentação:

- Possuir fontes de alimentação redundantes simétricas internas ao equipamento, sendo que cada fonte deverá possuir potência suficiente para manter o equipamento em pleno funcionamento em sua capacidade máxima, ou seja, com todas as portas ocupadas;
- Possuir fontes de alimentação que operem de 100V a 220V com frequência de 50Hz a 60Hz;
- Os cabos de energia deverão ser fornecidos no padrão brasileiro (NBR 14.136);
- As fontes e as unidades de ventilação devem ser capazes de serem trocadas com o equipamento em pleno funcionamento, sem nenhum impacto na performance (hot-swappable).

Alta Disponibilidade:

- Suportar Non-Stop Forwarding e Stateful Switchover (NSF/SSO);
- Suportar upgrade de software em serviço (In Service Software Upgrade – ISSU);
- Deve prover total redundância com outros equipamentos da mesma marca e modelo, devendo atender uma das seguintes formas de alta disponibilidade:

Formar um virtual switch, de forma que os dois possam ser vistos como uma entidade única, logicamente. Esta funcionalidade pode ser provida através de:

Tecnologias do tipo Virtual ou Multi-Chassis;

Tecnologias de Stacking (físico ou virtual), garantindo que a pilha continue a funcionar na eventual falha de um dispositivo, sendo a pilha gerenciada como uma entidade única;

Tecnologias do tipo Multi-LAG (Multi Link Aggregation) permitindo a redundância de link's entre switches distintos.

Em caso de empilhamento ou Multi-LAG, deverão ser fornecidos todos os componentes necessários para garantia da alta disponibilidade, incluindo todos os módulos e/ou cabos/transceivers para interconexão dos equipamentos, bem como as licenças necessárias, caso aplicável;

Cada switch deve ser fornecido com fontes e ventiladores redundantes e hot-swappable;

- Possuir fontes de alimentação redundantes que operem no modo N+1 ou N+N de forma a garantir o pleno funcionamento do equipamento conforme configuração solicitada, em caso de falha de pelo menos uma das fontes de alimentação.

Funcionalidades de Camada 2:

- Implementar até 4.000 VLAN IDs simultâneas conforme definições do padrão IEEE 802.1Q;
- Deve suportar VLANs dinâmicas. Deve permitir a criação, remoção e distribuição de VLANs de forma dinâmica através de portas configuradas como tronco IEEE 802.1Q;
- Implementar "VLAN Trunking" conforme padrão IEEE 802.1Q nas portas Fast Ethernet e Gigabit Ethernet. Deve ser possível estabelecer quais VLANs serão permitidas em cada um dos troncos 802.1Q configurados;
- Deve implementar Private VLANs;
- Implementar a funcionalidade de "Link Aggregation" (LAGs) conforme padrão IEEE 802.3ad, com no mínimo 8 (oito) portas por LAG (IEEE 802.3ad);
- Deve implementar o padrão IEEE 802.1d ("Spanning Tree Protocol"), IEEE 802.1s ("Multiple Spanning Tree") e IEEE 802.1w ("Rapid Spanning Tree");
- Deve implementar no mínimo 64 (sessenta e quatro) múltiplas Instâncias de Spanning Tree;
- Implementar mecanismo de proteção da "root bridge" do algoritmo Spanning-Tree para prover defesa contra ataques do tipo "Denial of Service" no ambiente de camada 2;
- Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo "fast forwarding" (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente;
- Deve implementar o protocolo IEEE 802.1AB Link Layer Discovery Protocol (LLDP), permitindo a descoberta dos elementos de rede vizinhos;
- Deve suportar exportação de fluxos (IPFIX ou Netflow) para análise do tráfego da rede;
- Deverá ter contadores de entrada e saída de pacotes por porta;
- Deverá suportar NTP.

Funcionalidades de Camada 3:

- Possuir roteamento nível 3 entre VLANs;
- Suportar roteamento de pacotes IPv4 e IPv6;
- Suporte a, pelo menos, 64.000 (sessenta e quatro mil) rotas IPv4 dinâmicas;
- Suporte a, pelo menos, 32.000 (trinta e duas mil) rotas IPv6 dinâmicas;
- Implementar roteamento estático e dinâmico;
- Implementar protocolo de roteamento dinâmico OSPF v2 e v3;
- Implementar protocolo de roteamento dinâmico BGPv4;
- Deve trabalhar simultaneamente com protocolos IPv4 e IPv6;
- Implementar o protocolo IGMP v2, v3;
- Implementar o protocolo VRRP (Virtual Router Redundancy Protocol);
- Implementar roteamento multicast PIM (Protocol Independent Multicast) em modo "sparse-mode", PIMv2 e PIM-SSM (Source-Specific Multicast);
- Implementar Policy Based Routing;
- IPv6 Management support (Telnet, FTP, SNMP, SSH, NTP).

Segurança:

- Implementar listas de controle de acesso (ACLs) baseadas em endereço IPv4, IPv6 MAC e portas de origem e destino;
- Suportar autenticação via RADIUS e TACACS;

- Possuir suporte a protocolo de autenticação para controle do acesso administrativo ao equipamento;
- Deverá permitir criação de ACL para VLANs (VACL's);
- Deverá permitir criação de ACL para acesso de terminais (VTY) para TELNET e SSH;
- Implementar mecanismo de autenticação para acesso local ou remoto ao equipamento baseada em um Servidor de Autenticação/Autorização do tipo RADIUS;
- Implementar filtragem de pacotes (ACL - Access Control List), com definições de parâmetros camada 2, 3 e 4;
- Permitir visualização das estatísticas de filtragem das listas de controle de acesso aplicadas;
- Proteger a interface de comando do equipamento através de senha;
- Implementar o protocolo SSH V2 para acesso à interface de linha de comando.
- Permitir a criação de listas de acesso baseadas em endereço IP para limitar o acesso ao switch via Telnet e SSH. Deve ser possível definir os endereços IP de origem das sessões Telnet e SSH;
- Implementar mecanismos de AAA (Authentication, Authorization e Accounting) com garantia de entrega;
- Implementar a criptografia de todos os pacotes enviados ao servidor de controle de acesso e não só os pacotes referentes à senha.
- Permitir controlar quais comandos os usuários ou grupos de usuários podem emitir em determinados elementos de rede.
- Possuir suporte a mecanismo de proteção da "Root Bridge" do algoritmo "Spanning-Tree" para defesa contra ataques do tipo "Denial of Service" no ambiente nível 2.
- Possuir suporte à suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta do switch esteja colocada no modo "Fast Forwarding" (conforme previsto no padrão IEEE 802.1w).
- Deve implementar o padrão IEEE 802.1AE para autenticação e encriptação MACSEc através dos algoritimo 256-bit Advanced Encryption Standard (AES) em todas as portas e velocidades.

Facilidades:

- Implementar Telnet e SSH para acesso à interface de linha de comando.
- Permitir a atualização remota do sistema operacional e arquivos de configuração utilizados no equipamento via interfaces ethernet.
- Ser configurável e gerenciável via GUI (graphical user interface), CLI (command line interface), SNMP, Telnet, SSH, HTTP e HTTPS com, no mínimo, 5 sessões simultâneas e independentes.
- Deve permitir a atualização de sistema operacional através do protocolo TFTP ou FTP.
- Deve permitir a transferência segura de arquivos para o equipamento através do protocolo SCP (Secure Copy) utilizando um cliente padrão ou SFTP (Secure FTP).
- Suportar protocolo SSH para gerenciamento remoto, implementando pelo menos o algoritmo de encriptação de dados 3DES.
- Permitir que a sua configuração seja feita através de terminal assíncrono.
- Permitir a gravação de log externo (syslog). Deve ser possível definir o endereço IP de origem dos pacotes Syslog gerados pelo switch.
- Permitir o armazenamento de sua configuração em memória não volátil, podendo, numa queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior à queda de alimentação.
- Possuir ferramentas para depuração e gerenciamento em primeiro nível, tais como debug, trace, log de eventos.
- Permitir o espelhamento da totalidade do tráfego de uma porta, de um grupo de portas e de VLANs para outra porta localizada no mesmo switch e em outro switch do mesmo tipo conectado à mesma

rede local. Deve ser possível definir o sentido do tráfego a ser espelhado: somente tráfego de entrada, somente tráfego de saída e ambos simultaneamente.

- Devem ser suportadas pelo menos duas sessões simultâneas de espelhamento.
- Permitir a adição manual de endereços MAC multicast na tabela de comutação, sem restrição à quantidade de portas a serem associadas.
- Deve ser fornecido com documentação técnica e manuais que contenham informações suficientes para possibilitar a instalação, configuração e operacionalização do equipamento.
- Deve permitir a criação de subgrupos dentro de uma mesma VLAN com conceito de portas isoladas e portas compartilhadas (“promíscuas”), onde portas isoladas não se comunicam com outras portas isoladas, mas apenas com as portas compartilhadas (“promíscuas”) de uma dada VLAN.
- Deve permitir a criação, remoção, gerenciamento e distribuição de VLANs de forma dinâmica através de portas configuradas como tronco IEEE 802.1Q.
- Deverá suportar funcionalidade que permita responder a pacotes para teste da implementação dos níveis de serviço especificados (SLA). Deveram ser suportadas no mínimo as seguintes operações de teste:

1. ICMP echo;
2. TCP connect (em qualquer porta TCP do intervalo 1-50000 que o administrador especifique).
3. UDP echo (em qualquer porta UDP do intervalo 1-50000 que o administrador especifique).
4. O switch deve suportar pelo menos 5 (cinco) destas operações de testes simultaneamente.

- Suportar facilidades de programabilidade através de NETCONF/YANG;
- Suportar scripts de configuração em Python;

Qualidade de Serviço (QoS):

- Possuir a facilidade de priorização de tráfego através do protocolo IEEE 802.1p.
- Possuir suporte a uma fila com prioridade estrita (prioridade absoluta em relação às demais classes dentro do limite de banda que lhe foi atribuído) para tratamento do tráfego “real-time” (voz e vídeo).
- Classificação e Reclassificação baseadas em endereço IP de origem/destino, portas TCP e UDP de origem e destino, endereços MAC de origem e destino.
- Classificação, Marcação e Remarcação baseadas em CoS ("Class of Service" - nivel 2) e DSCP ("Differentiated Services Code Poin\"- nivel 3), conforme definições do IETF (Internet Engineering Task Force).
- Suportar funcionalidades de QoS de “Traffic Shaping” e “Traffic Policing”.
- Deve ser possível a especificação de banda por classe de serviço.
- Para os pacotes que excederem a especificação, deve ser possível configurar ações tais como: transmissão do pacote sem modificação, transmissão com remarcação do valor de DSCP, descarte do pacote.
- Suportar mapeamento de prioridades nível 2, definidas pelo padrão IEEE 802.1p, em prioridades nível 3 (IETF DSCP – Differentiated Services Code Point definido pela Internet Engineering Task Force) e vice-versa.
- Suportar diferenciação de QoS por VLAN.
- Suporte aos mecanismos de QoS WRR (Weighted Round Robin) ou SRR (Shaped Round Robin).
- Suporte aos mecanismos de QoS WRED (Weighted Random Early Detection) ou WTD (Weighted Tail Drop)
- Implementar pelo menos oito filas por porta de saída (egress port).

Gerenciamento:

- O equipamento a ser ofertado deve ser totalmente compatível, e ser fornecido com todas as licenças necessárias para a integração com a PLATAFORMA DE GERENCIAMENTO descrito nesta Especificação Técnica.
- O equipamento a ser ofertado deve implementar gerenciamento orientado a modelo para as funcionalidades de configuração, telemetria, chamadas remotas de procedimentos (RPC) e notificações de eventos de acordo com o padrão YANG (RFC 6020 - YANG - A Data Modeling Language for NETCONF);
- Os Modelos YANG deste equipamento devem estar atualizados para a mesma versão do sistema operacional adotada para a comprovação dos demais requisitos desta especificação. Estes modelos devem estar hospedados em site público que possuam informações de controle de suas versões
- O equipamento a ser ofertado deve implementar, no mínimo, os protocolos de gerenciamento de redes NETCONF (RFC 6241 - Network Configuration Protocol) e gRPC (https://grpc.io/);
- O equipamento a ser ofertado deve implementar, no mínimo, as codificações de dados nos formatos XML (eXtensible Markup Language) e JSON (JavaScript Object Notation);
- O equipamento a ser ofertado deve implementar o método de transporte SSH para o protocolo NETCONF (RFC 4742 ou 6242 - Using the NETCONF Protocol over Secure Shell);
- O equipamento a ser ofertado deve implementar API (Application Programming Interface) modeladas de acordo com o padrão YANG e que implemente os protocolos e as codificações suportadas pela plataforma;
- O equipamento a ser ofertado deve implementar as operações CRUD (Create, Read, Update e Delete) para chamadas via API para modelos YANG abertos e nativos;
- Gerenciável via SSHv2;
- Deve ser gerenciável via SNMP (v1, v2 e v3);
- Implementar o protocolo Syslog para funções de “logging” de eventos;
- Implementar os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps;
- Possuir suporte a MIB II;
- Possibilitar a obtenção da configuração do equipamento através do protocolo SNMP;
- Possibilitar a obtenção via SNMP de informações de capacidade e desempenho da CPU, memória e portas;
- Permitir o controle da geração de traps por porta, possibilitando restringir a geração de traps a portas específicas;
- Implementar nativamente 2 grupos RMON (Alarms e Events);
- Suporte a gerenciamento via CLI, GUI através de interface Web ou da ferramenta de gerenciamento;

8. SWITCH DE DISTRIBUIÇÃO – TIPO III

Interfaces:

- Possuir 2 portas 40 GbE padrão QSFP para conexão de uplink;
- Cada equipamento deve ser fornecido com 02 (dois) Transceivers QSFP 40G BIDIRECIONAL SHORT REACH MMF;
- Possuir, no mínimo, 48 portas Ethernet 10/100/1000 Base-T com autosensing de velocidade e com conectores RJ-45 para conexão de acesso. Todas as 48 portas devem operar simultaneamente em conjunto com as 2 portas de uplink;
- Todas as portas Ethernet 10/100/1000 devem suportar configuração Half-Duplex (10/100) e Full-Duplex, com a opção de negociação automática;

- As interfaces 10/100/1000 devem obedecer às normas técnicas IEEE 802.3 (10BaseT), IEEE 802.3u (100BaseTX), 802.3ab (1000BaseT) e IEEE 802.3x (Flow Control), além de IEEE 802.3af e 802.3at (PoE e PoE+);
- Todas as portas Ethernet 10/100/1000 devem suportar autoconfiguração de crossover (Auto MDIX);
- Possuir capacidade de associação das portas de acesso em grupo de, no mínimo, 8 (oito) portas, formando uma única interface lógica com as mesmas facilidades das interfaces originais, compatível com a norma IEEE 802.3ad LACP. Deve ser possível criar pelo menos 24 grupos LACP;
- Possibilitar a configuração dinâmica de portas por software, permitindo a definição de portas ativas/inativas;
- Implementar VLANs por porta;
- Implementar VLANs compatíveis com o padrão IEEE 802.1q;
- Implementar mecanismo de seleção de quais vlans serão permitidas através de trunk 802.1q. Deve ser permitida a configuração dessa seleção de forma dinâmica;
- Possuir porta de console para ligação direta de terminal RS-232 para acesso à interface de linha de comando. Poderá opcionalmente ser fornecida porta de console com interface USB;
- Possuir porta Ethernet 10/100 Base-T dedicada para gerenciamento out-of-band;
- Possuir porta USB compatível com flash drives, para cópias de arquivos de configuração e arquivos de sistema operacional.

Fontes de Alimentação:

- Suportar fonte de alimentação redundante interna AC bivolt, com seleção automática de tensão (na faixa de 100 a 240 Volts) e frequência (de 50/60 Hz). As fontes deverão possuir alimentação independente, a fim de permitir a sua conexão a circuitos elétricos distintos;
- Deve permitir troca da fonte redundante sem interrupção do funcionamento do switch;
- A fonte de alimentação deverá possuir no minimo 437W para alimentação PoE+ (até 30W por porta), além da energia necessária para funcionamento do switch. Não serão aceitos dispositivos externos para complementação de energia PoE no switch;
- Suportar balanceamento de carga entre as fontes de alimentação redundantes, as fontes devem ser dimensionadas para permitir o completo funcionamento do switch com apenas 1 (uma) fonte;
- Permitir o compartilhamento das fontes internas ao equipamento entre diferentes elementos da pilha de switches;
- Deve possuir unidade de ventilação redundante e que permita substituição em caso de falha, sem necessidade de troca do switch.

Dimensões:

- Permitir ser montado em rack padrão de 19 (dezenove) polegadas, incluindo todos os acessórios necessários.
- Deve possuir no máximo 1 Rack Unit (RU).

Visualização:

- Possuir LEDs para a indicação do status das portas e atividade, além do modo duplex.

Gerenciamento:

- O equipamento a ser ofertado deve ser totalmente compatível, e ser fornecido com todas as licenças necessárias para a integração com a PLATAFORMA DE GERENCIAMENTO descrito nesta Especificação Técnica.

- Implementar os padrões abertos de gerência de rede SNMPv1 (RFC 1157), SNMPv2 (RFC 1901 a 1907) e SNMPv3 (RFC 2273 a 2275);
- Implementar pelo menos os seguintes níveis de segurança para SNMP versão 3:

1. Sem autenticação e sem privacidade (noAuthNoPriv);
2. Com autenticação e sem privacidade (authNoPriv);
3. Com autenticação e com privacidade (authPriv) utilizando algoritimo de criptografia AES 256-bit.

- Possibilitar a obtenção da configuração do equipamento através do protocolo SNMP;
- Possuir armazenamento interno das mensagens de log geradas pelo equipamento;
- Possuir capacidade de exportar as mensangens de log geradas pelo equipamento para um servidor syslog externo;
- Permitir o controle da geração de traps SNMP, possibilitando definir quais tipos de alarmes geram traps;
- Implementar nativamente pelo menos 2 grupos RMON (Alarms e Events);
- Implementar os protocolos LLDP (IEEE 802.1AB) e LLDP-MED;
- Suportar a coleta de informações de fluxos Layer 2, IPv4 e IPv6 através de IPFIX ou NetFlow. Deve coletar informações referentes a 100% dos pacotes que trafegam no equipamento.

Facilidades:

- O equipamento a ser ofertado deve implementar gerenciamento orientado a modelo para as funcionalidades de configuração, telemetria, chamadas remotas de procedimentos (RPC) e notificações de eventos de acordo com o padrão YANG (RFC 6020 - YANG - A Data Modeling Language for NETCONF);
- Os Modelos YANG deste equipamento devem estar atualizados para a mesma versão do sistema operacional adotada para a comprovação dos demais requisitos desta especificação. Estes modelos devem estar hospedados em site público que possuam informações de controle de suas versões
- O equipamento a ser ofertado deve implementar, no mínimo, os protocolos de gerenciamento de redes NETCONF (RFC 6241 - Network Configuration Protocol) e gRPC (https://grpc.io/);
- O equipamento a ser ofertado deve implementar, no mínimo, as codificações de dados nos formatos XML (eXtensible Markup Language) e JSON (JavaScript Object Notation);
- O equipamento a ser ofertado deve implementar o método de transporte SSH para o protocolo NETCONF (RFC 4742 ou 6242 - Using the NETCONF Protocol over Secure Shell);
- O equipamento a ser ofertado deve implementar API (Application Programming Interface) modeladas de acordo com o padrão YANG e que implemente os protocolos e as codificações suportadas pela plataforma;
- O equipamento a ser ofertado deve implementar as operações CRUD (Create, Read, Update e Delete) para chamadas via API para modelos YANG abertos e nativos;
- Gerenciável via SSHv2;
- Deve ser gerenciável via SNMP (v1, v2 e v3);
- Implementar o protocolo Syslog para funções de “logging” de eventos;
- Implementar os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps;
- Possuir suporte a MIB II;
- Possibilitar a obtenção da configuração do equipamento através do protocolo SNMP;
- Possibilitar a obtenção via SNMP de informações de capacidade e desempenho da CPU, memória e portas;

- Permitir o controle da geração de traps por porta, possibilitando restringir a geração de traps a portas específicas;
- Implementar nativamente 2 grupos RMON (Alarms e Events);
- Suporte a gerenciamento via CLI, GUI através de interface Web ou da ferramenta de gerenciamento;
- Implementar Telnet e SSH para acesso à interface de linha de comando.
- Permitir a atualização remota do sistema operacional e arquivos de configuração utilizados no equipamento via interfaces ethernet .
- Ser configurável e gerenciável via GUI (graphical user interface), CLI (command line interface), SNMP, Telnet, SSH, HTTP e HTTPS com, no mínimo, 5 sessões simultâneas e independentes.
- Deve permitir a atualização de sistema operacional através do protocolo TFTP ou FTP, e cópia segura e autenticada através de SCP (Secure Copy Protocol).
- Suportar protocolo SSH para gerenciamento remoto, implementando pelo menos o algoritmo de encriptação de dados 3DES.
- Permitir que a sua configuração seja feita através de terminal assíncrono.
- Permitir o armazenamento de sua configuração em memória não volátil, podendo, numa queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior à queda de alimentação.
- Possuir ferramentas para depuração e gerenciamento em primeiro nível, tais como debug, trace, log de eventos.
- Permitir o espelhamento da totalidade do tráfego de uma porta, de um grupo de portas e de VLANs para outra porta localizada no mesmo switch e em outro switch do mesmo tipo conectado à mesma rede local. Deve ser possível definir o sentido do tráfego a ser espelhado: somente tráfego de entrada, somente tráfego de saída e ambos simultaneamente.
- Permitir o espelhamento do tráfego de portas que residem em um dado módulo para uma porta que reside em módulo diferente do switch.
- Devem ser suportadas pelo menos duas sessões simultâneas de espelhamento.
- O espelhamento não pode interferir no funcionamento normal do equipamento
- Deve ser fornecido com documentação técnica e manuais que contenham informações suficientes para possibilitar a instalação, configuração e operacionalização do equipamento.
- Implementar funcionalidade de separação do tráfego de voz e dados em uma mesma porta de acesso (Voice VLAN), sem a necessidade de utilização de 802.1q.
- Deve responder a pacotes para teste da implementação dos níveis de serviço especificados (SLA). Deveram ser suportadas no mínimo as seguintes operações de teste:

1. ICMP echo;
2. TCP connect (em qualquer porta TCP do intervalo 1-50000 que o administrador especifique).
3. UDP echo (em qualquer porta UDP do intervalo 1-50000 que o administrador especifique).
4. O switch deve suportar pelo menos 5 (cinco) destas operações de testes simultaneamente.

- Permitir a atualização de software sem perda de pacotes;
- Suportar scripts de configuração em Python;

Protocolos:

- Implementar o protocolo NTPv3 e NTP v4 (Network Time Protocol, versão 3 e versão 4). Deve ser suportada autenticação entre os peers.
- Implementar DHCP Client, DHCP Relay, DHCP Server em múltiplas VLANs.

Roteamento:

- Implementar roteamento estático.
- Suportar roteamento dinâmico RIPv1 (RFC 1058), RIPv2 (RFC 2453).
- Suportar protocolo de roteamento dinâmico OSPF (RFC 2328, 1587, 1765 e 2370).
- Suportar protocolo de roteamento BGPv4 (RFC 1771, 1965, 1997, 1745, 2385).
- Suportar mecanismo de segurança dos protocolos OSPF e BGP permitindo a autenticação mútua entre peers BGP e OSPF.
- Implementar o roteamento nível 3 entre VLANs.
- Suportar o protocolo VRRP (RFC 2338) de redundância de gateway.
- Suportar a virtualização das tabelas de roteamento camada 3. As tabelas virtuais deverão ser completamente segmentadas.
- Suportar roteamento baseado em origem, com possibilidade de definição do próximo salto camada 3, baseado em uma condição de origem.

Capacidade e Desempenho:

- Possuir capacidade para pelo menos 32.000 endereços MAC na tabela de comutação.
- Implementar, no mínimo, 4000 vlans simultaneamente.
- Implementar, no mínimo, 2000 interfaces vlans (SVIs) simultaneamente, para roteamento nível 3 entre as vlans configuradas.
- Possuir capacidade de comutação de, no mínimo, 256 Gbps (Gigabits por segundo)
- Possuir uma taxa de encaminhamento de no mínimo 190 de Mpps (Milhões de pacotes por segundo).
- Suportar Jumbo frames de, no mínimo, 9198 Bytes.

Empilhamento:

- Possuir porta dedicada de empilhamento com capacidade de 480 Gbps (Gigabits por segundo). Este valor deve ser adicional à capacidade de comutação do switch. Deve ser fornecido um cabo de empilhamento por switch;
- Suportar empilhamento através da porta dedicada, com capacidade de empilhamento de no mínimo 8 switches;
- Suportar atualização automática de versão do sistema operacional dos switches que participam do empilhamento através da porta dedicada.

Segurança:

- Implementar mecanismo de autenticação para acesso local ou remoto ao equipamento baseada em um Servidor de Autenticação/Autorização do tipo TACACS+ e RADIUS.
- Suportar filtragem de pacotes (ACL - Access Control List) para IPv4 e IPv6.
- Proteger a interface de comando do equipamento através de senha.
- Implementar o protocolo SSH V2 para acesso à interface de linha de comando.
- Suportar a criação de listas de acesso baseadas em endereço IP para limitar o acesso ao switch via Telnet, SSH e SNMP. Deve ser possível definir os endereços IP de origem das sessões Telnet e SSH.
- Possibilitar o estabelecimento do número máximo de MACs que podem estar associados a uma dada porta do switch. Deve ser possível bloquear o tráfego excedente e enviar um trap SNMP caso o número de endereços MAC configurados para a porta seja excedido.

- Implementar listas de controle de acesso (ACLs) baseadas em endereço IP de origem e destino, portas TCP e UDP de origem e destino e flags TCP.
- Permitir a associação de um endereço MAC específico a uma dada porta do switch, de modo que somente a estação que tenha tal endereço possa usar a referida porta para conexão.
- Implementar mecanismos de AAA (Authentication, Authorization e Accounting) com garantia de entrega.
- Implementar a criptografia de todos os pacotes enviados ao servidor de controle de acesso e não só os pacotes referentes à senha.
- Permitir controlar e auditar quais comandos os usuários e grupos de usuários podem emitir em cada elementos de rede, independente do método de gerenciamento.
- Possuir suporte a mecanismo de proteção da "Root Bridge" do algoritmo "Spanning-Tree" para defesa contra ataques do tipo "Denial of Service" no ambiente nível 2.
- Possuir suporte à suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta do switch esteja colocada no modo "Fast Forwarding" (conforme previsto no padrão IEEE 802.1w).
- Possuir controle de broadcast, multicast e unicast por porta, podendo definir uma porcentagem limite de banda e pacotes por segundo.
- Possuir análise do protocolo DHCP e permitir que se crie uma tabela de associação entre endereços IP atribuídos dinamicamente, MAC da máquina que recebeu o endereço e porta física do switch em que se localiza tal MAC.
- Possuir método de segurança que utilize uma tabela criada pelo mecanismo de análise do protocolo DHCP, para filtragem de tráfego IP que possua origem diferente do endereço IP atribuido pelo Servidor de DHCP, essa filtragem deve ser por porta.

Padrões:

- Implementar padrão IEEE 802.1d (Spanning Tree Protocol) por VLAN.
- Implementar padrão IEEE 802.1q (Vlan Frame Tagging).
- Implementar padrão IEEE 802.1p (Class of Service) para cada porta.
- Implementar padrão IEEE 802.3ad.
- Implementar o protocolo de negociação Link Aggregation Control Protocol (LACP).
- Implementar padrão IEEE 802.1w (Rapid spanning Tree Protocol).
- Implementar padrão IEEE 802.1s (Multi-Instance Spanning-Tree);
- Os processos de Autenticação, Autorização e Accounting associados a controle de acesso administrativo ao equipamento, TACACS+, devem ser completamente independentes dos processos AAA no contexto 802.1x, RADIUS.
- Implementar controle de acesso por porta, usando o padrão IEEE 802.1x (Port Based Network Access Control). Devem ser atendidos, no mínimo, os seguintes requisitos:

Implementar funcionalidade que designe VLAN específica para o usuário, nos seguintes casos:

A estação não tem cliente 802.1x (suplicante);

As credenciais do usuário não estão corretas (falha de autenticação).

Implementar associação automática de VLAN da porta do switch através da qual o usuário requisitou acesso à rede (Assinalamento de Vlan).

Implementar associação automática de ACL da porta do switch através da qual o usuário requisitou acesso à rede (Downloadable ACL).

Implementar "accounting" das conexões IEEE 802.1x. O switch (cliente AAA) deve ser capaz de enviar, ao servidor AAA, pelo menos as seguintes informações sobre a conexão:

1. Nome do usuário;
2. Switch em que o computador do usuário está conectado;
3. Porta do switch utilizada par acesso;
4. Endereço MAC da máquina utilizada pelo usuário;
5. Endereço IP do usuário; vi. Horários de início e término da conexão;
6. Bytes transmitidos e recebidos durante a conexão.

- Deve ser possível definir, por porta, o intervalo de tempo para obrigar o cliente a se reautenticar (reautenticação periódica).
- Deve ser possível forçar manualmente a reautenticação de um usuário conectado a uma porta do switch habilitada para 802.1x.
- Suportar a autenticação 802.1x via endereço MAC em substituição à identificação de usuário, para equipamentos que não disponham de suplicantes.
- Suportar a configuração de 802.1x utilizando autenticação via usuário e MAC simultaneamente na mesma porta do switch.
- Deve suportar a autenticação 802.1x através do protocolos EAPOL
- Implementar o serviço de DHCP Server em múltiplas VLANS simultaneamente, para que possa atribuir endereços IP aos clientes 802.1x autenticados e autorizados.
- Deve ser suportada a autenticação de múltiplos usuários em uma mesma porta.
- Deve ter tratamento de autenticação 802.1x diferenciado entre “Voice Vlan” e “Data LAN”, na mesma porta para que um erro de autenticação em uma Vlan não interfira na outra.
- Deve ser suportada a atribuição de autenticação através do navegador (Web Authentication) caso a máquina que esteja utilizando para acesso à Rede não tenha cliente 802.1x operacional, o portal de autenticação local do switch deve utilizar protocolo seguro tal como HTTPS.
- Deve implementar o mecanismo mudança de autorização dinamica, Radius “Change of Authorization”, conforme descrito na RFC 5176.
- Deve implementar o padrão IEEE 802.1AE para autenticação e encriptação MACSEc através dos algoritimo 256-bit Advanced Encryption Standard (AES) em todas as portas e velocidades.

Multicast:

- Implementar mecanismo de controle de multicast através de IGMP Snooping de IGMPv1 (RFC 1112), IGMPv2 (RFC 2236) e IGMPv3 (RFC 3376).
- Implementar em todas as interfaces do switch o protocolo IGMP Snooping (v1, v2 e v3), não permitindo que o tráfego multicast seja tratado como broadcast no switch.
- Suportar roteamento multicast PIM (Protocol Independent Multicast) nos modos “sparse- mode” (RFC 2362) e “dense-mode”. Deve ser suportada, por interface, a operação simultânea nos modos “sparse-mode” e “dense mode”.
- Suportar no mínimo 4000 grupos multicast para IPv4.

Qualidade de Serviço (QoS):

- Implementar priorização de tráfego através do protocolo IEEE 802.1p.
- Possuir suporte a uma fila com prioridade estrita (prioridade absoluta em relação às demais classes dentro do limite de banda que lhe foi atribuído) para tratamento do tráfego “real-time” (voz e vídeo).
- Classificação e Reclassificação baseadas em endereço IP de origem/destino, portas TCP e UDP de origem e destino, endereços MAC de origem e destino.
- Classificação, Marcação e Remarcação baseadas em CoS ("Class of Service" - nivel 2) e DSCP ("Differentiated Services Code Point"- nivel 3), conforme definições do IETF (Internet Engineering

Task Force).

- Suportar funcionalidades de QoS de “Traffic Shaping” e “Traffic Policing”.
- Deve ser possível a especificação de banda por classe de serviço.
- Para os pacotes que excederem a especificação, deve ser possível configurar ações tais como:
    1. Transmissão do pacote sem modificação;
    2. Transmissão com remarcação do valor de DSCP;
    3. Descarte do pacote.
- Suportar mapeamento de prioridades nível 2, definidas pelo padrão IEEE 802.1p, em prioridades nível 3 (IETF DSCP – Differentiated Services Code Point definido pela Internet Engineering Task Force) e vice-versa.
- Suporte aos mecanismos de QoS WRR (Weighted Round Robin) ou SRR (Shaped Round Robin).
- Suporte aos mecanismos de QoS WRED (Weighted Random Early Detection) ou WTD (Weighted Tail Drop)
- Implementar pelo menos oito filas de prioridade por porta de saída (egress port).

Internet Protocol Versão 6 (Ipv6):

- Implementar IPv6.
- Permitir a configuração de endereços IPv6 para gerenciamento.
- Permitir consultas de DNS com resolução de nomes em endereços IPv6.
- Implementar ICMPv6 com as seguintes funcionalidades:
    1. ICMP request
    2. ICMP Reply
    3. ICMP Neighbor Discovery Protocol (NDP)
    4. ICMP MTU Discovery"
- Implementar protocolos de gerenciamento Ping, Traceroute, Telnet, SSH, TFTP, SNMP, SYSLOG, HTTP, HTTPS e DNS sobre IPv6.
- Implementar mecanismo de Dual Stack (IPv4 e IPv6), para permitir migração de IPv4 para IPv6.
- Implementar roteamento estático para IPv6.
- Suportar roteamento dinâmico RIPng para IPv6.
- Suportar protocolo de roteamento dinâmico OSPFv3 para IPv6.

9. SWITCH DE DISTRIBUIÇÃO – TIPO IV

Interfaces:

- Possuir 4 portas 10 GbE padrão SFP+ para conexão de uplink;
- Cada equipamento deve ser fornecido com 04 (quatro) Transceivers SFP+ 10G BIDIRECIONAL SHORT REACH MMF;
- Possuir, no mínimo, 48 portas Ethernet 10/100/1000 Base-T com autosensing de velocidade e com conectores RJ-45 para conexão de acesso. Todas as 48 portas devem operar simultaneamente em conjunto com as 2 portas de uplink;
- Todas as portas Ethernet 10/100/1000 devem suportar configuração Half-Duplex (10/100) e Full-Duplex, com a opção de negociação automática;
- As interfaces 10/100/1000 devem obedecer às normas técnicas IEEE 802.3 (10BaseT), IEEE 802.3u (100BaseTX), 802.3ab (1000BaseT) e IEEE 802.3x (Flow Control), além de IEEE 802.3af e 802.3at

(PoE e PoE+);

- Todas as portas Ethernet 10/100/1000 devem suportar autoconfiguração de crossover (Auto MDIX);
- Possuir capacidade de associação das portas de acesso em grupo de, no mínimo, 8 (oito) portas, formando uma única interface lógica com as mesmas facilidades das interfaces originais, compatível com a norma IEEE 802.3ad LACP. Deve ser possível criar pelo menos 24 grupos LACP;
- Possibilitar a configuração dinâmica de portas por software, permitindo a definição de portas ativas/inativas;
- Implementar VLANs por porta;
- Implementar VLANs compatíveis com o padrão IEEE 802.1q;
- Implementar mecanismo de seleção de quais vlans serão permitidas através de trunk 802.1q. Deve ser permitida a configuração dessa seleção de forma dinâmica;
- Possuir porta de console para ligação direta de terminal RS-232 para acesso à interface de linha de comando. Poderá opcionalmente ser fornecida porta de console com interface USB;
- Possuir porta Ethernet 10/100 Base-T dedicada para gerenciamento out-of-band;
- Possuir porta USB compatível com flash drives, para cópias de arquivos de configuração e arquivos de sistema operacional.

Fontes de Alimentação:

- Suportar fonte de alimentação redundante interna AC bivolt, com seleção automática de tensão (na faixa de 100 a 240 Volts) e frequência (de 50/60 Hz). As fontes deverão possuir alimentação independente, a fim de permitir a sua conexão a circuitos elétricos distintos;
- Deve permitir troca da fonte redundante sem interrupção do funcionamento do switch;
- A fonte de alimentação deverá possuir no minimo 437W para alimentação PoE+ (até 30W por porta), além da energia necessária para funcionamento do switch. Não serão aceitos dispositivos externos para complementação de energia PoE no switch;
- Suportar balanceamento de carga entre as fontes de alimentação redundantes, as fontes devem ser dimensionadas para permitir o completo funcionamento do switch com apenas 1 (uma) fonte;
- Permitir o compartilhamento das fontes internas ao equipamento entre diferentes elementos da pilha de switches;
- Deve possuir unidade de ventilação redundante e que permita substituição em caso de falha, sem necessidade de troca do switch.

Dimensões:

- Permitir ser montado em rack padrão de 19 (dezenove) polegadas, incluindo todos os acessórios necessários.
- Deve possuir no máximo 1 Rack Unit (RU).

Visualização:

- Possuir LEDs para a indicação do status das portas e atividade, além do modo duplex.

Gerenciamento:

- O equipamento a ser ofertado deve ser totalmente compatível, e ser fornecido com todas as licenças necessárias para a integração com a PLATAFORMA DE GERENCIAMENTO descrito nesta Especificação Técnica.
- Implementar os padrões abertos de gerência de rede SNMPv1 (RFC 1157), SNMPv2 (RFC 1901 a 1907) e SNMPv3 (RFC 2273 a 2275);
- Implementar pelo menos os seguintes níveis de segurança para SNMP versão 3:

1. Sem autenticação e sem privacidade (noAuthNoPriv);
2. Com autenticação e sem privacidade (authNoPriv);
3. Com autenticação e com privacidade (authPriv) utilizando algoritimo de criptografia AES 256-bit.

- Possibilitar a obtenção da configuração do equipamento através do protocolo SNMP;
- Possuir armazenamento interno das mensagens de log geradas pelo equipamento;
- Possuir capacidade de exportar as mensangens de log geradas pelo equipamento para um servidor syslog externo;
- Permitir o controle da geração de traps SNMP, possibilitando definir quais tipos de alarmes geram traps;
- Implementar nativamente pelo menos 2 grupos RMON (Alarms e Events);
- Implementar os protocolos LLDP (IEEE 802.1AB) e LLDP-MED;
- Suportar a coleta de informações de fluxos Layer 2, IPv4 e IPv6 através de IPFIX ou NetFlow. Deve coletar informações referentes a 100% dos pacotes que trafegam no equipamento.

Facilidades:

- O equipamento a ser ofertado deve implementar gerenciamento orientado a modelo para as funcionalidades de configuração, telemetria, chamadas remotas de procedimentos (RPC) e notificações de eventos de acordo com o padrão YANG (RFC 6020 - YANG - A Data Modeling Language for NETCONF);
- Os Modelos YANG deste equipamento devem estar atualizados para a mesma versão do sistema operacional adotada para a comprovação dos demais requisitos desta especificação. Estes modelos devem estar hospedados em site público que possuam informações de controle de suas versões
- O equipamento a ser ofertado deve implementar, no mínimo, os protocolos de gerenciamento de redes NETCONF (RFC 6241 - Network Configuration Protocol) e gRPC (https://grpc.io/);
- O equipamento a ser ofertado deve implementar, no mínimo, as codificações de dados nos formatos XML (eXtensible Markup Language) e JSON (JavaScript Object Notation);
- O equipamento a ser ofertado deve implementar o método de transporte SSH para o protocolo NETCONF (RFC 4742 ou 6242 - Using the NETCONF Protocol over Secure Shell);
- O equipamento a ser ofertado deve implementar API (Application Programming Interface) modeladas de acordo com o padrão YANG e que implemente os protocolos e as codificações suportadas pela plataforma;
- O equipamento a ser ofertado deve implementar as operações CRUD (Create, Read, Update e Delete) para chamadas via API para modelos YANG abertos e nativos;
- Gerenciável via SSHv2;
- Deve ser gerenciável via SNMP (v1, v2 e v3);
- Implementar o protocolo Syslog para funções de “logging” de eventos;
- Implementar os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps;
- Possuir suporte a MIB II;
- Possibilitar a obtenção da configuração do equipamento através do protocolo SNMP;
- Possibilitar a obtenção via SNMP de informações de capacidade e desempenho da CPU, memória e portas;
- Permitir o controle da geração de traps por porta, possibilitando restringir a geração de traps a portas específicas;
- Implementar nativamente 2 grupos RMON (Alarms e Events);

- Suporte a gerenciamento via CLI, GUI através de interface Web ou da ferramenta de gerenciamento;
- Implementar Telnet e SSH para acesso à interface de linha de comando.
- Permitir a atualização remota do sistema operacional e arquivos de configuração utilizados no equipamento via interfaces ethernet .
- Ser configurável e gerenciável via GUI (graphical user interface), CLI (command line interface), SNMP, Telnet, SSH, HTTP e HTTPS com, no mínimo, 5 sessões simultâneas e independentes.
- Deve permitir a atualização de sistema operacional através do protocolo TFTP ou FTP, e cópia segura e autenticada através de SCP (Secure Copy Protocol).
- Suportar protocolo SSH para gerenciamento remoto, implementando pelo menos o algoritmo de encriptação de dados 3DES.
- Permitir que a sua configuração seja feita através de terminal assíncrono.
- Permitir o armazenamento de sua configuração em memória não volátil, podendo, numa queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior à queda de alimentação.
- Possuir ferramentas para depuração e gerenciamento em primeiro nível, tais como debug, trace, log de eventos.
- Permitir o espelhamento da totalidade do tráfego de uma porta, de um grupo de portas e de VLANs para outra porta localizada no mesmo switch e em outro switch do mesmo tipo conectado à mesma rede local. Deve ser possível definir o sentido do tráfego a ser espelhado: somente tráfego de entrada, somente tráfego de saída e ambos simultaneamente.
- Permitir o espelhamento do tráfego de portas que residem em um dado módulo para uma porta que reside em módulo diferente do switch.
- Devem ser suportadas pelo menos duas sessões simultâneas de espelhamento.
- O espelhamento não pode interferir no funcionamento normal do equipamento
- Deve ser fornecido com documentação técnica e manuais que contenham informações suficientes para possibilitar a instalação, configuração e operacionalização do equipamento.
- Implementar funcionalidade de separação do tráfego de voz e dados em uma mesma porta de acesso (Voice VLAN), sem a necessidade de utilização de 802.1q.
- Deve responder a pacotes para teste da implementação dos níveis de serviço especificados (SLA). Deveram ser suportadas no mínimo as seguintes operações de teste:
    1. ICMP echo;
    2. TCP connect (em qualquer porta TCP do intervalo 1-50000 que o administrador especifique).
    3. UDP echo (em qualquer porta UDP do intervalo 1-50000 que o administrador especifique).
    4. O switch deve suportar pelo menos 5 (cinco) destas operações de testes simultaneamente.
- Permitir a atualização de software sem perda de pacotes;
- Suportar scripts de configuração em Python;

Protocolos:

- Implementar o protocolo NTPv3 e NTP v4 (Network Time Protocol, versão 3 e versão 4). Deve ser suportada autenticação entre os peers.
- Implementar DHCP Client, DHCP Relay, DHCP Server em múltiplas VLANs.

Roteamento:

- Implementar roteamento estático.
- Suportar roteamento dinâmico RIPv1 (RFC 1058), RIPv2 (RFC 2453).

- Suportar protocolo de roteamento dinâmico OSPF (RFC 2328, 1587, 1765 e 2370).
- Suportar protocolo de roteamento BGPv4 (RFC 1771, 1965, 1997, 1745, 2385).
- Suportar mecanismo de segurança dos protocolos OSPF e BGP permitindo a autenticação mútua entre peers BGP e OSPF.
- Implementar o roteamento nível 3 entre VLANs.
- Suportar o protocolo VRRP (RFC 2338) de redundância de gateway.
- Suportar a virtualização das tabelas de roteamento camada 3. As tabelas virtuais deverão ser completamente segmentadas.
- Suportar roteamento baseado em origem, com possibilidade de definição do próximo salto camada 3, baseado em uma condição de origem.

Capacidade e Desempenho:

- Possuir capacidade para pelo menos 32.000 endereços MAC na tabela de comutação.
- Implementar, no mínimo, 4000 vlans simultaneamente.
- Implementar, no mínimo, 2000 interfaces vlans (SVIs) simultaneamente, para roteamento nível 3 entre as vlans configuradas.
- Possuir capacidade de comutação de, no mínimo, 256 Gbps (Gigabits por segundo)
- Possuir uma taxa de encaminhamento de no mínimo 190 de Mpps (Milhões de pacotes por segundo).
- Suportar Jumbo frames de, no mínimo, 9198 Bytes.

Empilhamento:

- Possuir porta dedicada de empilhamento com capacidade de 480 Gbps (Gigabits por segundo). Este valor deve ser adicional à capacidade de comutação do switch. Deve ser fornecido um cabo de empilhamento por switch;
- Suportar empilhamento através da porta dedicada, com capacidade de empilhamento de no mínimo 8 switches;
- Suportar atualização automática de versão do sistema operacional dos switches que participam do empilhamento através da porta dedicada.

Segurança:

- Implementar mecanismo de autenticação para acesso local ou remoto ao equipamento baseada em um Servidor de Autenticação/Autorização do tipo TACACS+ e RADIUS.
- Suportar filtragem de pacotes (ACL - Access Control List) para IPv4 e IPv6.
- Proteger a interface de comando do equipamento através de senha.
- Implementar o protocolo SSH V2 para acesso à interface de linha de comando.
- Suportar a criação de listas de acesso baseadas em endereço IP para limitar o acesso ao switch via Telnet, SSH e SNMP. Deve ser possível definir os endereços IP de origem das sessões Telnet e SSH.
- Possibilitar o estabelecimento do número máximo de MACs que podem estar associados a uma dada porta do switch. Deve ser possível bloquear o tráfego excedente e enviar um trap SNMP caso o número de endereços MAC configurados para a porta seja excedido.
- Implementar listas de controle de acesso (ACLs) baseadas em endereço IP de origem e destino, portas TCP e UDP de origem e destino e flags TCP.
- Permitir a associação de um endereço MAC específico a uma dada porta do switch, de modo que somente a estação que tenha tal endereço possa usar a referida porta para conexão.

- Implementar mecanismos de AAA (Authentication, Authorization e Accounting) com garantia de entrega.
- Implementar a criptografia de todos os pacotes enviados ao servidor de controle de acesso e não só os pacotes referentes à senha.
- Permitir controlar e auditar quais comandos os usuários e grupos de usuários podem emitir em cada elementos de rede, independente do método de gerenciamento.
- Possuir suporte a mecanismo de proteção da "Root Bridge" do algoritmo "Spanning-Tree" para defesa contra ataques do tipo "Denial of Service" no ambiente nível 2.
- Possuir suporte à suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta do switch esteja colocada no modo "Fast Forwarding" (conforme previsto no padrão IEEE 802.1w).
- Possuir controle de broadcast, multicast e unicast por porta, podendo definir uma porcentagem limite de banda e pacotes por segundo.
- Possuir análise do protocolo DHCP e permitir que se crie uma tabela de associação entre endereços IP atribuídos dinamicamente, MAC da máquina que recebeu o endereço e porta física do switch em que se localiza tal MAC.
- Possuir método de segurança que utilize uma tabela criada pelo mecanismo de análise do protocolo DHCP, para filtragem de tráfego IP que possua origem diferente do endereço IP atribuido pelo Servidor de DHCP, essa filtragem deve ser por porta.

Padrões:

- Implementar padrão IEEE 802.1d (Spanning Tree Protocol) por VLAN.
- Implementar padrão IEEE 802.1q (Vlan Frame Tagging).
- Implementar padrão IEEE 802.1p (Class of Service) para cada porta.
- Implementar padrão IEEE 802.3ad.
- Implementar o protocolo de negociação Link Aggregation Control Protocol (LACP).
- Implementar padrão IEEE 802.1w (Rapid spanning Tree Protocol).
- Implementar padrão IEEE 802.1s (Multi-Instance Spanning-Tree);
- Os processos de Autenticação, Autorização e Accounting associados a controle de acesso administrativo ao equipamento, TACACS+, devem ser completamente independentes dos processos AAA no contexto 802.1x, RADIUS.
- Implementar controle de acesso por porta, usando o padrão IEEE 802.1x (Port Based Network Access Control). Devem ser atendidos, no mínimo, os seguintes requisitos:

Implementar funcionalidade que designe VLAN específica para o usuário, nos seguintes casos:

A estação não tem cliente 802.1x (suplicante);

As credenciais do usuário não estão corretas (falha de autenticação).

Implementar associação automática de VLAN da porta do switch através da qual o usuário requisitou acesso à rede (Assinalamento de Vlan).

Implementar associação automática de ACL da porta do switch através da qual o usuário requisitou acesso à rede (Downloadable ACL).

Implementar "accounting" das conexões IEEE 802.1x. O switch (cliente AAA) deve ser capaz de enviar, ao servidor AAA, pelo menos as seguintes informações sobre a conexão:

1. Nome do usuário;
2. Switch em que o computador do usuário está conectado;
3. Porta do switch utilizada par acesso;
4. Endereço MAC da máquina utilizada pelo usuário;

5. Endereço IP do usuário; vi. Horários de início e término da conexão;
6. Bytes transmitidos e recebidos durante a conexão.

- Deve ser possível definir, por porta, o intervalo de tempo para obrigar o cliente a se reautenticar (reautenticação periódica).
- Deve ser possível forçar manualmente a reautenticação de um usuário conectado a uma porta do switch habilitada para 802.1x.
- Suportar a autenticação 802.1x via endereço MAC em substituição à identificação de usuário, para equipamentos que não disponham de suplicantes.
- Suportar a configuração de 802.1x utilizando autenticação via usuário e MAC simultaneamente na mesma porta do switch.
- Deve suportar a autenticação 802.1x através do protocolos EAPOL
- Implementar o serviço de DHCP Server em múltiplas VLANS simultaneamente, para que possa atribuir endereços IP aos clientes 802.1x autenticados e autorizados.
- Deve ser suportada a autenticação de múltiplos usuários em uma mesma porta.
- Deve ter tratamento de autenticação 802.1x diferenciado entre "Voice Vlan" e "Data LAN", na mesma porta para que um erro de autenticação em uma Vlan não interfira na outra.
- Deve ser suportada a atribuição de autenticação através do navegador (Web Authentication) caso a máquina que esteja utilizando para acesso à Rede não tenha cliente 802.1x operacional, o portal de autenticação local do switch deve utilizar protocolo seguro tal como HTTPS.
- Deve implementar o mecanismo mudança de autorização dinamica, Radius "Change of Authorization", conforme descrito na RFC 5176.
- Deve implementar o padrão IEEE 802.1AE para autenticação e encriptação MACSEc através dos algoritimo 256-bit Advanced Encryption Standard (AES) em todas as portas e velocidades.

Multicast:

- Implementar mecanismo de controle de multicast através de IGMP Snooping de IGMPv1 (RFC 1112), IGMPv2 (RFC 2236) e IGMPv3 (RFC 3376).
- Implementar em todas as interfaces do switch o protocolo IGMP Snooping (v1, v2 e v3), não permitindo que o tráfego multicast seja tratado como broadcast no switch.
- Suportar roteamento multicast PIM (Protocol Independent Multicast) nos modos "sparse- mode" (RFC 2362) e "dense-mode". Deve ser suportada, por interface, a operação simultânea nos modos "sparse-mode" e "dense mode".
- Suportar no mínimo 4000 grupos multicast para IPv4.

Qualidade de Serviço (QoS):

- Implementar priorização de tráfego através do protocolo IEEE 802.1p.
- Possuir suporte a uma fila com prioridade estrita (prioridade absoluta em relação às demais classes dentro do limite de banda que lhe foi atribuído) para tratamento do tráfego "real-time" (voz e vídeo).
- Classificação e Reclassificação baseadas em endereço IP de origem/destino, portas TCP e UDP de origem e destino, endereços MAC de origem e destino.
- Classificação, Marcação e Remarcação baseadas em CoS ("Class of Service" - nivel 2) e DSCP ("Differentiated Services Code Point"- nivel 3), conforme definições do IETF (Internet Engineering Task Force).
- Suportar funcionalidades de QoS de "Traffic Shaping" e "Traffic Policing".
- Deve ser possível a especificação de banda por classe de serviço.
- Para os pacotes que excederem a especificação, deve ser possível configurar ações tais como:

1. Transmissão do pacote sem modificação;
2. Transmissão com remarcação do valor de DSCP;
3. Descarte do pacote.

- Suportar mapeamento de prioridades nível 2, definidas pelo padrão IEEE 802.1p, em prioridades nível 3 (IETF DSCP – Differentiated Services Code Point definido pela Internet Engineering Task Force) e vice-versa.
- Suporte aos mecanismos de QoS WRR (Weighted Round Robin) ou SRR (Shaped Round Robin).
- Suporte aos mecanismos de QoS WRED (Weighted Random Early Detection) ou WTD (Weighted Tail Drop)
- Implementar pelo menos oito filas de prioridade por porta de saída (egress port).

Internet Protocol Versão 6 (Ipv6):

- Implementar IPv6.
- Permitir a configuração de endereços IPv6 para gerenciamento.
- Permitir consultas de DNS com resolução de nomes em endereços IPv6.
- Implementar ICMPv6 com as seguintes funcionalidades:
  1. ICMP request
  2. ICMP Reply
  3. ICMP Neighbor Discovery Protocol (NDP)
  4. ICMP MTU Discovery"
- Implementar protocolos de gerenciamento Ping, Traceroute, Telnet, SSH, TFTP, SNMP, SYSLOG, HTTP, HTTPS e DNS sobre IPv6.
- Implementar mecanismo de Dual Stack (IPv4 e IPv6), para permitir migração de IPv4 para IPv6.
- Implementar roteamento estático para IPv6.
- Suportar roteamento dinâmico RIPng para IPv6.
- Suportar protocolo de roteamento dinâmico OSPFv3 para IPv6.

10. SWITCH DE ACESSO – TIPO I

Interfaces:

- Possuir 2 portas 40 GbE padrão QSFP+ para conexão de uplink;
- Cada equipamento deve ser fornecido com 02 (dois) Transceivers QSFP+ 40G BIDIRECIONAL SHORT REACH MMF;
- Possuir, no mínimo, 48 portas Multi-Gigabit Ethernet, sendo:
  1. Ao menos 8 portas 1/5/10 GbE UTP com conectores RJ-45
  2. Ao menos 40 portas 100/1000 UTP com conectores RJ-45
- Todas as 48 portas devem operar simultaneamente em conjunto com as 2 portas de uplink;
- Todas as 48 portas devem implementar o padrão IEEE 802.3af e 802.3at (PoE e PoE+) de forma simultânea;
- Possuir capacidade de associação das portas de acesso em grupo de, no mínimo, 8 (oito) portas, formando uma única interface lógica com as mesmas facilidades das interfaces originais, compatível com a norma IEEE 802.3ad LACP. Deve ser possível criar pelo menos 24 grupos LACP;
- Possibilitar a configuração dinâmica de portas por software, permitindo a definição de portas ativas/inativas;

- Implementar VLANs por porta;
- Implementar VLANs compatíveis com o padrão IEEE 802.1q;
- Implementar mecanismo de seleção de quais vlans serão permitidas através de trunk 802.1q. Deve ser permitida a configuração dessa seleção de forma dinâmica;
- Possuir porta de console para ligação direta de terminal RS-232 para acesso à interface de linha de comando. Poderá opcionalmente ser fornecida porta de console com interface USB;
- Possuir porta Ethernet 10/100 Base-T dedicada para gerenciamento out-of-band;
- Possuir porta USB compatível com flash drives, para cópias de arquivos de configuração e arquivos de sistema operacional.

Fontes de Alimentação:

- Suportar fonte de alimentação redundante interna AC bivolt, com seleção automática de tensão (na faixa de 100 a 240 Volts) e frequência (de 50/60 Hz). As fontes deverão possuir alimentação independente, a fim de permitir a sua conexão a circuitos elétricos distintos;
- Deve permitir troca da fonte redundante sem interrupção do funcionamento do switch;
- A fonte de alimentação deverá possuir no mínimo 740W para alimentação PoE+ (até 30W por porta), além da energia necessária para funcionamento do switch. Não serão aceitos dispositivos externos para complementação de energia PoE no switch;
- Suportar balanceamento de carga entre as fontes de alimentação redundantes, as fontes devem ser dimensionadas para permitir o completo funcionamento do switch com apenas 1 (uma) fonte;
- Permitir o compartilhamento das fontes internas ao equipamento entre diferentes elementos da pilha de switches;
- Deve possuir unidade de ventilação redundante e que permita substituição em caso de falha, sem necessidade de troca do switch.

Dimensões:

- Permitir ser montado em rack padrão de 19 (dezenove) polegadas, incluindo todos os acessórios necessários.
- Deve possuir no máximo 1 Rack Unit (RU).

Visualização:

- Possuir LEDs para a indicação do status das portas e atividade, além do modo duplex.

Gerenciamento:

- O equipamento a ser ofertado deve ser totalmente compatível, e ser fornecido com todas as licenças necessárias para a integração com a PLATAFORMA DE GERENCIAMENTO descrito nesta Especificação Técnica.
- Implementar os padrões abertos de gerência de rede SNMPv1 (RFC 1157), SNMPv2 (RFC 1901 a 1907) e SNMPv3 (RFC 2273 a 2275);
- Implementar pelo menos os seguintes níveis de segurança para SNMP versão 3:
    1. Sem autenticação e sem privacidade (noAuthNoPriv);
    2. Com autenticação e sem privacidade (authNoPriv);
    3. Com autenticação e com privacidade (authPriv) utilizando algoritimo de criptografia AES 256-bit.
- Possibilitar a obtenção da configuração do equipamento através do protocolo SNMP;
- Possuir armazenamento interno das mensagens de log geradas pelo equipamento;

- Possuir capacidade de exportar as mensangens de log geradas pelo equipamento para um servidor syslog externo;
- Permitir o controle da geração de traps SNMP, possibilitando definir quais tipos de alarmes geram traps;
- Implementar nativamente pelo menos 2 grupos RMON (Alarms e Events);
- Implementar os protocolos LLDP (IEEE 802.1AB) e LLDP-MED;
- Suportar a coleta de informações de fluxos Layer 2, IPv4 e IPv6 através de IPFIX ou NetFlow. Deve coletar informações referentes a 100% dos pacotes que trafegam no equipamento.

Facilidades:

- O equipamento a ser ofertado deve implementar gerenciamento orientado a modelo para as funcionalidades de configuração, telemetria, chamadas remotas de procedimentos (RPC) e notificações de eventos de acordo com o padrão YANG (RFC 6020 - YANG - A Data Modeling Language for NETCONF);
- Os Modelos YANG deste equipamento devem estar atualizados para a mesma versão do sistema operacional adotada para a comprovação dos demais requisitos desta especificação. Estes modelos devem estar hospedados em site público que possuam informações de controle de suas versões
- O equipamento a ser ofertado deve implementar, no mínimo, os protocolos de gerenciamento de redes NETCONF (RFC 6241 - Network Configuration Protocol) e gRPC (https://grpc.io/);
- O equipamento a ser ofertado deve implementar, no mínimo, as codificações de dados nos formatos XML (eXtensible Markup Language) e JSON (JavaScript Object Notation);
- O equipamento a ser ofertado deve implementar o método de transporte SSH para o protocolo NETCONF (RFC 4742 ou 6242 - Using the NETCONF Protocol over Secure Shell);
- O equipamento a ser ofertado deve implementar API (Application Programming Interface) modeladas de acordo com o padrão YANG e que implemente os protocolos e as codificações suportadas pela plataforma;
- O equipamento a ser ofertado deve implementar as operações CRUD (Create, Read, Update e Delete) para chamadas via API para modelos YANG abertos e nativos;
- Gerenciável via SSHv2;
- Deve ser gerenciável via SNMP (v1, v2 e v3);
- Implementar o protocolo Syslog para funções de “logging” de eventos;
- Implementar os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps;
- Possuir suporte a MIB II;
- Possibilitar a obtenção da configuração do equipamento através do protocolo SNMP;
- Possibilitar a obtenção via SNMP de informações de capacidade e desempenho da CPU, memória e portas;
- Permitir o controle da geração de traps por porta, possibilitando restringir a geração de traps a portas específicas;
- Implementar nativamente 2 grupos RMON (Alarms e Events);
- Suporte a gerenciamento via CLI, GUI através de interface Web ou da ferramenta de gerenciamento;
- Implementar Telnet e SSH para acesso à interface de linha de comando.
- Permitir a atualização remota do sistema operacional e arquivos de configuração utilizados no equipamento via interfaces ethernet .
- Ser configurável e gerenciável via GUI (graphical user interface), CLI (command line interface), SNMP, Telnet, SSH, HTTP e HTTPS com, no mínimo, 5 sessões simultâneas e independentes.

- Deve permitir a atualização de sistema operacional através do protocolo TFTP ou FTP, e cópia segura e autenticada através de SCP (Secure Copy Protocol).
- Suportar protocolo SSH para gerenciamento remoto, implementando pelo menos o algoritmo de encriptação de dados 3DES.
- Permitir que a sua configuração seja feita através de terminal assíncrono.
- Permitir o armazenamento de sua configuração em memória não volátil, podendo, numa queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior à queda de alimentação.
- Possuir ferramentas para depuração e gerenciamento em primeiro nível, tais como debug, trace, log de eventos.
- Permitir o espelhamento da totalidade do tráfego de uma porta, de um grupo de portas e de VLANs para outra porta localizada no mesmo switch e em outro switch do mesmo tipo conectado à mesma rede local. Deve ser possível definir o sentido do tráfego a ser espelhado: somente tráfego de entrada, somente tráfego de saída e ambos simultaneamente.
- Permitir o espelhamento do tráfego de portas que residem em um dado módulo para uma porta que reside em módulo diferente do switch.
- Devem ser suportadas pelo menos duas sessões simultâneas de espelhamento.
- O espelhamento não pode interferir no funcionamento normal do equipamento
- Deve ser fornecido com documentação técnica e manuais que contenham informações suficientes para possibilitar a instalação, configuração e operacionalização do equipamento.
- Implementar funcionalidade de separação do tráfego de voz e dados em uma mesma porta de acesso (Voice VLAN), sem a necessidade de utilização de 802.1q.
- Deve responder a pacotes para teste da implementação dos níveis de serviço especificados (SLA). Deveram ser suportadas no mínimo as seguintes operações de teste:
    1. ICMP echo;
    2. TCP connect (em qualquer porta TCP do intervalo 1-50000 que o administrador especifique).
    3. UDP echo (em qualquer porta UDP do intervalo 1-50000 que o administrador especifique).
    4. O switch deve suportar pelo menos 5 (cinco) destas operações de testes simultaneamente.
- Permitir a atualização de software sem perda de pacotes;
- Suportar scripts de configuração em Python;

Protocolos:

- Implementar o protocolo NTPv3 e NTP v4 (Network Time Protocol, versão 3 e versão 4). Deve ser suportada autenticação entre os peers.
- Implementar DHCP Client, DHCP Relay, DHCP Server em múltiplas VLANs.

Roteamento:

- Implementar roteamento estático.
- Suportar roteamento dinâmico RIPv1 (RFC 1058), RIPv2 (RFC 2453).
- Suportar protocolo de roteamento dinâmico OSPF (RFC 2328, 1587, 1765 e 2370).
- Suportar protocolo de roteamento BGPv4 (RFC 1771, 1965, 1997, 1745, 2385).
- Suportar mecanismo de segurança dos protocolos OSPF e BGP permitindo a autenticação mútua entre peers BGP e OSPF.
- Implementar o roteamento nível 3 entre VLANs.
- Suportar o protocolo VRRP (RFC 2338) de redundância de gateway.

- Suportar a virtualização das tabelas de roteamento camada 3. As tabelas virtuais deverão ser completamente segmentadas.
- Suportar roteamento baseado em origem, com possibilidade de definição do próximo salto camada 3, baseado em uma condição de origem.

Capacidade e Desempenho:

- Possuir capacidade para pelo menos 32.000 endereços MAC na tabela de comutação.
- Implementar, no mínimo, 1000 vlans simultaneamente.
- Implementar, no mínimo, 1000 interfaces vlans (SVIs) simultaneamente, para roteamento nível 3 entre as vlans configuradas.
- Possuir capacidade de comutação de, no mínimo, 400 Gbps (Gigabits por segundo)
- Possuir uma taxa de encaminhamento de no mínimo 290 de Mpps (Milhões de pacotes por segundo).
- Suportar Jumbo frames de, no mínimo, 9198 Bytes.

Empilhamento:

- Possuir porta dedicada de empilhamento com capacidade de 160 Gbps (Gigabits por segundo). Este valor deve ser adicional à capacidade de comutação do switch. Deve ser fornecido um cabo de empilhamento por switch;
- Suportar empilhamento através da porta dedicada, com capacidade de empilhamento de no mínimo 8 switches;
- Suportar atualização automática de versão do sistema operacional dos switches que participam do empilhamento através da porta dedicada.

Segurança:

- Implementar mecanismo de autenticação para acesso local ou remoto ao equipamento baseada em um Servidor de Autenticação/Autorização do tipo TACACS+ e RADIUS.
- Suportar filtragem de pacotes (ACL - Access Control List) para IPv4 e IPv6.
- Proteger a interface de comando do equipamento através de senha.
- Implementar o protocolo SSH V2 para acesso à interface de linha de comando.
- Suportar a criação de listas de acesso baseadas em endereço IP para limitar o acesso ao switch via Telnet, SSH e SNMP. Deve ser possível definir os endereços IP de origem das sessões Telnet e SSH.
- Possibilitar o estabelecimento do número máximo de MACs que podem estar associados a uma dada porta do switch. Deve ser possível bloquear o tráfego excedente e enviar um trap SNMP caso o número de endereços MAC configurados para a porta seja excedido.
- Implementar listas de controle de acesso (ACLs) baseadas em endereço IP de origem e destino, portas TCP e UDP de origem e destino e flags TCP.
- Permitir a associação de um endereço MAC específico a uma dada porta do switch, de modo que somente a estação que tenha tal endereço possa usar a referida porta para conexão.
- Implementar mecanismos de AAA (Authentication, Authorization e Accounting) com garantia de entrega.
- Implementar a criptografia de todos os pacotes enviados ao servidor de controle de acesso e não só os pacotes referentes à senha.
- Permitir controlar e auditar quais comandos os usuários e grupos de usuários podem emitir em cada elementos de rede, independente do método de gerenciamento.
- Possuir suporte a mecanismo de proteção da “Root Bridge” do algoritmo “Spanning-Tree” para defesa contra ataques do tipo “Denial of Service” no ambiente nível 2.

- Possuir suporte à suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta do switch esteja colocada no modo “Fast Forwarding” (conforme previsto no padrão IEEE 802.1w).
- Possuir controle de broadcast, multicast e unicast por porta, podendo definir uma porcentagem limite de banda e pacotes por segundo.
- Possuir análise do protocolo DHCP e permitir que se crie uma tabela de associação entre endereços IP atribuídos dinamicamente, MAC da máquina que recebeu o endereço e porta física do switch em que se localiza tal MAC.
- Possuir método de segurança que utilize uma tabela criada pelo mecanismo de análise do protocolo DHCP, para filtragem de tráfego IP que possua origem diferente do endereço IP atribuido pelo Servidor de DHCP, essa filtragem deve ser por porta.

Padrões:

- Implementar padrão IEEE 802.1d (Spanning Tree Protocol) por VLAN.
- Implementar padrão IEEE 802.1q (Vlan Frame Tagging).
- Implementar padrão IEEE 802.1p (Class of Service) para cada porta.
- Implementar padrão IEEE 802.3ad.
- Implementar o protocolo de negociação Link Aggregation Control Protocol (LACP).
- Implementar padrão IEEE 802.1w (Rapid spanning Tree Protocol).
- Implementar padrão IEEE 802.1s (Multi-Instance Spanning-Tree);
- Os processos de Autenticação, Autorização e Accounting associados a controle de acesso administrativo ao equipamento, TACACS+, devem ser completamente independentes dos processos AAA no contexto 802.1x, RADIUS.
- Implementar controle de acesso por porta, usando o padrão IEEE 802.1x (Port Based Network Access Control). Devem ser atendidos, no mínimo, os seguintes requisitos:

Implementar funcionalidade que designe VLAN específica para o usuário, nos seguintes casos:

A estação não tem cliente 802.1x (suplicante);

As credenciais do usuário não estão corretas (falha de autenticação).

Implementar associação automática de VLAN da porta do switch através da qual o usuário requisitou acesso à rede (Assinalamento de Vlan).

Implementar associação automática de ACL da porta do switch através da qual o usuário requisitou acesso à rede (Downloadable ACL).

Implementar “accounting” das conexões IEEE 802.1x. O switch (cliente AAA) deve ser capaz de enviar, ao servidor AAA, pelo menos as seguintes informações sobre a conexão:

1. Nome do usuário;
2. Switch em que o computador do usuário está conectado;
3. Porta do switch utilizada par acesso;
4. Endereço MAC da máquina utilizada pelo usuário;
5. Endereço IP do usuário; vi. Horários de início e término da conexão;
6. Bytes transmitidos e recebidos durante a conexão.

- Deve ser possível definir, por porta, o intervalo de tempo para obrigar o cliente a se reautenticar (reautenticação periódica).
- Deve ser possível forçar manualmente a reautenticação de um usuário conectado a uma porta do switch habilitada para 802.1x.

- Suportar a autenticação 802.1x via endereço MAC em substituição à identificação de usuário, para equipamentos que não disponham de suplicantes.
- Suportar a configuração de 802.1x utilizando autenticação via usuário e MAC simultaneamente na mesma porta do switch.
- Deve suportar a autenticação 802.1x através do protocolos EAPOL
- Implementar o serviço de DHCP Server em múltiplas VLANS simultaneamente, para que possa atribuir endereços IP aos clientes 802.1x autenticados e autorizados.
- Deve ser suportada a autenticação de múltiplos usuários em uma mesma porta.
- Deve ter tratamento de autenticação 802.1x diferenciado entre "Voice Vlan" e "Data LAN", na mesma porta para que um erro de autenticação em uma Vlan não interfira na outra.
- Deve ser suportada a atribuição de autenticação através do navegador (Web Authentication) caso a máquina que esteja utilizando para acesso à Rede não tenha cliente 802.1x operacional, o portal de autenticação local do switch deve utilizar protocolo seguro tal como HTTPS.
- Deve implementar o mecanismo mudança de autorização dinamica, Radius "Change of Authorization", conforme descrito na RFC 5176.
- Deve implementar o padrão IEEE 802.1AE para autenticação e encriptação MACSEc através dos algoritimo 256-bit Advanced Encryption Standard (AES) em todas as portas e velocidades.

Multicast:

- Implementar mecanismo de controle de multicast através de IGMP Snooping de IGMPv1 (RFC 1112), IGMPv2 (RFC 2236) e IGMPv3 (RFC 3376).
- Implementar em todas as interfaces do switch o protocolo IGMP Snooping (v1, v2 e v3), não permitindo que o tráfego multicast seja tratado como broadcast no switch.
- Suportar roteamento multicast PIM (Protocol Independent Multicast) nos modos "sparse- mode" (RFC 2362) e "dense-mode". Deve ser suportada, por interface, a operação simultânea nos modos "sparse-mode" e "dense mode".
- Suportar no mínimo 4000 grupos multicast para IPv4.

Qualidade de Serviço (QoS):

- Implementar priorização de tráfego através do protocolo IEEE 802.1p.
- Possuir suporte a uma fila com prioridade estrita (prioridade absoluta em relação às demais classes dentro do limite de banda que lhe foi atribuído) para tratamento do tráfego "real-time" (voz e vídeo).
- Classificação e Reclassificação baseadas em endereço IP de origem/destino, portas TCP e UDP de origem e destino, endereços MAC de origem e destino.
- Classificação, Marcação e Remarcação baseadas em CoS ("Class of Service" - nivel 2) e DSCP ("Differentiated Services Code Point"- nivel 3), conforme definições do IETF (Internet Engineering Task Force).
- Suportar funcionalidades de QoS de "Traffic Shaping" e "Traffic Policing".
- Deve ser possível a especificação de banda por classe de serviço.
- Para os pacotes que excederem a especificação, deve ser possível configurar ações tais como:
    1. Transmissão do pacote sem modificação;
    2. Transmissão com remarcação do valor de DSCP;
    3. Descarte do pacote.
- Suportar mapeamento de prioridades nível 2, definidas pelo padrão IEEE 802.1p, em prioridades nível 3 (IETF DSCP – Differentiated Services Code Point definido pela Internet Engineering Task Force) e vice-versa.

- Suporte aos mecanismos de QoS WRR (Weighted Round Robin) ou SRR (Shaped Round Robin).
- Suporte aos mecanismos de QoS WRED (Weighted Random Early Detection) ou WTD (Weighted Tail Drop)
- Implementar pelo menos oito filas de prioridade por porta de saída (egress port).

Internet Protocol Versão 6 (Ipv6):

- Implementar IPv6.
- Permitir a configuração de endereços IPv6 para gerenciamento.
- Permitir consultas de DNS com resolução de nomes em endereços IPv6.
- Implementar ICMPv6 com as seguintes funcionalidades:
    1. ICMP request
    2. ICMP Reply
    3. ICMP Neighbor Discovery Protocol (NDP)
    4. ICMP MTU Discovery"
- Implementar protocolos de gerenciamento Ping, Traceroute, Telnet, SSH, TFTP, SNMP, SYSLOG, HTTP, HTTPS e DNS sobre IPv6.
- Implementar mecanismo de Dual Stack (IPv4 e IPv6), para permitir migração de IPv4 para IPv6.
- Implementar roteamento estático para IPv6.
- Suportar roteamento dinâmico RIPng para IPv6.
- Suportar protocolo de roteamento dinâmico OSPFv3 para IPv6.

11. SWITCH DE ACESSO – TIPO II

Interfaces:

- Possuir 4 portas 1/10 GbE padrão SFP+ para conexão de uplink;
- Cada equipamento deve ser fornecido com 04 (quatro) Transceivers SFP+ 10G BIDIRECIONAL SHORT REACH MMF;
- Possuir, no mínimo, 48 portas Ethernet 10/100/1000 Base-T com autosensing de velocidade e com conectores RJ-45 para conexão de acesso. Todas as 48 portas devem operar simultaneamente em conjunto com as 2 portas de uplink;
- Todas as portas Ethernet 10/100/1000 devem suportar configuração Half-Duplex (10/100) e Full-Duplex, com a opção de negociação automática;
- As interfaces 10/100/1000 devem obedecer às normas técnicas IEEE 802.3 (10BaseT), IEEE 802.3u (100BaseTX), 802.3ab (1000BaseT) e IEEE 802.3x (Flow Control), além de IEEE 802.3af e 802.3at (PoE e PoE+);
- Todas as portas Ethernet 10/100/1000 devem suportar autoconfiguração de crossover (Auto MDIX);
- Possuir capacidade de associação das portas de acesso em grupo de, no mínimo, 8 (oito) portas, formando uma única interface lógica com as mesmas facilidades das interfaces originais, compatível com a norma IEEE 802.3ad LACP. Deve ser possível criar pelo menos 24 grupos LACP;
- Possibilitar a configuração dinâmica de portas por software, permitindo a definição de portas ativas/inativas;
- Implementar VLANs por porta;
- Implementar VLANs compatíveis com o padrão IEEE 802.1q;
- Implementar mecanismo de seleção de quais vlans serão permitidas através de trunk 802.1q. Deve ser permitida a configuração dessa seleção de forma dinâmica;

- Possuir porta de console para ligação direta de terminal RS-232 para acesso à interface de linha de comando. Poderá opcionalmente ser fornecida porta de console com interface USB;
- Possuir porta Ethernet 10/100 Base-T dedicada para gerenciamento out-of-band;
- Possuir porta USB compatível com flash drives, para cópias de arquivos de configuração e arquivos de sistema operacional.

Fontes de Alimentação:

- Suportar fonte de alimentação redundante interna AC bivolt, com seleção automática de tensão (na faixa de 100 a 240 Volts) e frequência (de 50/60 Hz). As fontes deverão possuir alimentação independente, a fim de permitir a sua conexão a circuitos elétricos distintos;
- Deve permitir troca da fonte redundante sem interrupção do funcionamento do switch;
- A fonte de alimentação deverá possuir no minimo 740W para alimentação PoE+ (até 30W por porta), além da energia necessária para funcionamento do switch. Não serão aceitos dispositivos externos para complementação de energia PoE no switch;
- Suportar balanceamento de carga entre as fontes de alimentação redundantes, as fontes devem ser dimensionadas para permitir o completo funcionamento do switch com apenas 1 (uma) fonte;
- Permitir o compartilhamento das fontes internas ao equipamento entre diferentes elementos da pilha de switches;
- Deve possuir unidade de ventilação redundante e que permita substituição em caso de falha, sem necessidade de troca do switch.

Dimensões:

- Permitir ser montado em rack padrão de 19 (dezenove) polegadas, incluindo todos os acessórios necessários.
- Deve possuir no máximo 1 Rack Unit (RU).

Visualização:

- Possuir LEDs para a indicação do status das portas e atividade, além do modo duplex.

Gerenciamento:

- O equipamento a ser ofertado deve ser totalmente compatível, e ser fornecido com todas as licenças necessárias para a integração com a PLATAFORMA DE GERENCIAMENTO descrito nesta Especificação Técnica.
- Implementar os padrões abertos de gerência de rede SNMPv1 (RFC 1157), SNMPv2 (RFC 1901 a 1907) e SNMPv3 (RFC 2273 a 2275);
- Implementar pelo menos os seguintes níveis de segurança para SNMP versão 3:
    1. Sem autenticação e sem privacidade (noAuthNoPriv);
    2. Com autenticação e sem privacidade (authNoPriv);
    3. Com autenticação e com privacidade (authPriv) utilizando algoritimo de criptografia AES 256-bit.
- Possibilitar a obtenção da configuração do equipamento através do protocolo SNMP;
- Possuir armazenamento interno das mensagens de log geradas pelo equipamento;
- Possuir capacidade de exportar as mensangens de log geradas pelo equipamento para um servidor syslog externo;
- Permitir o controle da geração de traps SNMP, possibilitando definir quais tipos de alarmes geram traps;
- Implementar nativamente pelo menos 2 grupos RMON (Alarms e Events);

- Implementar os protocolos LLDP (IEEE 802.1AB) e LLDP-MED;
- Suportar a coleta de informações de fluxos Layer 2, IPv4 e IPv6 através de IPFIX ou NetFlow. Deve coletar informações referentes a 100% dos pacotes que trafegam no equipamento.

Facilidades:

- O equipamento a ser ofertado deve implementar gerenciamento orientado a modelo para as funcionalidades de configuração, telemetria, chamadas remotas de procedimentos (RPC) e notificações de eventos de acordo com o padrão YANG (RFC 6020 - YANG - A Data Modeling Language for NETCONF);
- Os Modelos YANG deste equipamento devem estar atualizados para a mesma versão do sistema operacional adotada para a comprovação dos demais requisitos desta especificação. Estes modelos devem estar hospedados em site público que possuam informações de controle de suas versões
- O equipamento a ser ofertado deve implementar, no mínimo, os protocolos de gerenciamento de redes NETCONF (RFC 6241 - Network Configuration Protocol) e gRPC (https://grpc.io/);
- O equipamento a ser ofertado deve implementar, no mínimo, as codificações de dados nos formatos XML (eXtensible Markup Language) e JSON (JavaScript Object Notation);
- O equipamento a ser ofertado deve implementar o método de transporte SSH para o protocolo NETCONF (RFC 4742 ou 6242 - Using the NETCONF Protocol over Secure Shell);
- O equipamento a ser ofertado deve implementar API (Application Programming Interface) modeladas de acordo com o padrão YANG e que implemente os protocolos e as codificações suportadas pela plataforma;
- O equipamento a ser ofertado deve implementar as operações CRUD (Create, Read, Update e Delete) para chamadas via API para modelos YANG abertos e nativos;
- Gerenciável via SSHv2;
- Deve ser gerenciável via SNMP (v1, v2 e v3);
- Implementar o protocolo Syslog para funções de “logging” de eventos;
- Implementar os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps;
- Possuir suporte a MIB II;
- Possibilitar a obtenção da configuração do equipamento através do protocolo SNMP;
- Possibilitar a obtenção via SNMP de informações de capacidade e desempenho da CPU, memória e portas;
- Permitir o controle da geração de traps por porta, possibilitando restringir a geração de traps a portas específicas;
- Implementar nativamente 2 grupos RMON (Alarms e Events);
- Suporte a gerenciamento via CLI, GUI através de interface Web ou da ferramenta de gerenciamento;
- Implementar Telnet e SSH para acesso à interface de linha de comando.
- Permitir a atualização remota do sistema operacional e arquivos de configuração utilizados no equipamento via interfaces ethernet .
- Ser configurável e gerenciável via GUI (graphical user interface), CLI (command line interface), SNMP, Telnet, SSH, HTTP e HTTPS com, no mínimo, 5 sessões simultâneas e independentes.
- Deve permitir a atualização de sistema operacional através do protocolo TFTP ou FTP, e cópia segura e autenticada através de SCP (Secure Copy Protocol).
- Suportar protocolo SSH para gerenciamento remoto, implementando pelo menos o algoritmo de encriptação de dados 3DES.
- Permitir que a sua configuração seja feita através de terminal assíncrono.

- Permitir o armazenamento de sua configuração em memória não volátil, podendo, numa queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior à queda de alimentação.
- Possuir ferramentas para depuração e gerenciamento em primeiro nível, tais como debug, trace, log de eventos.
- Permitir o espelhamento da totalidade do tráfego de uma porta, de um grupo de portas e de VLANs para outra porta localizada no mesmo switch e em outro switch do mesmo tipo conectado à mesma rede local. Deve ser possível definir o sentido do tráfego a ser espelhado: somente tráfego de entrada, somente tráfego de saída e ambos simultaneamente.
- Permitir o espelhamento do tráfego de portas que residem em um dado módulo para uma porta que reside em módulo diferente do switch.
- Devem ser suportadas pelo menos duas sessões simultâneas de espelhamento.
- O espelhamento não pode interferir no funcionamento normal do equipamento
- Deve ser fornecido com documentação técnica e manuais que contenham informações suficientes para possibilitar a instalação, configuração e operacionalização do equipamento.
- Implementar funcionalidade de separação do tráfego de voz e dados em uma mesma porta de acesso (Voice VLAN), sem a necessidade de utilização de 802.1q.
- Deve responder a pacotes para teste da implementação dos níveis de serviço especificados (SLA). Deveram ser suportadas no mínimo as seguintes operações de teste:
    1. ICMP echo;
    2. TCP connect (em qualquer porta TCP do intervalo 1-50000 que o administrador especifique).
    3. UDP echo (em qualquer porta UDP do intervalo 1-50000 que o administrador especifique).
    4. O switch deve suportar pelo menos 5 (cinco) destas operações de testes simultaneamente.
- Permitir a atualização de software sem perda de pacotes;
- Suportar scripts de configuração em Python;

Protocolos:

- Implementar o protocolo NTPv3 e NTP v4 (Network Time Protocol, versão 3 e versão 4). Deve ser suportada autenticação entre os peers.
- Implementar DHCP Client, DHCP Relay, DHCP Server em múltiplas VLANs.

Roteamento:

- Implementar roteamento estático.
- Suportar roteamento dinâmico RIPv1 (RFC 1058), RIPv2 (RFC 2453).
- Suportar protocolo de roteamento dinâmico OSPF (RFC 2328, 1587, 1765 e 2370).
- Suportar protocolo de roteamento BGPv4 (RFC 1771, 1965, 1997, 1745, 2385).
- Suportar mecanismo de segurança dos protocolos OSPF e BGP permitindo a autenticação mútua entre peers BGP e OSPF.
- Implementar o roteamento nível 3 entre VLANs.
- Suportar o protocolo VRRP (RFC 2338) de redundância de gateway.
- Suportar a virtualização das tabelas de roteamento camada 3. As tabelas virtuais deverão ser completamente segmentadas.
- Suportar roteamento baseado em origem, com possibilidade de definição do próximo salto camada 3, baseado em uma condição de origem.

Capacidade e Desempenho:

- Possuir capacidade para pelo menos 16.000 endereços MAC na tabela de comutação.
- Implementar, no mínimo, 1000 vlans simultaneamente.
- Implementar, no mínimo, 1000 interfaces vlans (SVIs) simultaneamente, para roteamento nível 3 entre as vlans configuradas.
- Possuir capacidade de comutação de, no mínimo, 176 Gbps (Gigabits por segundo)
- Possuir uma taxa de encaminhamento de no mínimo, 130 Mpps (Milhões de pacotes por segundo).
- Suportar Jumbo frames de, no mínimo, 9198 Bytes.

Empilhamento:

- Possuir porta dedicada de empilhamento com capacidade de 80 Gbps (Gigabits por segundo). Este valor deve ser adicional à capacidade de comutação do switch. Deve ser fornecido um cabo de empilhamento por switch;
- Suportar empilhamento através da porta dedicada, com capacidade de empilhamento de no mínimo 8 switches;
- Suportar atualização automática de versão do sistema operacional dos switches que participam do empilhamento através da porta dedicada.

Segurança:

- Implementar mecanismo de autenticação para acesso local ou remoto ao equipamento baseada em um Servidor de Autenticação/Autorização do tipo TACACS+ e RADIUS.
- Suportar filtragem de pacotes (ACL - Access Control List) para IPv4 e IPv6.
- Proteger a interface de comando do equipamento através de senha.
- Implementar o protocolo SSH V2 para acesso à interface de linha de comando.
- Suportar a criação de listas de acesso baseadas em endereço IP para limitar o acesso ao switch via Telnet, SSH e SNMP. Deve ser possível definir os endereços IP de origem das sessões Telnet e SSH.
- Possibilitar o estabelecimento do número máximo de MACs que podem estar associados a uma dada porta do switch. Deve ser possível bloquear o tráfego excedente e enviar um trap SNMP caso o número de endereços MAC configurados para a porta seja excedido.
- Implementar listas de controle de acesso (ACLs) baseadas em endereço IP de origem e destino, portas TCP e UDP de origem e destino e flags TCP.
- Permitir a associação de um endereço MAC específico a uma dada porta do switch, de modo que somente a estação que tenha tal endereço possa usar a referida porta para conexão.
- Implementar mecanismos de AAA (Authentication, Authorization e Accounting) com garantia de entrega.
- Implementar a criptografia de todos os pacotes enviados ao servidor de controle de acesso e não só os pacotes referentes à senha.
- Permitir controlar e auditar quais comandos os usuários e grupos de usuários podem emitir em cada elementos de rede, independente do método de gerenciamento.
- Possuir suporte a mecanismo de proteção da “Root Bridge” do algoritmo “Spanning-Tree” para defesa contra ataques do tipo “Denial of Service” no ambiente nível 2.
- Possuir suporte à suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta do switch esteja colocada no modo “Fast Forwarding” (conforme previsto no padrão IEEE 802.1w).
- Possuir controle de broadcast, multicast e unicast por porta, podendo definir uma porcentagem limite de banda e pacotes por segundo.
- Possuir análise do protocolo DHCP e permitir que se crie uma tabela de associação entre endereços IP atribuídos dinamicamente, MAC da máquina que recebeu o endereço e porta física do switch em que se localiza tal MAC.

- Possuir método de segurança que utilize uma tabela criada pelo mecanismo de análise do protocolo DHCP, para filtragem de tráfego IP que possua origem diferente do endereço IP atribuido pelo Servidor de DHCP, essa filtragem deve ser por porta.

Padrões:

- Implementar padrão IEEE 802.1d (Spanning Tree Protocol) por VLAN.
- Implementar padrão IEEE 802.1q (Vlan Frame Tagging).
- Implementar padrão IEEE 802.1p (Class of Service) para cada porta.
- Implementar padrão IEEE 802.3ad.
- Implementar o protocolo de negociação Link Aggregation Control Protocol (LACP).
- Implementar padrão IEEE 802.1w (Rapid spanning Tree Protocol).
- Implementar padrão IEEE 802.1s (Multi-Instance Spanning-Tree);
- Os processos de Autenticação, Autorização e Accounting associados a controle de acesso administrativo ao equipamento, TACACS+, devem ser completamente independentes dos processos AAA no contexto 802.1x, RADIUS.
- Implementar controle de acesso por porta, usando o padrão IEEE 802.1x (Port Based Network Access Control). Devem ser atendidos, no mínimo, os seguintes requisitos:

Implementar funcionalidade que designe VLAN específica para o usuário, nos seguintes casos:

A estação não tem cliente 802.1x (suplicante);

As credenciais do usuário não estão corretas (falha de autenticação).

Implementar associação automática de VLAN da porta do switch através da qual o usuário requisitou acesso à rede (Assinalamento de Vlan).

Implementar associação automática de ACL da porta do switch através da qual o usuário requisitou acesso à rede (Downloadable ACL).

Implementar “accounting” das conexões IEEE 802.1x. O switch (cliente AAA) deve ser capaz de enviar, ao servidor AAA, pelo menos as seguintes informações sobre a conexão:

1. Nome do usuário;
2. Switch em que o computador do usuário está conectado;
3. Porta do switch utilizada par acesso;
4. Endereço MAC da máquina utilizada pelo usuário;
5. Endereço IP do usuário; vi. Horários de início e término da conexão;
6. Bytes transmitidos e recebidos durante a conexão.

- Deve ser possível definir, por porta, o intervalo de tempo para obrigar o cliente a se reautenticar (reautenticação periódica).
- Deve ser possível forçar manualmente a reautenticação de um usuário conectado a uma porta do switch habilitada para 802.1x.
- Suportar a autenticação 802.1x via endereço MAC em substituição à identificação de usuário, para equipamentos que não disponham de suplicantes.
- Suportar a configuração de 802.1x utilizando autenticação via usuário e MAC simultaneamente na mesma porta do switch.
- Deve suportar a autenticação 802.1x através do protocolos EAPOL
- Implementar o serviço de DHCP Server em múltiplas VLANS simultaneamente, para que possa atribuir endereços IP aos clientes 802.1x autenticados e autorizados.
- Deve ser suportada a autenticação de múltiplos usuários em uma mesma porta.

- Deve ter tratamento de autenticação 802.1x diferenciado entre “Voice Vlan” e “Data LAN”, na mesma porta para que um erro de autenticação em uma Vlan não interfira na outra.
- Deve ser suportada a atribuição de autenticação através do navegador (Web Authentication) caso a máquina que esteja utilizando para acesso à Rede não tenha cliente 802.1x operacional, o portal de autenticação local do switch deve utilizar protocolo seguro tal como HTTPS.
- Deve implementar o mecanismo mudança de autorização dinamica, Radius “Change of Authorization”, conforme descrito na RFC 5176.
- Deve implementar o padrão IEEE 802.1AE para autenticação e encriptação MACSEc através dos algoritimo 256-bit Advanced Encryption Standard (AES) em todas as portas e velocidades.

Multicast:

- Implementar mecanismo de controle de multicast através de IGMP Snooping de IGMPv1 (RFC 1112), IGMPv2 (RFC 2236) e IGMPv3 (RFC 3376).
- Implementar em todas as interfaces do switch o protocolo IGMP Snooping (v1, v2 e v3), não permitindo que o tráfego multicast seja tratado como broadcast no switch.
- Suportar roteamento multicast PIM (Protocol Independent Multicast) nos modos “sparse- mode” (RFC 2362) e “dense-mode”. Deve ser suportada, por interface, a operação simultânea nos modos “sparse-mode” e “dense mode”.
- Suportar no mínimo 4000 grupos multicast para IPv4.

Qualidade de Serviço (QoS):

- Implementar priorização de tráfego através do protocolo IEEE 802.1p.
- Possuir suporte a uma fila com prioridade estrita (prioridade absoluta em relação às demais classes dentro do limite de banda que lhe foi atribuído) para tratamento do tráfego “real-time” (voz e vídeo).
- Classificação e Reclassificação baseadas em endereço IP de origem/destino, portas TCP e UDP de origem e destino, endereços MAC de origem e destino.
- Classificação, Marcação e Remarcação baseadas em CoS ("Class of Service" - nivel 2) e DSCP ("Differentiated Services Code Point"- nivel 3), conforme definições do IETF (Internet Engineering Task Force).
- Suportar funcionalidades de QoS de “Traffic Shaping” e “Traffic Policing”.
- Deve ser possível a especificação de banda por classe de serviço.
- Para os pacotes que excederem a especificação, deve ser possível configurar ações tais como:
    1. Transmissão do pacote sem modificação;
    2. Transmissão com remarcação do valor de DSCP;
    3. Descarte do pacote.
- Suportar mapeamento de prioridades nível 2, definidas pelo padrão IEEE 802.1p, em prioridades nível 3 (IETF DSCP – Differentiated Services Code Point definido pela Internet Engineering Task Force) e vice-versa.
- Suporte aos mecanismos de QoS WRR (Weighted Round Robin) ou SRR (Shaped Round Robin).
- Suporte aos mecanismos de QoS WRED (Weighted Random Early Detection) ou WTD (Weighted Tail Drop)
- Implementar pelo menos oito filas de prioridade por porta de saída (egress port).

Internet Protocol Versão 6 (Ipv6):

- Implementar IPv6.
- Permitir a configuração de endereços IPv6 para gerenciamento.

- Permitir consultas de DNS com resolução de nomes em endereços IPv6.
- Implementar ICMPv6 com as seguintes funcionalidades:
    1. ICMP request
    2. ICMP Reply
    3. ICMP Neighbor Discovery Protocol (NDP)
    4. ICMP MTU Discovery"
- Implementar protocolos de gerenciamento Ping, Traceroute, Telnet, SSH, TFTP, SNMP, SYSLOG, HTTP, HTTPS e DNS sobre IPv6.
- Implementar mecanismo de Dual Stack (IPv4 e IPv6), para permitir migração de IPv4 para IPv6.
- Implementar roteamento estático para IPv6.
- Suportar roteamento dinâmico RIPng para IPv6.
- Suportar protocolo de roteamento dinâmico OSPFv3 para IPv6.

12. CONTROLADORA WIRELESS LAN

Caracteristicas

- A controladora WLAN deve ser capaz de controlar, no mínimo, 1500 (um mil e quinhentos) pontos de acesso nos padrões IEEE 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac Wave 1 e Wave 2, 802.11ax;
- Os controladores da rede sem fio poderão ser do tipo virtual appliances ou physical appliances (com software e hardware integrados pelo mesmo fabricante da solução de WLAN);
- No caso da solução ser fornecida como virtual appliance, a mesma deve ser acompanhada dos seguintes recursos:
- Deve ser fornecido o hardware com recursos computacionais (Disco Rigido, Processador, Memória RAM e Interfaces de Rede) necessários para atender aos itens desta Especificação Técnica em sua capacidade máxima.
- Deve ser fornecida com o sistema de virtualização devidamente licenciado, sendo permitido a utilização dos seguintes sistemas de virtualização:
    1. VMware ESXi;
    2. KVM;
    3. Microsoft Hyper-V;
- Deverá ser fornecida com licenças para controlar 50 (cinquenta) pontos de acesso, devendo permitir upgrade desta capacidade somente com adição de licenças;
- Deverá estar licenciado para todas as funcionalidades exigidas nesta especificação;
- Suportar, no mínimo, 30.000 (trinta mil) usuários simultâneos;
- Deverá ter throughput mínimo de 5 Gbps;
- No caso da solução ser fornecida como physical appliance, a mesma deve ser acompanhada dos seguintes recursos:
    1. Duir LED que indique, no mínimo, as seguintes condições:

Estado de operação;

Atividade das portas;

Estado dos ventiladores;

Estado da Temperatura;

Estado das fontes de alimentação.

- Permitir que seja instalado em um rack de 19 polegadas, incluindo todos os acessórios necessários;
- Deverá possuir fontes e ventiladores redundantes.
- Implementar criptografia do tráfego de dados e controle, na comunicação entre APs e controladora;
- Deve possuir funcionalidade que permita a utilização dos APs em sites remotos, onde através de conexão pela internet este automaticamente estabeleça um túnel seguro até o controlador permitindo que os SSIDs corporativos sejam disponibilizados aos usuários. Deverá também permitir a criação de um SSID local, que efetue a conexão direta via internet, sem a utilização do túnel seguro. Caso esta funcionalidade necessite de licenças adicionais, estas deverão estar contempladas para totalidade da capacidade do controlador.

1. Deverá suportar no mínimo os seguintes modos de operação dos Pontos de Acessos:
    1. Centralizado;
    2. Local.
2. A rede Wifi local não pode se tornar inoperante devido à ocorrência de qualquer uma das 03 (três) falhas isoladas ou simultâneas listadas a seguir:
    1. Falha no controlador Wifi;
    2. Falha no Sistema de Autenticação Centralizado;
    3. Falha no link de comunicação entre os pontos de acesso e o controlador (WAN ou LAN).
    4. Deverá também, na ocorrência de inoperância, de acordo com o item anterior, deve continuar operando e permitir:
    5. Que os usuários já autenticados na rede e associados aos pontos de acesso continuem a possuir acesso à rede. Deve permitir que os usuários efetuem roaming entre os pontos de acesso do mesmo site nesta situação;
    6. Que novos usuários se autentiquem de acordo com 802.1x e se associem à rede sem qualquer prejuízo de acesso aos mesmos;

- No caso de falha do Sistema de Autenticação, deverá permitir a criação de de uma base de usuários interna ao ponto de acesso, para que os usuários sejam autenticados através de 802.11x;
- O controlador WLAN deve permitir uma topologia redundante “N+1”, permitindo escalabilidade e alta disponibilidade. No caso de falha do Controlador WLAN, os Pontos de Acesso relacionados deverão se associar a um controlador WLAN alternativo de forma automática. O controlador redundante poderá estar em uma rede IP diferente;
- O equipamento deve também ser capaz de operar em topologia do tipo “1+1”, onde temos um equipamento ativos e um segundo redundante, com outro equipamento do mesmo tipo. Neste tipo de topologia, para redução no tempo de indisponibilidade dos serviços, deve ser implementada persistência de sessão entre APs e as controladoras ativa e standby, resultando na comutação entre controladoras com no máximo 1 (um) segundo de tempo de interrupção do serviço. Também é garantida a sincronização automática de configurações estre a controladora ativa e a redundante. O controlador WiFi “redundante” poderá estar fisicamente em outro local desde que estes estejam em uma mesma rede IP;
- Quando operando em uma topologia do tipo “1+1”, para que não exista interrupção no serviço prestada aos clientes, as sessões dos usuários devem ser também sincronizadas entre os controladores em alta disponibilidade;
- Deverá ser fornecido 1 (um) par de controladores, com as mesmas características e componentes de hardware, em topologia “1+1” e totalmente licenciada para esta funcionalidade.
- Permitir que os eventos sejam gravados remotamente utilizando syslog;
- Permitir armazenamento de sua configuração em memória não volátil, podendo, numa queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração

anterior à queda de alimentação;

- Implementar os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps;
- Possui suporte a MIB II, conforme RFC 1213;
- Possuir suporte a Network Configuration Protocol (NETCONF), conforme RFC 6241;
- Possuir suporte a NETCONF over SSH, conforme RFC 6242;
- Possuir suporte a NETCONF Event Notification, conforme RFC 5277;
- Possuir suporte ao padrão YANG, conforme RFC 6020
- Possuir suporte a Partial Lock Remote Procedure Call, conforme RFC 5717
- Possibilitar a obtenção da configuração lógica e física do equipamento através do protocolo SNMP;
- Possibilitar a obtenção via SNMP de, no mínimo, informações de capacidade e desempenho da CPU, memória e portas;
- Deve ser capaz de controlar Pontos de Acesso nos padrões 802.11a/b/g/n/ac wave 1 e wave 2/ax simultaneamente;
- Deve atender aos padrões IEEE 802.11d e 802.11h;
- Deve possuir capacidade instalada para controlar pontos de acesso “indoor” e “outdoor”, simultaneamente, sem que seja necessária qualquer licença adicional às fornecidas, permitindo ainda criação de redes Mesh (“indoor e outdoor”);
- Deve implementar o protocolo IEEE 802.1X, com pelo menos os seguintes métodos EAP:
    1. EAP-Transport Layer Security (EAP-TLS);
    2. EAP-TTLS/MSCHAPv2;
    3. PEAPv0/EAP-MSCHAPv2;
    4. PEAPv1/EAP-GTC;
    5. EAP-FAST,
    6. EAP Subscriber Identity Module (EAP-SIM).
- Deve suportar a autenticação com geração dinâmica de chaves criptográficas por sessão e por usuário;
- Deve possuir, quando utilizando Pontos de Acessos específicos, capacidade para classificar e mitigar interferências não WiFi que impactem diretamente no funcionamento da rede em menos de 1 minuto;
- Deve detectar, classificar e mitigar interferências não WiFi, com no mínimo 15 fontes de interferência que impactem diretamente no funcionamento da rede, em menos de 60 segundos. Caso esta funcionalidade necessite de licenças adicionai, estas deverão estar contempladas para totalidade da capacidade exigida.
- Dever suportar WPA com algoritmo de criptografia TKIP;
- Deve implementar WPA-2 (Wi-Fi Protected Access) com algoritmo de criptografia AES;
- Deve implementar o padrão IEEE 802.11i;
- Possibilitar roaming com integridade de sessão, dando suporte à aplicações em tempo real, tais como, VoIP, VoWLAN, videoconferência, dentre outras;
- Deve implementar roaming rápido para os usuários autenticados por 802.1X (Fast Secure Roaming). O roaming de um cliente autenticado entre dois Pontos de Acesso deve ser inferior à 150 ms (milisegundos);
- Deve ser fornecida com recursos instalados para implementar mecanismo de autenticação através de portal Web (Captive Portal) para usuários visitantes;

- Deve permitir a criação de um usuário especial para gerenciamento de usuários visitantes temporários;
- Permitir a utilização de portal Web (Captive Portal) externo a controladora.
- Deve ser fornecido com recursos instalados para implementar listas de controle de acesso (ACL) com suporte a contadores (ACL Counters), ou seja, para um determinado pacote deve ser possível verificar qual entrada da lista de controle de acesso foi utilizada;
- Implementar listas de controle de acesso (ACL) baseadas em protocolos e endereços MAC;
- Deve ser fornecida com recursos instalados para implementar o bloqueio da comunicação entre usuários em um mesmo SSID;
- Deve ser fornecido com recursos instalados para implementar mecanismo para detecção de Pontos de Acesso invasor (Rogue AP);
- Deve ser fornecida com recursos instalados para implementar mecanismo para detecção de clientes invasores (Rogue clients detection);
- Deve ser fornecida com recursos instalados para implementar mecanismo para detecção de Redes Ad-Hoc;
- Deve possuir recursos para implementar mecanismo para contenção de Pontos de Acesso invasores (Rogue AP);
- Implementar suporte a assinaturas de ataques de RF e prevenção de intrusão para ajudar ao administrador a customizar arquivos de assinatura de ataques para rapidamente detectar ataques de RF mais comuns tais como: denial of service (DoS), Netstumbler e FakeAP;
- Implementar varedura de RF continua, programada ou sob demanda;
- Deve possuir recursos para implementar ajuste dinâmico de canais 802.11 para otimizar a cobertura de rede e mudar as condições RF baseado em performance;
- Deve permitir acesso à interface de gerenciamento para todas as funcionalidades que existem localmente no controlador WLAN, sendo, no mínimo, suporte as seguintes opções:
    1. Telnet,
    2. Secure Shell (SSH) Protocol;
    3. HTTP;
    4. Secure HTTP (HTTPS);
    5. Porta Console.
- Deve possuir recursos instalados para implementar detecção de interferência e reajuste dos parâmetros de RF evitando problemas de cobertura e performance;
- Deve possuir recursos instalados para implementar balanceamento de carga de usuários de modo automático através de múltiplos pontos de acesso para otimizar a performance durante elevada utilização da rede;
- Deve possuir recursos instalados para implementar mecanismos automáticos de gerenciamento de recursos de rádio, detectando áreas sem cobertura, indisponibilidades de pontos de acesso, e executando auto configuração, auto correção e auto otimização;
- Deve possuir recursos instalados para implementar mecanismo que ajusta dinamicamente a saída de potência dos Pontos de Acesso individualmente para acomodar as condições de alterações da rede, garantindo a performance e escalabilidade;
- Deve possuir recursos instalados para implementar mecanismo que no evento de falha de um ponto de acesso, o controlador ajuste automaticamente potência dos pontos de acesso adjacentes para dar cobertura de área onde o ponto de acesso que falhou estava provendo o sinal;
- Ajustar, dinamicamente, o nível de potência e canal dos rádios dos APs, de modo a otimizar o tamanho da célula de RF, garantido a performance e escalabilidade;
- Permitir a seleção/uso de servidor Radius ou LDAP com base no SSID;

- Permitir o uso de VoWLAN e dados sobre um mesmo SSID;
- Deve suportar 802.11e com WMM, U-APSD e T-SPEC;
- Deve possuir base de dados de usuários interno para autenticação de usuários convidados/temporários (acesso guest);
- Implementar associação dinâmica de usuáriso a VLAN, com base nos parâmetros da etapa de autenticação;
- Deve possuir funcionalidade que permita a configuração de contingência dos pontos de acesso, ou seja, no caso de falha de um controlador os pontos de acesso configurados serão conectados ao controlador de contingência;
- Suportar, no mínimo, 4096 VLANs;
- Deve implementar um mecanismo de controle de associação de banda, de forma que usuários com capacidade de comunicação 802.11a/b/g/n em 2,4GHz e 5GHz sejam preferencialmente, e sempre que possível, alocados nos canais da banda de 5GHz do Ponto de Acesso, quando os mesmos se associem à rede WLAN.
- Deve permitir a configuração da técnica "beamforming" de transmissão de forma otimizar a relação de sinal ruído e a performance de transmissão de dados para determinados usuários da rede WLAN.
- Deve possuir mecanismo de otimização automática de tráfego multicast para vídeo, permitindo a definição de largura de banda por grupo multicast. Este mecanismo deve permitir que o tráfego de multicast seja enviado aos clientes da rede WiFi na velocidade de conexão destes clientes, por exemplo 300 Mbps, mesmo que está não seja “rate” mandatório.
- Implementar padrão Wireless Multi-media QoS (WMM) da Wi-Fi Alliance para priorização de tráfego, suportando aplicações em tempo real, tais como, VoIP, vídeo, dentre outras;
- Implementar qualidade de serviço com a marcação de pacotes utilizando Diffeservice e suporte a 802.1p, para QoS.
- Deve permitir visibilidade e controle das aplicações, permitindo a priorização de aplicações críticas, redução na prioridade de aplicações menos críticas e o bloqueio de aplicações não permitidas já na camada de acesso. Deve ter a capacidade de identificar, no mínimo, 1000 (um mil) aplicações diferentes;
- Deve implementar técnica de inspeção de pacotes para controle de aplicações que não utilizam portas fixas ou que utilizam protocolo TCP porta 80 ou 443;
- Permitir, opcionalmente, a reserva automática de banda da rede WLAN para o controle de admissão de chamada de voz;
- Permitir configurar os APs como sensores de RF para fazer a monitoração do ambiente Wireless;
- Possuir funcionalidade que permita definir prioridade para contingência dos Pontos de Acesso, ou seja, no caso de falha de um controlador os pontos de acesso configurados com maior prioridade terão preferência a se conectarem ao controlador de contingência.
- Implementar DHCP Relay;
- Implementar tagging de VLAN através do protocolo 802.1Q
- Permitir o uso de múltiplos SSIDs simultaneamente;
- Permitir definir o número máximo de clientes por SSIDs.

13. PONTO DE ACESSO WLAN

Interfaces:

- Deve possuir ao menos 1 (uma) interfaces de rede Multigigabit ethernet 100/1000/2500 Base-T com conectores RJ-45;

- Quando utilizado cabeamento Cat 5e, não deve sofrer nenhuma perda de funcionalidade e/ou desempenho;
- A interfaces deve permitir alimentação elétrica no padrão IEEE 802.3at (PoE+), utilizando a porta do switch onde estiver conectado;
- Quando alimentado pela interface de rede, não deve sofrer nenhuma perda de funcionalidade e/ou desempenho.

Gerenciamento:

- O equipamento a ser ofertado deve ser totalmente compatível, e ser fornecido com todas as licenças necessárias para a integração com o PLATAFORMA DE GERENCIAMENTO descrito nesta Especificação Técnica.
- O equipamento a ser ofertado deve ser totalmente compatível, e ser fornecido com todas as licenças necessárias para a integração com a CONTROLADORA WIRELESS LAN descrita nesta Especificação Técnica.
- Deve possuir uma porta console para gerenciamento fora de banda (out-of-band management);
- Deve permitir o armazenamento de sua configuração em memória não volátil (flash), devendo, em situação de queda e posterior reestabelecimento da alimentação elétrica, voltar à operação normalmente na mesma configuração anterior ao incidente;
- Deve ser gerenciável via SNMP versões 2 ou 2c e 3;
- Deve permitir a configuração e gerenciamento através de browser padrão com protocolo HTTPS;
- Deve possuir suporte a MIB II;
- Deve implementar o envio de eventos por meio do protocolo Syslog.

Antenas:

- Possuir antenas internas integradas e não aparentes compatíveis com as frequências de rádio dos padrões 2.4GHz e 5GHz com as seguintes características:

Radio Flexível (2.4GHz ou 5GHz configurável):

1. 2.4GHz: Ganho de, pelo menos, 4 dBi com padrão de irradiação omnidirecional;
2. 5.0GHz: Ganho de, pelo menos, 5 dBi com padrão de irradiação omnidirecional.

Rádio dedicado de 5-GHz:

1. Ganho de, pelo menos, 5 dBi com padrão de irradiação omnidirecional.

Segurança:

- Deve implementar mecanismos de autenticação, autorização e accounting (AAA);
- Deve implementar autenticação em servidores RADIUS externos;
- Deve implementar autenticação 802.1x com atribuição dinâmica de VLAN de acordo com o usuário autenticado;
- Deve implementar recursos que permitam mecanismo de autenticação através de portal Web para clientes visitantes, com nome e senha;
- Deve implementar a configuração de filtros baseados em protocolos;
- Deve implementar a configuração de filtros baseados em endereços MAC (Media Access Control);
- Deve suportar a passagem de tráfego VPN IPSec;
- Deve implementar o protocolo IEEE 802.1X, com pelo menos os seguintes métodos EAP:
    1. EAP-Transport Layer Security (EAP-TLS);

2. EAP-TTLS/MSCHAPv2;
3. PEAPv0/EAP-MSCHAPv2;
4. PEAPv1/EAP-GTC;
5. EAP Subscriber Identity Module (EAP-SIM).

- Deve suportar a autenticação com geração dinâmica de chaves criptográficas por sessão e por usuário;
- Deve implementar suplicante 802.1x para identificar o ponto de acesso, ao ser conectado na estrutura de rede cabeada;
- Possuir módulo de criptografia em hardware;
- Implementar WPA (Wi-Fi Protected Access com algoritmo de criptografia TKIP e Message Integrity Check-MIC);
- Implementar WPA-2 (Wi-Fi Protected Access com algoritmo de criptografia AES, 128 bits);
- Implementar WPA-3 (Wi-Fi Protected Access com algoritmo de criptografia AES, 192 bits);
- Deve implementar a capacidade de realizar triangulação de RF (Rádio Frequência) nas bandas 802.11a/b/g/n/ac/ax para identificação de acesso intruso não autorizados (rogues) em todos os canais de 2,4 GHz e 5 GHz sem impacto no seu desempenho;
- Deve implementar recursos para detecção de redes Ad Hoc;
- Deve detectar interferências WiFi (provenientes de dispositivos padrão IEEE802.11) e detectar e classificar interferências não-WiFi, tais como Bluetooth, telefones sem fio, câmeras de video sem fio, microondas e outros;
- Deve ter a capacidade de mudar de canal caso seja detectada alguma das interferências listadas no item anterior no canal de operação atual e devem permanecer no novo canal caso a interferência seja persistente;
- Deve permitir habilitar e desabilitar a divulgação do SSID;
- Deve implementar recursos em conjunto com a controladora para realizar o isolamento de usuários, bloqueando a comunicação entre dispositivos clientes em um mesmo SSID.

Padrões:

- Deverá possuir, em conjunto com o conjunto controlador WiFi fornecida neste projeto, certificado emitido pelo "WiFi® Alliance" comprovando os seguintes padrões, protocolos e funcionalidades:
    1. IEEE 802.11a;
    2. IEEE 802.11b;
    3. IEEE 802.11g;
    4. IEEE 802.11n:
        1. 2.4 GHz, 5 GHz – Concurrent;
        2. 3 Spatial Streams 2.4 GHz;
        3. 3 Spatial Streams 5 GHz;
        4. Short Guard Interval;
        5. TX A-MPDU;
        6. 40 MHz operation in 5 GHz;
        7. HT Duplicate (MCS 32);
        8. OBSS on Extension Channel;
        9. RIFS Test;
    5. IEEE 802.11ac:

        1. 3 Spatial Streams 5 GHz;
        2. Rx MCS 8-9 (256-QAM);
        3. Rx A-MPDU of A-MSDU;
        4. Tx SU beamformer;
        5. Low Density Parity Check coding;
        6. Tx DL MU-MIMO;
        7. Rx 160 MHz operations;
    6. IEEE 802.11d;
    7. WPA2® Enterprise/Personal;
    8. WPA3® Enterprise/Personal;
    9. Protected Management Frames;
    10. EAP Type(s):
        1. EAP-TLS;
        2. EAP-TTLS/MSCHAPv2;
        3. PEAPv0/EAP-MSCHAPv2;
        4. PEAPv1/EAP-GTC;
        5. EAP-SIM;
        6. EAP-AKA;
        7. EAP-AKA Prime;
        8. EAP-FAST.
    11. WMM®;
    12. Passpoint®:
        1. Online Signup (OSU) and Policy Provisioning.
- Deve ser homologado pela ANATEL;
- Deve permitir operação simultânea nos padrões IEEE 802.11b/g/n/ax, na faixa de 2,4 GHz, e 802.11a/n/ac/ax, na faixa de 5 GHz;
- Deve implementar a tecnologia 802.11ac Wave 2 MU-MIMO (Multi-User, Multiple Input, Multiple Output);
- Deve implementar a tecnologia 802.11ax MU-MIMO (Multi-User, Multiple Input, Multiple Output) com 4 (quatro) fluxos espaciais;
- Deve ser capaz de suportar taxa de dados de até 5.2 Gbps (PHY) em 802.11ax;
- Deve implementar HT20 e HT40 para IEEE 802.11n;
- Deve implementar VHT20, VHT40, VHT80 e VHT160 para IEEE 802.11ac;
- Deve implementar HE20, HE40, HE80 e HE160 para IEEE 802.11ax
- Deve implementar o protocolo CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) para acesso ao meio de transmissão;
- O equipamento deve ser capaz de implementar 802.11 dynamic frequency selection (DFS);
- Deve possuir suporte à 802.11 Cyclic Shift Diversity (CSD) ou Cyclic Delay Diversity (CDD) ;
- Deve implementar Maximal Ratio Combining (MRC);
- Deve implementar o protocolo NTP (Network Time Protocol) ou o protocolo SNTP (Simple Network Time Protocol) em modo cliente;

- Deve implementar o protocolo TFTP (Trivial File Transfer Protocol) ou o protocolo FTP (File Transfer Protocol) em modo cliente;
- Deve implementar o protocolo DHCP em modo cliente.
-

Facilidades:

- O Ponto de Acesso WLAN deverá possuir, no mínimo as seguintes opções de funcionamento:
    1. Arquitetura sem controlador onde o Ponto de Acesso opera em modo distribuído ou colaborativo, para efetuar as tarefas de controle de espectro de radiofrequência, balanceamento de carga de usuários, controle das políticas de segurança e qualidade de serviços (QoS), autenticação de clientes em 802.1x, fornecimento de informações de clientes conectados e pontos de acesso vizinhos, sem depender de solução de software ou dispositivo externo/remoto;
    2. Arquitetura com controlador onde o Ponto de Acesso opera de modo dependente da Controladora WiFi, possibilitando conexão a Rede Fabric e a não Fabric.
- Deve permitir o agrupamento, em uma única rede Wi-Fi, quando operando no modo distribuído/colaborativo (sem Controladora WiFi), um total de pelo menos 100 (cem) Pontos de Acesso e em conjunto com estes, deve suportar o atendimento de no mínimo 2.000 (dois mil) clientes associados simultaneamente;
- Na solução de arquitetura sem controlador WLAN, o Ponto de Acesso deve possuir capacidade de operação em topologia redundante com um outro do mesmo tipo e modelo, sem nenhuma perda de funcionalidade;
- Na solução dependente de controlador central WLAN, o Ponto de Acesso deve possuir capacidade de associar-se automaticamente a um controlador WLAN alternativo, não permitindo que a rede se torne inoperante, em caso de falha de um dos controladores WLAN;
- Deve possuir arquitetura de rádios flexíveis, permitido que pondo de acesso automaticamente determine, de acordo com as características de RF do ambiente, qual a melhor maneira de operação, deve possuir no mínimo as seguintes possibilidades de operação:
    1. Clientes em 2.4-GHz e 5-GHz: Um radio atendendo clientes em 2.4-GHz e o outro atendendo clientes em 5-GHz;
    2. Clientes em 5-GHz: Os dois rádios atendendo clientes em 5-Ghz;
    3. Clientes em 5 GHZ e Monitoramento de Segurança: Um radio atendendo clientes 5-GHz, e o outro monitorando todo o espectro de RF para identificação de ataques (wIPS), interferências não WiFi e dispositivos rogues.
- Caso o ponto de acesso não possua arquitetura de radios flexiveis, deverá ser fornecido um segundo ponto de acesso, atendendo todas as características de radio, referentes a frequência de 5GHz e todas as demais características. Deverá ser fornecido com antenna de ganho de pelo menos 6 dBi, com padrão de irradiação directional com 90º de plano de elevação, neste caso a antena poderá ser externa;
- Deve implementar, no mínimo, MIMO (Multiple-Input and Multiple-Output) 4x4 com pelo menos 3 fluxos espaciais em SU-MIMO (Single User MIMO) e em MU-MIMO (Multi-User MIMO);
- Deve permitir a conexão de, no mínimo, 200 dispositivos simultâneos por rádio;
- Possuir estrutura metálica que permita fixação do equipamento em teto e também em parede, devem ser fornecidos os acessórios metálicos para que possa ser feita a fixação;
- Deve operar nos seguintes modos: “Modo Local”, “Modo Monitor” e “Modo Analisador de Espectro”;
- Operando em “Modo Local” o ponto de acesso deve fornecer informações ao Controlador WiFi ao qual está associado referentes à qualidade do espectro de RF no canal de operação atual ao mesmo tempo que processa dados 802.11 dos usuários da rede WiFi. Deve fazer tanto a transmissão de

dados WiFi quanto a análise de espectro simultaneamente, sem prejuízo ao fornecimento de wifi aos usuários;

- Operando em "Modo Monitor" deve fornecer informações ao Controlador WiFi referente à qualidade do espectro de RF para todos os canais monitorados em 2.4GHz e em 5GHz, simultaneamente, identificando equipamentos interferentes na rede WiFi e rogue APs;
- Deve implementar a visualização/identificação e marcação das aplicações para permitir o bloqueio ou priorização;
- Deve implementar recursos para ajustar dinamicamente a potência de sinal para acomodar as condições de alterações de rede, interferências ou falha de Pontos de Acesso adjacentes, garantindo o desempenho e escalabilidade;
- Deve implementar a técnica de balanceamento de carga de usuários, permitindo que clientes sejam automaticamente distribuídos entre Pontos de Acesso adjacentes operando em canais distintos, com o objetivo de balancear a carga entre os Pontos de Acesso;
- Deve implementar a técnica de direcionamento de banda, permitindo que clientes com suporte a faixa de frequência de 5 GHz se conectem aos Pontos de Acesso utilizando, preferencialmente, a faixa de 5 GHz;
- Deve implementar a técnica de "beam forming", permitindo concentrar os sinais de rádio na direção dos clientes com os quais estão se comunicando, a fim de ganhar melhor capacidade e taxa de transferência;
- Deve implementar roaming com integridade de sessão possibilitando o uso de aplicações em tempo real, tais como VoIP e videoconferência;
- O equipamento deve realizar a monitoração real-time das frequências de Rádio Frequência (análise espectral) em busca de interferências WiFi e Interferências Não-WiFi e simultaneamente atender os usuários da rede WiFi.
- As funções de monitoração real-time em Rádio Frequência (análise espectral) devem ser realizadas via hardware, com chipset (ASIC) dedicado para esta função localizado dentro do ponto de acesso;
- Deve detectar interferências WiFi (provenientes de dispositivos padrão IEEE802.11) e detectar e classificar interferências não-WiFi, tais como Bluetooth, telefones sem fio, câmeras de video sem fio, Microondas e outros;
- Deve ter a capacidade de mudar de canal caso seja detectada alguma das interferências listadas no item anterior no canal de operação atual e devem permanecer no novo canal caso a interferência seja persistente;
- O equipamento deve realizar a monitoração real-time das frequências de Rádio Frequência (análise espectral) em busca de interferências WiFi e Interferências Não-WiFi em canais de 20, 40, 80, ou 160-MHz e simultaneamente atender os usuários da rede WiFi;
- Deve possuir capacidade de criação e utilização de, no mínimo, 16 SSIDs (Service Set IDentifier);
- Deve possuir capacidade de criação e utilização de, no mínimo, 16 VLANs (Virtual Local Area Network) conforme padrão IEEE 802.1Q;
- Deve poder operar de tal forma que realize o chaveamento (switching) do tráfego local dos usuários sem que este tráfego tenha que passar através do(s) Controlador(es) WiFi - operação em modo de "chaveamento de tráfego local".
- Operando no modo de "chaveamento de tráfego local", o controlador WiFi e os pontos de acesso devem:

    1. O modo de operação de chaveamento de tráfego local deve prever que se a comunicação entre o ponto de acesso WiFi e o(s) Controlador(es) WiFi seja interrompida por qualquer motivo, como por exemplo falha no link WAN, LAN ou no(s) próprio(s) Controlador(es) WiFi, o ponto de acesso WiFi deve continuar operando e permitindo que os usuários já autenticados na rede e associados aos pontos de acesso continuem a possuir acesso à rede. Deve permitir que os usuários efetuem roaming rápido entre os pontos de acesso do mesmo site nesta situação;

2. Uma vez que a comunicação entre o ponto de acesso e o(s) Controlador(es) WiFi seja interrompida por qualquer motivo, como por exemplo falha no link WiFi ou no(s) próprio(s) Controlador(es) WiFi, o ponto de acesso WiFi em modo de chaveamento de tráfego local deve possuir meios de continuar operando e ter funcionalidade que permita que novos usuários se autentiquem de acordo com 802.1x e se associem à rede sem qualquer prejuízo de acesso aos mesmos;
3. Uma vez que a comunicação entre o ponto de acesso e o(s) Controlador(es) WiFi seja interrompida por qualquer motivo, como por exemplo falha no link WiFi ou no(s) próprio(s) Controlador(es) WiFi, o ponto de acesso WiFi em modo de chaveamento de tráfego local deve possuir meios de continuar operando e ter funcionalidade que permita que os usuarios efetuem roaming sem qualquer prejuízo de acesso aos mesmos.

- Deve implementar DHCP relay.
- Deve permitir a configuração da técnica "beamforming" de transmissão de forma otimizar a relação de sinal ruído e a performance de transmissão de dados para determinados usuários da rede WLAN. Deve perimitir esta formação de banda para cliente 802.11ac;
- Deve possuir potência máxima de transmissão, por rádio, de pelo menos 23 dBm em 2,4 GHz e em 5 GHz.
- Operar em Canais de 20MHz para 2,4GHz e possibilitar channel bounding, canal de 40 MHz canais de 80MHz e canais de 180MHz para 5GHz.
- Possuir pelo menos as seguintes taxas de transmissão e com fallback automático: IEEE 802.11 a/g: 54, 48, 36, 24, 18, 12, 9 e 6 Mbps.
- Possuir pelo menos as seguintes taxas de transmissão e com fallback automático: IEEE 802.11n: MSC0 – MCS23 (6.5Mbps - 450Mbps).
- Possuir pelo menos as seguintes taxas de transmissão e com fallback automático: IEEE 802.11ac: MSC0 – MCS9 para 1,2 e 3 Spatial Streams (6.5Mbps – 2,304Gbps).

14. PLATAFORMA DE GERENCIAMENTO

Características Técnicas

- Esta plataforma poderá ser entregue em formato de appliance virtual ou hardware dedicado;
- Tanto o hardware quanto os softwares necessários para a implantação da Plataforma de Gerência da Solução deverão fazer parte do fornecimento, incluindo o computador/servidor e as licenças de sistema operacional, além de outros dispositivos eventualmente necessários para o seu pleno funcionamento inclusive em alta-disponibilidade (ativo-standby) ou (ativo-ativo);
- Caso seja fornecido no formato de appliance virtual, o hardware (computador/servidor) poderá ser compartilhado com a “Controladora de Acesso a Rede”, especificada neste documento, desde que atenda individualmente os requisitos mínimos de cada uma das soluções;
- Em ambas as soluções, o hardware deve ter no mínimo 2 (duas) interfaces de rede ethernet 1000BaseT com conectores RJ-45;
- Deve ser fornecido com a versão mais recente (última versão) comercial disponível do software interno instalado;
- Deverá suportar o gerenciamento de até 10 mil dispositivos em sua configuração máxima, o hardware deverá estar dimensionado para estas capacidades;
- Esta Plataforma de gerenciamento deve ser do mesmo fabricante dos Itens Switch Core, Switch de Distribuição – Tipo I, Tipo II, Tipo III e Tipo IV, Switch de Acesso - Tipo I e Tipo II, Controladora de Rede WIFI, Ponto de Acesso, e Controladora de Acesso a Rede. Deve ser capaz de gerenciar todos os tipos de switches, controladores e pontos de acesso descritos neste documento e capaz de fornecer todas as funcionalidades descritas neste documento para todos os equipamentos descritos;

- Possuir alta disponibilidade, ativo/standby, trabalhando com no mínimo dois servidores físicos ou virtuais. Os servidores podem estar em sites diferenciados ou subnets diferenciadas. As licenças necessárias e o hardware necessário para implementar esse recurso devem estar incluídas, inclusive de banco de dados se for o caso;
- Implementando alta disponibilidade, trabalhando com no mínimo, dois sistemas completos, garantindo replicação automática da toda base de dados. As licenças necessárias para implementar este recurso deverão incluídas;
- A plataforma de gerência ofertada deverá possuir todas as licenças com todas as funcionalidades exigidas nesta especificação e contemplando o total de dispositivos exigidos nesta especificação;
- Deverá possuir menu unificado e intuitivo, ao qual o operador poderá acessar as tarefes necessária para gerenciamento da rede;
- Possuir "Workflows" de configuração baseados nas melhores práticas do fabricante para vários tipos de tecnologias a serem implementadas;
- Permitir a adição de novas funcionalidades, sem a necessidade de atualização completa, somente com instalação da nova funcionalidade;
- Possuir a funcionalidade a qual o operador tenha acesso rápido a um resumo das informações mais importantes sobre o usuário ou dispositivo gerenciado;
- Ter mapas da topologia da rede com representação dos dispositivos e suas interconexões. Deverá apresentar no mapa se o dispositivo possui alarme associado a ele.
- Permitir a criação de templates de configuração, permitindo "scheduling" de horário para aplicação do mesmo;
- Permitir a criação de templates, formados por conjunto de outros templates, possibilitando uma fácil automação para configurações mais complexas;
- Possuir templates de configuração de controle e visibilidade de aplicações (AVC), NetFlow, NBAR2 e QoS;
- Deve possibilitar a visualização rápida de alarmes e estatísticas de utilização dos recursos dos dispositivos gerenciados, para fácil e rápido monitoramento e troubleshooting;
- Deve possuir suporte para gerenciamento de falhas via Simple Network Management Protocol (SNMP) version 3 (além do SNMP versão 2 e 1) para gerenciamento seguro entre a plataforma de gerenciamento e todos os dispositivos gerenciados;
- Sistema de gerência deve ser acessado através de qualquer browser via HTTP ou Secure HTTP (HTTPS), permitindo o acesso à plataforma de gerência a qualquer momento de qualquer local;
- Permitir a criação de Domínios de Gerência Virtuais, ou seja, permitir a criação de perfis de administração que possibilitem limitar a administração de seguimentos da rede wireless e a toda rede;
- Permitir a visualização de alertas da rede em tempo real;
- Suporte a criação e aplicação de políticas que permitam ao administrador gerir/criar VLAN, qualidade de serviço (QoS) e política de segurança;
- Permitir troubleshooting de clientes com dificuldade de se conectarem a rede;
- Deve permitir a autenticação dos operadores através de base local e através de RADIUS e TCACAS+;
- Deve implementar protocolo de autenticação para controle do acesso administrativo a qualquer componente da gerência da solução utilizando servidor RADIUS e TACACS+ para auditoria de comandos com mecanismos de AAA;
- Deve executar o registro das ações executadas pelos operadores nos equipamentos gerenciados, para efeito de auditoria;
- Deve permitir o acesso de, no mínimo, 25 (vinte e cinco) operadores do sistema de forma simultânea;

- Deve implementar controle de acesso baseado em privilégios, permitindo a criação de grupos de operadores com limitação de quais equipamentos e quais serviços da plataforma poderão ser usados;
- Deve possuir interface web que permita o acesso integral à ferramenta através de um navegador padrão (Firefox, Internet Explorer e Google Crome);
- Deve permitir a descoberta de elementos de rede através da faixa de endereços IP, e tabela de roteamento;
- Deve permitir a configuração, monitoramento, adição e gerência de um dispositivo e também de um grupo de dispositivos;
- Deve possuir recursos instalados e licenciados para o gerenciamento de redes, contemplando a configuração, monitoramento dos dispositivos WLAN, LAN e WAN, permitindo o gerenciamento integrado de redes sem fio e cabeada na mesma plataforma;
- Deve permitir a customização página principal do sistema, permitindo a inclusão alarmes, estatísticas de desempenho;
- Deve permitir importar uma lista de dispositivos através de um arquivo;
- Deve permitir visualização de estatísticas de utilização do equipamento contemplando no mínimo utilização de memória e de CPU;
- Deve permitir a visualização de informações dos dispositivos e componentes instalados, trazendo no mínimo, informações como fabricante, modelo, número de série, versão de hardware e software e outras informações que sejam disponibilizadas pelo equipamento gerenciado;
- Deve permitir a localização de endereço IP e de endereço MAC na infraestrutura de rede;
- Deve permitir a visualização do histórico dos arquivos de configuração dos dispositivos;
- Deve permitir visualizar, comparar, aplicar e fazer o backup da configuração dos dispositivos gerenciados;
- Deve permitir atualizar o software do dispositivo gerenciado;
- Deve permitir a criação de modelos de configuração para serem aplicados aos dispositivos gerenciados. Deve permitir criar modelos de parte da configuração e da configuração inteira do dispositivo;
- Deve permitir o agendamento de backups da configuração dos dispositivos gerenciados;
- Deve possuir recursos instalados e licenças para a criação de relatórios de histórico de backups e atualizações de software;
- Deve permitir a criação de regras de verificação de configuração e comparar com a configuração dos dispositivos gerenciados, gerando relatório da verificação;
- Deve possuir recursos instalados para executar operação como servidor syslog, permitindo a recepção de mensagens Syslog dos dispositivos;
- Deve possuir capacidade de gerar alarmes a partir de traps SNMP e mensagens Syslog;
- Deve possuir mecanismo de análise de causa do problema para a supressão de eventos que são apenas sintoma da falha;
- Deve possuir painel único de visualização dos alarmes e a partir desta tela verificar detalhes específicos de um alarme;
- Deve possuir a capacidade de enviar e-mails para um administrador em caso de algum evento especificado de acordo com o nível de criticidade;
- Deve possuir capacidade de monitorar o desempenho dos equipamentos gerenciados;
- Deve possuir capacidade de monitorar a utilização de CPU, utilização de Memória, tempo de resposta e Disponibilidade;
- Deve permitir ao administrador escolher quais monitores de desempenho devem ser configurados para ativar um alarme;
- Deve permitir a visualização em tempo real de itens monitorados;

- Deve permitir a visualização e configuração de listas de controle de acesso (ACL) nos equipamentos gerenciados e compatíveis;
- Deve permitir a criação de templates ACL's para a distribuição em diversos equipamentos;
- Deve possuir capacidade de configurar interface VLAN ou interfaces virtuais, adicionar portas de acesso e do tipo trunk;
- Deve fornecer informações dos clientes online associados;
- A plataforma de gerência da solução deve permitir a coleta de informações dos clientes conectados, incluindo informações de endereçamento de camada 3 do modelo OSI;
- Deverá ser possível monitorar os endereçamentos IPv4 e IPv6 dos clientes na página de administração da plataforma de gerência;
- Deve fornecer informações estatísticas de performance baseadas no histórico dos Controladores e Pontos de Acesso Gerenciados;
- Deve prover relatórios contendo ameaças de segurança recorrentes antes que estes causem danos à infraestrutura sem fio e/ou à cabeada;
- Deve possuir capacidade de gerar relatórios customizados, com no mínimo os seguintes tópicos:
    1. Ativos de Rede;
    2. Estado dos dispositivos e Links;
    3. Lista total de portas e lista de portas disponíveis;
    4. Inventário dos equipamentos;
    5. Informações sobre os dispositivos ativos;

15. INTERFACE 100GB QSFP SR

- Transceiver ótico do tipo QSFP padrão 100GBase-SR4;
- Deve operar sobre fibras do tipo multimodo;
- Deve atingir distância de até 100 metros;
- Deverá ser compatível com o padrão IEEE 802.3bm;
- Deve permitir sua instalação e operação em conjunto com as portas QSFP solicitadas nesta Especificação Técnica.

16. INTERFACE 100GB QSFP LR

- Transceiver ótico do tipo QSFP padrão 100GBase-LR4;
- Deve operar sobre fibras do tipo monomodo;
- Deve atingir distância de até 10 quilometros;
- Deverá ser compatível com o padrão IEEE 802.3bm;
- Deve permitir sua instalação e operação em conjunto com as portas QSFP solicitadas nesta Especificação Técnica;

17. INTERFACE 40GB QSFP SR

- Transceiver ótico do tipo QSFP padrão 40GBase-SR4;
- Deve operar sobre fibras do tipo multimodo;
- Deve atingir distância de até 100 metros;

- Deverá ser compatível com o padrão IEEE 802.3ba;
- Deve permitir sua instalação e operação em conjunto com as portas QSFP solicitadas nesta Especificação Técnica;

18. **INTERFACE 40GB QSFP LR**

- Transceiver ótico do tipo QSFP padrão 40GBase-LR4;
- Deve operar sobre fibras do tipo monomodo;
- Deve atingir distância de até 10 quilometros;
- Deverá ser compatível com o padrão IEEE 802.3ba;
- Deve permitir sua instalação e operação em conjunto com as portas QSFP solicitadas nesta Especificação Técnica;

19. **INTERFACE 25GB SFP28 SR**

- Transceiver ótico do tipo SFP28 padrão 25GBase-SR;
- Deve operar sobre fibras do tipo multimodo;
- Deve atingir distância de até 100 metros;
- Deve possuir conector do tipo LC duplex;
- Deverá ser compatível com o padrão IEEE 802.3by;
- Deve permitir sua instalação e operação em conjunto com as portas SFP28 solicitadas nesta Especificação Técnica;
-

20. **INTERFACE 25GB SFP28 LR**

- Transceiver ótico do tipo SFP28 padrão 25GBase-LR;
- Deve operar sobre fibras do tipo multimodo;
- Deve atingir distância de até 10 quilometros;
- Deve possuir conector do tipo LC duplex;
- Deverá ser compatível com o padrão IEEE 802.3cc;
- Deve permitir sua instalação e operação em conjunto com as portas SFP28 solicitadas nesta Especificação Técnica;

21. **INTERFACE 10GB SFP+ SR**

1. Transceiver ótico do tipo SFP+ padrão 10GBase-SR;
2. Deve operar sobre fibras do tipo multimodo;
3. Deve atingir distância de até 400 metros;
4. Deve possuir conector do tipo LC duplex;
5. Deverá ser compatível com o padrão IEEE 802.3ae;
6. Deve permitir sua instalação e operação em conjunto com as portas SFP+ solicitadas neste documento;

22. **INTERFACE 10GB SFP+ LR**

- Transceiver ótico do tipo SFP+ padrão 10GBase-LR;
- Deve operar sobre fibras do tipo monomodo;
- Deve atingir distância de até 10 quilometros;
- Deve possuir conector do tipo LC duplex;
- Deverá ser compatível com o padrão IEEE 802.3ae;
- Deve permitir sua instalação e operação em conjunto com as portas SFP+ solicitadas neste documento;

23. **INTERFACE 1GB SFP SX**

- Transceiver ótico do tipo SFP padrão 1000Base-SX;
- Deve operar sobre fibras do tipo multimodo;
- Deve atingir distância de até 500 metros;
- Deve atender o padrão IEEE 802.3z;
- Deve possuir conector do tipo LC duplex;
- Deve permitir sua instalação e operação em conjunto com as portas SFP solicitadas neste documento;

24. **INTERFACE 1GB SFP LX**

- Transceiver ótico do tipo SFP padrão 1000Base-LX;
- Deve operar sobre fibras do tipo monomodo;
- Deve atingir distância de até 10 quilômetros;
- Deve atender o padrão IEEE 802.3z;
- Deve possuir conector do tipo LC duplex;
- Deve permitir sua instalação e operação em conjunto com as portas SFP solicitadas neste documento;

25. **CONVERSOR QSFP PARA 4 SFP+**

- Cabo passivo com entrada padrão 40G QSFP e saída em 4 conectoras 10G SFP+.
- Os conectores devem ser fixos ao cabo;
- Deve possuir 5 metros de comprimento;
- Deve permitir sua instalação e operação em conjunto com as portas QSFP solicitadas neste documento;

26. **SERVIÇOS DE INSTALAÇÃO (INCLUSOS NOS ÍTENS DE FORNECIMENTO)**

Serviços de instalação e configuração para switch core e modulo de interface TIPO I, II, III E IV

- Este item preconiza o fornecimento dos seguintes serviços a serem executados pela CONTRATADA.
- Montagem do equipamento no bastidor disponibilizado para este fim;

- Configuração das funcionalidades básicas para que o equipamento entre em operação no ambiente proposto. Entende-se como funcionalidades básicas os seguintes itens:
    1. Configuração de até 10 (dez) grupos LACP;
    2. Configuração de até 20 (vinte) VLANs;
    3. Configuração de até 20 (vinte) instancias Spanning-Tree;
    4. Configuração de até 3 (três) áreas do protocolo de roteamento OSPFv2 ou OSPFv3;
    5. Configuração de até 20 (vinte) sub-redes;
    6. Configuração de funcionalidades de segurança, tais como:
        1. BPDU Guard;
        2. DHCP Snooping;
        3. IP Source Guard;
        4. Port Security;
        5. DAI – Dynamic ARP Inspection.
    7. Configuração de protocolos de gerenciamento, tais como:
        1. Syslog;
        2. SNMPv2 e SNMPv3;
        3. NTP.
- Identificação física do equipamento conforme norma TIA/EIA 606;
- Inclusão dos dados de configuração deste equipamento na documentação AS-BUILT.

Serviços de instalação e configuração para switch de distribuição TIPO I, II, III E IV

- Este item preconiza o fornecimento dos seguintes serviços a serem executados pela CONTRATADA.
- Montagem do equipamento no bastidor disponibilizado para este fim;
- Configuração das funcionalidades básicas para que o equipamento entre em operação no ambiente proposto. Entende-se como funcionalidades básicas os seguintes itens:
    1. Configuração de até 10 (dez) grupos LACP;
    2. Configuração de até 20 (vinte) VLANs;
    3. Configuração de até 20 (vinte) instancias Spanning-Tree;
    4. Configuração de até 3 (três) áreas do protocolo de roteamento OSPFv2 ou OSPFv3;
    5. Configuração de até 20 (vinte) sub-redes;
    6. Configuração de funcionalidades de segurança, tais como:
        1. BPDU Guard;
        2. DHCP Snooping;
        3. IP Source Guard;
        4. Port Security;
        5. DAI – Dynamic ARP Inspection.
    7. Configuração de protocolos de gerenciamento, tais como:
        1. Syslog;
        2. SNMPv2 e SNMPv3;
        3. NTP.

- Identificação física do equipamento conforme norma TIA/EIA 606;
- Inclusão dos dados de configuração deste equipamento na documentação AS-BUILT.

Serviços de instalação e configuração para switches de acesso TIPO I E II

- Este item preconiza o fornecimento dos seguintes serviços a serem executados pela CONTRATADA.
- Montagem do equipamento no bastidor disponibilizado para este fim;
- Configuração das funcionalidades básicas para que o equipamento entre em operação no ambiente proposto. Entende-se como funcionalidades básicas os seguintes itens:
    1. Configuração de até 10 (dez) grupos LACP;
    2. Configuração de até 20 (vinte) VLANs;
    3. Configuração de até 20 (vinte) instancias Spanning-Tree;
    4. Configuração de até 20 (vinte) sub-redes;
    5. Configuração de funcionalidades de segurança, tais como:
        1. BPDU Guard;
        2. DHCP Snooping;
        3. IP Source Guard;
        4. Port Security;
        5. DAI – Dynamic ARP Inspection.
    6. Configuração de protocolos de gerenciamento, tais como:
        1. Syslog;
        2. SNMPv2 e SNMPv3;
        3. NTP.
- Identificação física do equipamento conforme norma TIA/EIA 606;
- Inclusão dos dados de configuração deste equipamento na documentação AS-BUILT.

Serviços de instalação e configuração para controladora sem fio

- Este item preconiza o fornecimento dos seguintes serviços a serem executados pela CONTRATADA.
- Montagem do equipamento no bastidor disponibilizado para este fim;
- Definição da topologia, segmentação e endereçamento das WLANs.
- Configurar os SSIDs (Locais e Visitantes) para as redes conforme planejamento previamente estabelecido.
- Configuração de QoS: regras de classificação, priorização e policiamento de acordo com as aplicações a serem utilizadas na rede wireless.
- Definição de políticas de bloqueio e permissão de acesso.
- A rede de visitante (guest) deverá encaminhar o tráfego de internet através de servidores e topologia de rede definidos em conjunto com a equipe de TI
- Configuração de Endereços/Interfaces de Gerência.
- Configuração de redes locais (VLANs).
- Configuração do controle de acesso de usuários à rede através do padrão IEEE 802.1x integrado ao servidor RADIUS e serviço de diretório Microsoft Active Directory, quando aplicável.
- Configurações de grupos de ponto de acesso.

- Configuração de algoritmo de criptografia, métodos de autenticação e segurança a serem utilizados.
- Configurações dos recursos de IDS/IPS, quando aplicável.
- Configuração do captive portal de autenticação (portal cativo).

Serviços de instalação e configuração para ponto de acesso sem fio

- Compõem a etapa de instalação dos pontos de acesso os seguintes serviços:
- Realização do estudo de campo;
- Elaboração e apresentação de cronograma detalhado do projeto de instalação dos pontos de acesso;
- Instalação física e configuração dos pontos de acesso, com a versão mais atual de software (firmware) recomendada pelo fabricante;
    1. Caberá à CONTRATADA fazer a conexão dos pontos de acesso aos pontos lógicos de acesso, fornecendo os materiais e a mão de obra necessários para tanto, segundo orientações da CONTRATANTE.
    2. Caso ainda não haja disponibilidade de ponto lógico de acesso nos locais determinados para a instalação, será responsabilidade da CONTRATANTE providenciar a instalação desses pontos lógicos.
- Configuração de endereçamento IP, Telnet Seguro (SSH), Web (HTTP/HTTPS), quando aplicável, conforme definido na etapa de projeto;
- Configuração de parâmetros SNMP para monitoração/gerência remota;
- Configuração de Syslog, quando aplicável;
- Configuração de sincronismo de hora NTP ou SNTP;
- Interfaces de roteamento IP;
- Implementação dos recursos de qualidade de serviço (QoS), conforme Projeto de Rede Wireless elaborado;
- Ativação de VLANs e SSIDs definidos no projeto;
- Configuração de alarmes e notificações automatizadas via SNMP e/ou SMTP, disponíveis na solução;
- Realizar testes de desempenho de RF dos pontos de acesso wireless;
- Aperfeiçoar o posicionamento de pontos de acesso da solução instalada;
- Integração com a CONTROLADORA SEM FIO;
- Identificação e representação gráfica dos pontos de acesso no mapa de controle da solução de gerenciamento;
- Testes de funcionamento;
- Implantação da solução de rede sem fio em caráter definitivo no ambiente proposto pela equipe de tecnologia da informação;

Serviços de instalação e configuração para sistema de gerencia da rede

- Este item preconiza o fornecimento dos seguintes serviços a serem executados pela CONTRATADA.
- Montagem do equipamento no bastidor disponibilizado para este fim;
- Configuração das funcionalidades básicas para que o equipamento entre em operação no ambiente proposto. Entende-se como funcionalidades básicas os seguintes itens:
    1. Configuração das políticas de acesso ao portal de administração;
    2. Configuração dos perfis de usuário com acesso de administração;
    3. Configuração da funcionalidade Single Sign On (SSO);

4. Configuração dos protocolos RADIUS/TACACS+ para integração com servidores AAA (authentication, authorization, and accounting);
5. Configuração de políticas de agrupamento de dispositivos, tais como switches, access points e roteadores;
6. Configuração da funcionalidade de mapeamento e montagem de topologia;

27. GARANTIA, SUPORTE E MANUTENÇÃO (INCLUSOS NO FORNECIMENTO DA SOLUÇÃO)

- A SOLUÇÃO deverá ter garantia total de no mínimo 36 (trinta e seis) meses para todos os itens fornecidos, incluindo Hardware e Software, sendo que a garantia deverá ser "on site", isto é, no local onde o item estiver instalado, contados a partir do recebimento definitivo do contrato;
- Sem apresentar qualquer ônus ao CONTRATANTE, a garantia deverá abranger a manutenção corretiva com a cobertura de todo e qualquer defeito apresentado, inclusive a substituição de peças, partes e componentes e acessórios, através de suporte técnico, conforme descrito a seguir:

1. Switch Core, Switch de Distribuição e controladora wi-fi: Garantia em regime 24x7;
2. Demais equipamentos: Garantia em regime 8x5;
3. Os valores de suporte e garantia deverão estar associados aos equipamentos e não cobrados a parte;

- Os serviços de suporte deverão ser realizados no Brasil, em português, para solução de problemas de software incluindo atualização de versões e releases;
- A CONTRATADA deverá disponibilizar o acompanhamento dos chamados de suporte;
- A CONTRATADA deverá informar um número para o CONTRATANTE, para que os pedidos de suporte e atendimento possam ser realizados;
- A Garantia oferecida deve estar respaldada pelo fabricante dos equipamentos. Deve ser possível comprovar através de acesso ao site do fabricante que os equipamentos entregues estão cobertos pela garantia do mesmo;
- As atualizações de versões de software deverão ser fornecidas gratuitamente pela CONTRATADA. Os softwares deverão ser disponibilizados para Download eletrônico através de site a ser informado pela CONTRATADA ou enviados através de mídia física;
- O objeto deste estudo não requer a transferência de conhecimento ou tecnologia.

Rio de Janeiro, 31 de Maio de 2021

Documento assinado eletronicamente por **Elio Thomé de Souza Filho**, **Analista de Sistemas**, em 31/05/2021, às 17:32, conforme horário oficial de Brasília, com fundamento nos art. 21º e 22º do Decreto nº 46.730, de 9 de agosto de 2019.

Documento assinado eletronicamente por **Daniel Luzente de Lima**, **Diretor**, em 31/05/2021, às 17:32, conforme horário oficial de Brasília, com fundamento nos art. 21º e 22º do Decreto nº 46.730, de 9 de agosto de 2019.

A autenticidade deste documento pode ser conferida no site http://sei.fazenda.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **17696592** e o código CRC **DF0E0A39**.

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

Governo do Estado do Rio de Janeiro

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

Vice Presidência de Tecnologia

ANEXO II

MODELO DE ORDEM DE FORNECIMENTO

1. **IDENTIFICAÇÃO DA ORDEM DE FORNECIMENTO**

N° da OF [XXX/XXXX]	DATA DE EMISSÃO [XX/XX/XXXX]	N° DO CONTRATO [XXX/XXXX]	DATA DO CONTRATO [XX/XX/XXXX]

2. **IDENTIFICAÇÃO DA EMPRESA CONTRATADA**

Nome da Empresa:				
CNPJ:		Inscrição Estadual:		
Endereço:				
Cidade:			UF:	
CEP:	Telefone:			Fax:

3. **PRODUTOS A SEREM FORNECIDOS**

Descrição:	Switch Core	**Quantidade**	**Data**	**Local**	**Valor**	**Servidor responsáve**
	Switch Core - Módulo de Interface Tipo I					
	Switch Core - Módulo de Interface Tipo II					
	Switch Core - Módulo de Interface Tipo III					
	Switch Core - Módulo de Interface Tipo IV					
	Switch de Distribuição - Tipo I					
	Switch de Distribuição - Tipo II					
	Switch de Distribuição - Tipo III					
	Switch de Distribuição - Tipo IV					
	Switch de Acesso - Tipo I					

	Switch de Acesso - Tipo II					
	Controladora Wireless LAN					
	Ponto de Acesso WLAN					
	Plataforma de Gerenciamento					
	INTERFACE 100GB QSFP SR					
	INTERFACE 100GB QSFP LR					
	INTERFACE 40GB QSFP SR					
	INTERFACE 40GB QSFP LR					
	INTERFACE 25GB SFP28 SR					
	INTERFACE 25GB SFP28 LR					
	INTERFACE 10GB SFP+ SR					
	INTERFACE 10GB SFP+ LR					
	INTERFACE 1GB SFP SX					
	INTERFACE 1GB SFP LX					
	CONVERSOR QSFP PARA 4 SFP+					
Valor Total						

(*) Observar prazos máximos do Edital

4. **APLICAÇÃO DE MULTAS E GLOSAS**

A análise da execução do objeto permite concluir pelo encerramento da Ordem de Fornecimento, com as seguintes observações: RELATÓRIO DE GLOSAS [ANEXAR O TERMO DE RECEBIMENTO DEFINITIVO E PARECER DOS FISCAIS] [CIDADE],_____de_____de_____.	
Gestor / Carimbo	Empresa / Carimbo

5. **ENCERRAMENTO DA ORDEM DE FORNECIMENTO**

A análise da execução do objeto permite concluir pelo encerramento da Ordem de Fornecimento com as seguintes observações:

a. XXXXXXXXXXXXXXXX
b. XXXXXXXXXXXXXXXX
c. XXXXXXXXXXXXXXXX

[CIDADE],_____de_____de_____.

Gestor / Carimbo

Rio de Janeiro, 31 de Maio de 2021.

Documento assinado eletronicamente por **Elio Thomé de Souza Filho**, **Analista de Sistemas**, em 31/05/2021, às 17:32, conforme horário oficial de Brasília, com fundamento nos art. 21º e 22º do Decreto nº 46.730, de 9 de agosto de 2019.

Documento assinado eletronicamente por **Daniel Luzente de Lima**, **Diretor**, em 31/05/2021, às 17:32, conforme horário oficial de Brasília, com fundamento nos art. 21º e 22º do Decreto nº 46.730, de 9 de agosto de 2019.

A autenticidade deste documento pode ser conferida no site http://sei.fazenda.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **17696892** e o código CRC **18880D01**.

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

Governo do Estado do Rio de Janeiro

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

Vice Presidência de Tecnologia

ANEXO III

MODELO DE TERMO DE RECEBIMENTO PROVISÓRIO

Identificação Contrato:	**Nº da OS**
Objeto:	
CONTRATANTE:	
Contratada:	

Por este instrumento, atestamos que os serviços (ou bens), integrantes da O.S. acima identificada, ou conforme definido no Modelo de Execução do contrato supracitado, foram recebidos nesta data e serão objetos de avaliação quanto à adequação da Solução de Tecnologia da Informação e à conformidade de qualidade, de acordo com os Critérios de Aceitação previamente definidos no Modelo de Gestão do Contrato pela CONTRATANTE.

Ressaltamos que o recebimento definitivo destes serviços (ou bens) ocorrerá em até ___dias, desde que não ocorram problemas técnicos ou divergências quanto às especificações constantes do Termo de Referência do Contrato acima identificado.

De Acordo

CONTRATANTE	**CONTRATADA**
Membro da comissão fiscalizadora	**Preposto**

Nome:	***Nome:***
Matrícula:	***Qualificação:***

_____, _____ de _____ de 20___.

Rio de Janeiro, 31 de Maio de 2021

Documento assinado eletronicamente por **Elio Thomé de Souza Filho**, **Analista de Sistemas**, em 31/05/2021, às 17:32, conforme horário oficial de Brasília, com fundamento nos art. 21º e 22º do Decreto nº 46.730, de 9 de agosto de 2019.

Documento assinado eletronicamente por **Daniel Luzente de Lima**, **Diretor**, em 31/05/2021, às 17:32, conforme horário oficial de Brasília, com fundamento nos art. 21º e 22º do Decreto nº 46.730, de 9 de agosto de 2019.

A autenticidade deste documento pode ser conferida no site http://sei.fazenda.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **17697476** e o código CRC **C0190475**.

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

Governo do Estado do Rio de Janeiro

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

Vice Presidência de Tecnologia

ANEXO IV

MODELO DE TERMO DE RECEBIMENTO DEFINITIVO

Este presente termo visa atestar que os produtos e serviços prestados pela empresa [NOME DA EMPRESA] por ocasião do Contrato n°_____/_____, foram fornecidos e homologados pelos fiscais do contrato em conjunto com o gestor do contrato.

O [ÓRGÃO] recebeu e homologou os seguintes produtos e serviços:

ITEM	DESCRIÇÃO	QUANTIDADE

Informa-se que todos os requisitos do Edital referente a está contratação foram cumpridos e que a aceitação do objeto está ratificada.

Encaminha-se a empresa CONTRATADA

ASSINATURAS	
Fiscal Requisitante do Contrato	Gestor do Contrato

(*) Trata-se de um modelo de referência, podendo ser aperfeiçoado durante a execução contratual.

Rio de Janeiro, 31 de Maio de 2021

Documento assinado eletronicamente por **Elio Thomé de Souza Filho**, **Analista de Sistemas**, em 31/05/2021, às 17:32, conforme horário oficial de Brasília, com fundamento nos art. 21º e 22º do Decreto nº 46.730, de 9 de agosto de 2019.

Documento assinado eletronicamente por **Daniel Luzente de Lima**, **Diretor**, em 31/05/2021, às 17:32, conforme horário oficial de Brasília, com fundamento nos art. 21º e 22º do Decreto nº 46.730, de 9 de agosto de 2019.

A autenticidade deste documento pode ser conferida no site http://sei.fazenda.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **17697748** e o código CRC **EB8A4D74**.

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

Governo do Estado do Rio de Janeiro

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

Vice Presidência de Tecnologia

ANEXO V

MODELO DE TERMO DE COMPROMISSO E SIGILO

O _____, sediado em _____, CNPJ n.°_____, doravante denominado CONTRATANTE, e, de outro lado, a _____, sediada em _____ , CNPJ n.°_____, doravante denominada CONTRATADA;

CONSIDERANDO que, em razão do CONTRATO N.º XX/20XX doravante denominado CONTRATO PRINCIPAL, a CONTRATADA poderá ter acesso a informações sigilosas do CONTRATANTE;

CONSIDERANDO a necessidade de ajustar as condições de revelação destas informações sigilosas, bem como definir as regras para o seu uso e proteção;

CONSIDERANDO o disposto na Política de Segurança da Informação do CONTRATANTE; Resolvem celebrar o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO, doravante TERMO, vinculado ao CONTRATO PRINCIPAL, mediante as seguintes cláusulas e condições:

Cláusula Primeira – DO OBJETO

Constitui objeto deste TERMO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela CONTRATADA, no que diz respeito ao trato de informações sigilosas, disponibilizadas pelo CONTRATANTE, por força dos procedimentos necessários para a execução do objeto do CONTRATO PRINCIPAL celebrado entre as partes e em acordo com o que dispõem a Lei nº 12.527, de 18/11/2011 e o Decreto Estadual nº 46.475/2018, que regulamentam os procedimentos para acesso e tratamento de informação classificada em qualquer grau de sigilo.

Cláusula Segunda – DOS CONCEITOS E DEFINIÇÕES

Para os efeitos deste TERMO, são estabelecidos os seguintes conceitos e definições:

INFORMAÇÃO: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

INFORMAÇÃO SIGILOSA: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado.

CONTRATO PRINCIPAL: contrato celebrado entre as partes, ao qual este TERMO se vincula.

Cláusula Terceira – DA INFORMAÇÃO SIGILOSA

Serão consideradas como informação sigilosa, toda e qualquer informação classificada ou não nos graus de sigilo ultrassecreto, secreto e reservado. O TERMO abrangerá toda informação escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: know-how, técnicas, especificações, relatórios, compilações, código fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, cópias, modelos, amostras de ideias, aspectos financeiros e econômicos, definições, informações sobre as

atividades do CONTRATANTE e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não ao CONTRATO PRINCIPAL, doravante denominados INFORMAÇÕES, a que diretamente ou pelos seus empregados, a CONTRATADA venha a ter acesso, conhecimento ou que venha a lhe ser confiada durante e em razão das atuações de execução do CONTRATO PRINCIPAL celebrado entre as partes.

Cláusula Quarta – DOS LIMITES DO SIGILO

As obrigações constantes deste TERMO não serão aplicadas às INFORMAÇÕES que:

I – sejam comprovadamente de domínio público no momento da revelação, exceto se tal fato decorrer de ato ou omissão da CONTRATADA;

II – tenham sido comprovadas e legitimamente recebidas de terceiros, estranhos ao presente TERMO;

III – sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as partes cumpram qualquer medida de proteção pertinente e tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

Cláusula Quinta – DOS DIREITOS E OBRIGAÇÕES

As partes se comprometem a não revelar, copiar, transmitir, reproduzir, utilizar, transportar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que qualquer empregado envolvido direta ou indiretamente na execução do CONTRATO PRINCIPAL, em qualquer nível hierárquico de sua estrutura organizacional e sob quaisquer alegações, faça uso dessas INFORMAÇÕES, que se restringem estritamente ao cumprimento do CONTRATO PRINCIPAL.

Parágrafo Primeiro – A CONTRATADA se compromete a não efetuar qualquer tipo de cópia da informação sigilosa sem o consentimento expresso e prévio do CONTRATANTE.

Parágrafo Segundo – A CONTRATADA compromete-se a dar ciência e obter o aceite formal da direção e empregados que atuarão direta ou indiretamente na execução do CONTRATO PRINCIPAL sobre a existência deste TERMO bem como da natureza sigilosa das informações.

I – A CONTRATADA deverá firmar acordos por escrito com seus empregados visando garantir o cumprimento de todas as disposições do presente TERMO e dará ciência ao CONTRATANTE dos documentos comprobatórios.

Parágrafo Terceiro – A CONTRATADA obriga-se a tomar todas as medidas necessárias à proteção da informação sigilosa do CONTRATANTE, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pelo CONTRATANTE.

Parágrafo Quarto – Cada parte permanecerá como fiel depositária das informações reveladas à outra parte em função deste TERMO.

I – Quando requeridas, as INFORMAÇÕES deverão retornar imediatamente ao proprietário, bem como todas e quaisquer cópias eventualmente existentes.

Parágrafo Quinto – A CONTRATADA obriga-se por si, sua controladora, suas controladas, coligadas, representantes, procuradores, sócios, acionistas e cotistas, por terceiros eventualmente consultados, seus empregados e contratados, assim como por quaisquer outras pessoas vinculadas à CONTRATADA, direta ou indiretamente, a manter sigilo, bem como a limitar a utilização das informações disponibilizadas em face da execução do CONTRATO PRINCIPAL.

Parágrafo Sexto - A CONTRATADA, na forma disposta no parágrafo primeiro, acima, também se obriga a:

I – Não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor das INFORMAÇÕES, no território brasileiro ou no exterior, para nenhuma pessoa, física ou jurídica, e para nenhuma outra finalidade que não seja exclusivamente relacionada ao objetivo aqui referido, cumprindo-lhe adotar cautelas e precauções adequadas no sentido de impedir o uso indevido por qualquer pessoa que, por qualquer razão, tenha acesso a elas;

II – Responsabilizar-se por impedir, por qualquer meio em direito admitido, arcando com todos os custos do impedimento, mesmo judiciais, inclusive as despesas processuais e outras despesas derivadas, a divulgação ou utilização das INFORMAÇÕES por seus agentes, representantes ou por terceiros;

III – Comunicar ao CONTRATANTE, de imediato, de forma expressa e antes de qualquer divulgação, caso tenha que revelar qualquer uma das INFORMAÇÕES, por determinação judicial ou ordem de atendimento obrigatório determinado por órgão competente; e

IV – Identificar as pessoas que, em nome da CONTRATADA, terão acesso às informações sigilosas.

Cláusula Sexta – DA VIGÊNCIA

O presente TERMO tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de sua assinatura até expirar o prazo de classificação da informação a que a CONTRATADA teve acesso em razão do CONTRATO PRINCIPAL.

A vigência deste Termo independe do prazo de vigência do contrato assinado.

Cláusula Sétima – DAS PENALIDADES

A quebra do sigilo e/ou da confidencialidade das INFORMAÇÕES, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislações em vigor que tratam desse assunto, podendo até culminar na rescisão do CONTRATO PRINCIPAL firmado entre as PARTES. Neste caso, a CONTRATADA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pelo CONTRATANTE, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis, conforme art. 87 da Lei nº. 8.666/93.

Cláusula Oitava – DISPOSIÇÕES GERAIS

Este TERMO de Confidencialidade é parte integrante e inseparável do CONTRATO PRINCIPAL.

Parágrafo Primeiro – Surgindo divergências quanto à interpretação do disposto neste instrumento, ou quanto à execução das obrigações dele decorrentes, ou constatando-se casos omissos, as partes buscarão solucionar as divergências de acordo com os princípios de boa-fé, da equidade, da razoabilidade, da economicidade e da moralidade.

Parágrafo Segundo – O disposto no presente TERMO prevalecerá sempre em caso de dúvida e, salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos conexos firmados entre as partes quanto ao sigilo de informações, tal como aqui definidas.

Parágrafo Terceiro - Havendo necessidade legal devido a Programas de Governo, a CONTRATADA assume o compromisso de assinar Termo de Sigilo (ou equivalente) adicional relacionado ao Programa, prevalecendo as cláusulas mais restritivas em benefício do CONTRATANTE.

Parágrafo Quarto – Ao assinar o presente instrumento, a CONTRATADA manifesta sua concordância no sentido de que:

I – O CONTRATANTE terá o direito de, a qualquer tempo e sob qualquer motivo, auditar e monitorar as atividades da CONTRATADA;

II – A CONTRATADA deverá disponibilizar, sempre que solicitadas formalmente pelo CONTRATANTE, todas as informações requeridas pertinentes ao CONTRATO PRINCIPAL;

III – A omissão ou tolerância das partes, em exigir o estrito cumprimento das condições estabelecidas neste instrumento, não constituirá novação ou renúncia, nem afetará os direitos, que poderão ser exercidos a qualquer tempo;

IV – Todas as condições, TERMOS e obrigações ora constituídos serão regidos pela legislação e regulamentação brasileiras pertinentes;

V – O presente TERMO somente poderá ser alterado mediante TERMO aditivo firmado pelas partes;

VI – Alterações do número, natureza e quantidade das informações disponibilizadas para a CONTRATADA não descaracterizarão ou reduzirão o compromisso e as obrigações pactuadas neste TERMO, que permanecerá válido e com todos seus efeitos legais em qualquer uma das situações tipificadas neste instrumento;

VII – O acréscimo, complementação, substituição ou esclarecimento de qualquer uma das informações disponibilizadas para a CONTRATADA, serão incorporados a este TERMO, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações iniciais disponibilizadas, sendo necessário a formalização de TERMO aditivo a CONTRATO PRINCIPAL;

VIII – Este TERMO não deve ser interpretado como criação ou envolvimento das Partes, ou suas filiadas, nem em obrigação de divulgar INFORMAÇÕES para a outra Parte, nem como obrigação de celebrarem qualquer outro acordo entre si.

Cláusula Nona – DO FORO

O CONTRATANTE elege o foro da _____ , onde está localizada a sede do CONTRATANTE, para dirimir quaisquer dúvidas originadas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO é assinado pelas partes em 2 vias de igual teor e um só efeito.

_____, _____ de _____ de 20____

De acordo.

CONTRATANTE

CONTRATADA

Matrícula: _____

Testemunhas

Testemunha 1 _____

Testemunha 2 _____

Rio de Janeiro, 31 de Maio de 2021

Documento assinado eletronicamente por **Elio Thomé de Souza Filho**, **Analista de Sistemas**, em 31/05/2021, às 17:32, conforme horário oficial de Brasília, com fundamento nos art. 21º e 22º do Decreto nº 46.730, de 9 de agosto de 2019.

Documento assinado eletronicamente por **Daniel Luzente de Lima**, **Diretor**, em 31/05/2021, às 17:32, conforme horário oficial de Brasília, com fundamento nos art. 21º e 22º do Decreto nº 46.730, de 9 de agosto de 2019.

A autenticidade deste documento pode ser conferida no site http://sei.fazenda.rj.gov.br/sei/controlador_externo.php?

acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **17698140** e o código CRC **E19DE23E**.

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

Governo do Estado do Rio de Janeiro

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

Vice Presidência de Tecnologia

ANEXO VI

PLANILHA DE COMPOSIÇÃO DE LANCES

Descrição	Quantidade	Valor Unitário	Valor Total
Switch Core	42		
Switch Core - Módulo de Interface Tipo I	34		
Switch Core - Módulo de Interface Tipo II	60		
Switch Core - Módulo de Interface Tipo III	51		
Switch Core - Módulo de Interface Tipo IV	48		
Switch de Distribuição - Tipo I	166		
Switch de Distribuição - Tipo II	64		
Switch de Distribuição - Tipo III	241		
Switch de Distribuição - Tipo IV	80		
Switch de Acesso - Tipo I	1237		
Switch de Acesso - Tipo II	698		
Controladora WLAN	66		
Ponto de Acesso WLAN	3833		
Plataforma de Gerenciamento	23		
INTERFACE 100GB QSFP SR	581		
INTERFACE 100GB QSFP LR	102		
INTERFACE 40GB QSFP SR	840		
INTERFACE 40GB QSFP LR	250		
INTERFACE 25GB SFP28 SR	558		
INTERFACE 25GB SFP28 LR	134		

INTERFACE 10GB SFP+ SR	906		
INTERFACE 10GB SFP+ LR	552		
INTERFACE 1GB SFP SX	283		
INTERFACE 1GB SFP LX	93		
CONVERSOR QSFP PARA 4 SFP+	686		
VALOR TOTAL DA PROPOSTA			

Os preços deverão contemplar todos os custos para a prestação do serviço de acordo com as condições estabelecidas neste Termo de Referência.

Rio de Janeiro, 31 de Maio de 2021.

Documento assinado eletronicamente por **Elio Thomé de Souza Filho**, **Analista de Sistemas**, em 31/05/2021, às 17:32, conforme horário oficial de Brasília, com fundamento nos art. 21º e 22º do Decreto nº 46.730, de 9 de agosto de 2019.

Documento assinado eletronicamente por **Daniel Luzente de Lima**, **Diretor**, em 31/05/2021, às 17:32, conforme horário oficial de Brasília, com fundamento nos art. 21º e 22º do Decreto nº 46.730, de 9 de agosto de 2019.

A autenticidade deste documento pode ser conferida no site http://sei.fazenda.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **17698806** e o código CRC **54828BE2**.

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