EDITAL DE LICITAÇÃO

Os Grupos 1 e 2 – são de ampla concorrência

Os Itens 17 e 18 - são exclusivos para ME e EPP

Torna-se público, para conhecimento dos interessados, que **a DEFENSORIA PÚBLICA DO ESTADO DO TOCANTINS, UASG: 926040, por meio de seu Pregoeiro**, designado pela **Portaria nº 304, de 22 de março de 2022,** fará realizar licitação, na modalidade **PREGÃO ELETRÔNICO,** do tipo **MENOR PREÇO**, pelo sistema de registro de preços, para eventual contratação de empresa fornecedora de *switches* gerenciáveis, cordões ópticos, *access points*, *sofware* de gerencia, serviços de instalação e treinamento especializados, para atender as necessidades da Defensoria Pública do Estado do Tocantins, nos quantitativos e especificações constantes do Termo de Referência, ANEXO – I ao presente Edital. A licitação será regida pela Lei 10.520/2002, Decreto Federal 10.024/2019, Decreto Federal 7.892/2013, Lei Complementar nº 123/2006, Decreto Federal 8.538/2015, e subsidiariamente pela Lei nº 8.666, de 21 de junho de 1993 e suas alterações, além das demais normas pertinentes e das condições estabelecidas no presente Edital e seus Anexos.

1. DA SESSÃO PÚBLICA DO PREGÃO ELETRÔNICO

PROCESSO INTERNO: 22.0.000001581-8

PREGÃO ELETRÔNICO: 46/2022

DIA: 07/11/2022

HORÁRIO: 08h

ENDEREÇO ELETRÔNICO: www.compras.gov.br

CÓDIGO UASG: 926040

DISPONIBILIDADE DO EDITAL: www.compras.gov.br e http://www.defensoria.to.def.br/

1.1. Constitui parte integrante deste Edital

1.1.1. Anexo I – Termo de Referência

1.1.2. Anexo II – Minuta Ata de Registro de Preços

1.1.3. Anexo III – Minuta de Contrato

1.1.4. Anexo IV – Modelo da Proposta Readequada

2. DO OBJETO

2.1. O objeto da presente licitação é a escolha da melhor proposta para a eventual contratação de empresa fornecedora de *switches* gerenciáveis, cordões ópticos, *access points*, *sofware* de gerencia, serviços de instalação e treinamento especializados, nos quantitativos e especificações constantes neste Edital e seus anexos.

2.2. A disputa se dará por item, e o critério de julgamento adotado será:

a) para os grupos 1 e 2, menor preço por grupo.

b) para os itens 17 e 18, menor preço por item;

2.3. Em caso de discordância existente entre as especificações descritas no Comprasnet e as especificações constantes deste Edital, prevalecerão as últimas.

3. DA DESPESA E DOS RECURSOS ORÇAMENTÁRIOS

3.1. A despesa com a execução do objeto desta licitação é estimada em **R$ 5.882.032,81 (cinco milhões, oitocentos e oitenta e dois mil trinta e dois reais e oitenta e um centavos),** conforme Anexo I – Termo de Referência.

3.2. As despesas decorrentes da presente licitação correrão com recursos oriundos do Tesouro Estadual, consignados no Orçamento da Defensoria Pública do Estado do Tocantins, cuja programação é a seguinte:

Programa de trabalho: 03.091.1173.1112; 03.126.1143.2254; 03.091.1173.4004

Elemento de Despesa: 3.3.90.40 e 4.4.90.52

Fonte: 1.500.0000.000, detalhamento 666666; 1.759.0000.240 detalhamento 005035

UG: 49010 e 50350

4. DO CREDENCIAMENTO

4.1. O Credenciamento é o nível básico do registro cadastral no SICAF, que permite a participação dos interessados na modalidade licitatória Pregão, em sua forma eletrônica.

4.2. O cadastro no SICAF deverá ser feito no Portal de Compras do Governo Federal, no sítio www.compras.gov.br, por meio de certificado digital conferido pela Infraestrutura de Chaves Públicas Brasileira – ICP - Brasil.

4.3. O credenciamento junto ao provedor do sistema implica a responsabilidade do licitante ou de seu representante legal e a presunção de sua capacidade técnica para realização das transações inerentes a este Pregão.

4.4. O licitante responsabiliza-se exclusiva e formalmente pelas transações efetuadas em seu nome, assume como firmes e verdadeiras suas propostas e seus lances, inclusive os atos praticados diretamente ou por seu representante, excluída a responsabilidade do provedor do sistema ou do órgão ou entidade promotora da licitação por eventuais danos decorrentes de uso indevido das credenciais de acesso, ainda que por terceiros.

5. DA PARTICIPAÇÃO NO PREGÃO

5.1. Poderão participar deste Pregão interessados cujo ramo de atividade seja compatível com o objeto desta licitação, e que estejam com Credenciamento regular no Sistema de Cadastramento Unificado de Fornecedores – SICAF, conforme disposto no art. 9º da IN SEGES/MP nº 3, de 2018.

5.1.1. Os licitantes deverão utilizar o certificado digital para acesso ao Sistema.

5.1.2. Os grupos 1 e 2 são de ampla concorrência;

5.1.3. Os itens 17 e 18 são exclusivos para Micro Empresas e Empresas de Pequeno Porte.

5.1.3.1. Será concedido tratamento favorecido para as microempresas e empresas de pequeno porte, nos limites previstos da Lei Complementar nº 123, de 2006.

5.2. Não poderão participar desta licitação os interessados:

5.2.1. proibidos de participar de licitações e celebrar contratos administrativos, na forma da legislação vigente;

5.2.1.1. Não serão admitidos participantes cuja sanção, de suspensão temporária ou de impedimento vigente, tenha sido aplicada por qualquer órgão ou entidade da Administração Pública, pouco importando a órbita federativa.

5.2.2. que não atendam às condições deste Edital e seu(s) anexo(s);

5.2.3. estrangeiros que não tenham representação legal no Brasil com poderes expressos para receber citação e responder administrativa ou judicialmente;

5.2.4. que se enquadrem nas vedações previstas no artigo 9º da Lei nº 8.666, de 1993;

5.2.5. que estejam sob falência, concurso de credores, concordata ou em processo de dissolução ou liquidação;

5.2.6. entidades empresariais que estejam reunidas em consórcio;

5.2.7. Organizações da Sociedade Civil de Interesse Público - OSCIP, atuando nessa condição (Acórdão nº 746/2014-TCU-Plenário).

5.3. Como condição para participação no Pregão, a licitante assinalará "sim" ou "não" em campo próprio do sistema eletrônico, relativo às seguintes declarações:

5.3.1. que cumpre os requisitos estabelecidos no artigo 3° da Lei Complementar nº 123, de 2006, estando apta a usufruir do tratamento favorecido estabelecido em seus arts. 42 a 49;

5.3.1.1. no grupo exclusivo para participação de microempresas e empresas de pequeno porte, a assinalação do campo "não" impedirá o prosseguimento no certame;

5.3.1.2. nos grupos em que a participação não for exclusiva para microempresas e empresas de pequeno porte, a assinalação do campo "não" apenas produzirá o efeito de o licitante não ter direito ao tratamento favorecido previsto na Lei Complementar nº 123, de 2006, mesmo que microempresa, empresa de pequeno porte ou sociedade cooperativa.

5.3.2. que está ciente e concorda com as condições contidas no Edital e seus anexos;

5.3.3. que cumpre os requisitos para a habilitação definidos no Edital e que a proposta apresentada está em conformidade com as exigências editalícias;

5.3.4. que inexistem fatos impeditivos para sua habilitação no certame, ciente da obrigatoriedade de declarar ocorrências posteriores;

5.3.5. que não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do artigo 7°, XXXIII, da Constituição;

5.3.6. que a proposta foi elaborada de forma independente.

5.3.7. que não possui, em sua cadeia produtiva, empregados executando trabalho degradante ou forçado, observando o disposto nos incisos III e IV do art. 1º e no inciso III do art. 5º da Constituição Federal;

5.3.8. que cumpre reserva de cargos prevista em lei para pessoa com deficiência ou para reabilitado da Previdência Social e que atendam às regras de acessibilidade previstas na legislação, conforme disposto no art. 93 da Lei nº 8.213, de 24 de julho de 1991.

5.4. A declaração falsa relativa ao cumprimento de qualquer condição sujeitará o licitante às sanções previstas em lei e neste Edital.

6. DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

6.1. Os licitantes encaminharão, exclusivamente por meio do sistema, concomitantemente com os documentos de habilitação exigidos no edital, proposta com a descrição do objeto ofertado e o preço, até a data e horário limites para entrega de propostas.

6.2. O envio da proposta, acompanhada dos documentos de habilitação exigidos neste Edital, ocorrerá por meio de chave de acesso e senha.

6.3. Os licitantes poderão deixar de apresentar os documentos de habilitação que constem do SICAF, assegurado aos demais licitantes o direito de acesso aos dados constantes dos sistemas.

6.4. As Microempresas e Empresas de Pequeno Porte deverão encaminhar a documentação de habilitação, ainda que haja alguma restrição de regularidade fiscal e trabalhista, nos termos do art. 43, § 1º da LC nº 123, de 2006.

6.5. Incumbirá ao licitante acompanhar as operações no sistema eletrônico durante a sessão pública do Pregão, ficando responsável pelo ônus decorrente da perda de negócios, diante da inobservância de quaisquer mensagens emitidas pelo sistema ou de sua desconexão.

6.5.1. Até a data e o horário estabelecidos para abertura da sessão pública, os licitantes poderão retirar ou substituir a proposta e os documentos de habilitação anteriormente inseridos no sistema;

6.5.2. Não será estabelecida, nessa etapa do certame, ordem de classificação entre as propostas apresentadas, o que somente ocorrerá após a realização dos procedimentos de negociação e julgamento da proposta.

6.5.3. Os documentos que compõem a proposta e a habilitação do licitante melhor classificado somente serão disponibilizados para avaliação do pregoeiro e para acesso público após o encerramento do envio de lances.

7. DO PREENCHIMENTO DA PROPOSTA NO PORTAL DE COMPRAS

7.1. O licitante deverá enviar sua proposta mediante o preenchimento, no sistema eletrônico, dos seguintes campos:

7.1.1. Valor unitário e total do item, conforme planilha respectiva constante do Termo de Referência.

7.1.2. Descrição do objeto, contendo as informações similares à especificação do Termo de Referência: indicando, no que for aplicável, o modelo, a marca, prazo de validade ou de garantia.

7.2. Todas as especificações do objeto contidas na proposta vinculam a Contratada.

7.3. Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente no fornecimento dos bens.

7.4. Os preços ofertados, tanto na proposta inicial, quanto na etapa de lances, serão de exclusiva responsabilidade do licitante, não lhe assistindo o direito de pleitear qualquer alteração, sob alegação de erro, omissão ou qualquer outro pretexto.

7.5. O prazo de validade da proposta não será inferior a **60 (sessenta) dias**, a contar da data de sua apresentação.

8. DA ABERTURA DA SESSÃO, CLASSIFICAÇÃO DAS PROPOSTAS E FORMULAÇÃO DE LANCES

8.1. A abertura da presente licitação dar-se-á em sessão pública, por meio de sistema eletrônico, na data, horário e local indicados neste Edital.

8.2. O Pregoeiro verificará as propostas apresentadas, desclassificando desde logo aquelas que não estejam em conformidade com os requisitos estabelecidos neste Edital, contenham vícios insanáveis ou não apresentem as especificações técnicas exigidas no Termo de Referência.

8.2.1. Também será desclassificada a proposta que identifique o licitante.

8.2.2. A desclassificação será sempre fundamentada e registrada no sistema, com acompanhamento em tempo real por todos os participantes.

8.2.3. A não desclassificação da proposta não impede o seu julgamento definitivo em sentido contrário, levado a efeito na fase de aceitação.

8.3. O sistema ordenará automaticamente as propostas classificadas, sendo que somente estas participarão da fase de lances.

8.4. O sistema disponibilizará campo próprio para troca de mensagens entre o Pregoeiro e os licitantes.

8.5. Iniciada a etapa competitiva, os licitantes deverão encaminhar lances exclusivamente por meio do sistema eletrônico, sendo imediatamente informados do seu recebimento e do valor consignado no registro.

8.5.1. O lance deverá ser ofertado pelo valor unitário do item.

8.6. Os licitantes poderão oferecer lances sucessivos, observando o horário fixado para abertura da sessão e as regras estabelecidas no Edital.

8.7. O licitante somente poderá oferecer lance de valor inferior ao último por ele ofertado e registrado pelo sistema.

8.8. O intervalo mínimo de diferença de valores entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta deverá ser 0,5% (meio por cento).

8.9. O intervalo entre os lances enviados pelo mesmo licitante não poderá ser inferior a vinte (20) segundos e o intervalo entre lances não poderá ser inferior a três (3) segundos, sob pena de serem automaticamente descartados pelo sistema os respectivos lances.

8.10. Será adotado para o envio de lances no pregão eletrônico o modo de disputa “aberto”, em que os licitantes apresentarão lances públicos e sucessivos, com prorrogações.

8.11. A etapa de lances da sessão pública terá duração de dez minutos e, após isso, será prorrogada automaticamente pelo sistema quando houver lance ofertado nos últimos dois minutos do período de duração da sessão pública.

8.12. A prorrogação automática da etapa de lances, de que trata o item anterior, será de dois minutos e ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive no caso de lances intermediários.

8.13. Não havendo novos lances na forma estabelecida nos itens anteriores, a sessão pública encerrar-se-á automaticamente.

8.14. Encerrada a fase competitiva sem que haja a prorrogação automática pelo sistema, poderá o pregoeiro, assessorada pela equipe de apoio, justificadamente, admitir o reinício da sessão pública de lances, em prol da consecução do melhor preço.

8.15. Não serão aceitos dois ou mais lances de mesmo valor, prevalecendo aquele que for recebido e registrado em primeiro lugar.

8.16. Durante o transcurso da sessão pública, os licitantes serão informados, em tempo real, do valor do menor lance registrado, vedada a identificação do licitante.

8.17. No caso de desconexão com o Pregoeiro, no decorrer da etapa competitiva do Pregão, o sistema eletrônico poderá permanecer acessível aos licitantes para a recepção dos lances.

8.18. Quando a desconexão do sistema eletrônico para o Pregoeiro a persistir por tempo superior a dez minutos, a sessão pública será suspensa e reiniciada somente após decorridas vinte e quatro horas da comunicação do fato pelo Pregoeiro aos participantes, no sítio eletrônico utilizado para divulgação.

8.19. O Critério de julgamento adotado será:

a) para os grupos 1 e 2, menor preço por grupo.

b) para os itens 17 e 18, menor preço por item; conforme definido no item 3 do ANEXO I ao Edital.

8.20. Caso o licitante não apresente lances, concorrerá com o valor de sua proposta.

8.21. Em relação a itens não exclusivos para participação de microempresas e empresas de pequeno porte, uma vez encerrada a etapa de lances, será efetivada a verificação automática, junto à Receita Federal, do porte da entidade empresarial. O sistema identificará em coluna própria as microempresas e empresas de pequeno porte participantes, procedendo à comparação com os valores da primeira colocada, se esta for

empresa de maior porte, assim como das demais classificadas, para o fim de aplicar-se o disposto nos arts. 44 e 45 da LC nº 123, de 2006, regulamentada pelo Decreto nº 8.538, de 2015.

8.22. Nessas condições, as propostas de microempresas e empresas de pequeno porte que se encontrarem na faixa de até 5% (cinco por cento) acima da melhor proposta ou melhor lance serão consideradas empatadas com a primeira colocada.

8.23. A melhor classificada nos termos do item anterior terá o direito de encaminhar uma última oferta para desempate, obrigatoriamente em valor inferior ao da primeira colocada, no prazo de 5 (cinco) minutos controlados pelo sistema, contados após a comunicação automática para tanto.

8.24. Caso a microempresa ou a empresa de pequeno porte melhor classificada desista ou não se manifeste no prazo estabelecido, serão convocadas as demais licitantes microempresa e empresa de pequeno porte que se encontrem naquele intervalo de 5% (cinco por cento), na ordem de classificação, para o exercício do mesmo direito, no prazo estabelecido no subitem anterior.

8.25. No caso de equivalência dos valores apresentados pelas microempresas e empresas de pequeno porte que se encontrem nos intervalos estabelecidos nos subitens anteriores, será realizado sorteio entre elas para que se identifique aquela que primeiro poderá apresentar melhor oferta.

8.26. Havendo eventual empate entre propostas ou lances, o critério de desempate será aquele previsto no art. 3º, § 2º, da Lei nº 8.666, de 1993, assegurando-se a preferência, sucessivamente, aos bens produzidos:

8.26.1. no País;

8.26.2. por empresas brasileiras;

8.26.3. por empresas que invistam em pesquisa e no desenvolvimento de tecnologia no País;

8.26.4. por empresas que comprovem cumprimento de reserva de cargos prevista em lei para pessoa com deficiência ou para reabilitado da Previdência Social e que atendam às regras de acessibilidade previstas na legislação.

8.27. Persistindo o empate, a proposta vencedora será sorteada pelo sistema eletrônico dentre as propostas empatadas.

8.28. Encerrada a etapa de envio de lances da sessão pública, o Pregoeiro deverá encaminhar, pelo sistema eletrônico, contraproposta ao licitante que tenha apresentado o melhor preço, para que seja obtida melhor proposta, vedada a negociação em condições diferentes das previstas neste Edital.

8.28.1. A negociação será realizada por meio do sistema, podendo ser acompanhada pelos demais licitantes.

8.28.2. A negociação pode se resumir à provocação do licitante para se manifestar quanto à possibilidade de redução do preço no prazo que o Pregoeiro assinalar, prevalecendo a última proposta em caso de silêncio.

8.28.3. O Pregoeiro solicitará ao licitante melhor classificado que, no prazo de 2 (duas) horas, envie a proposta adequada ao último lance ofertado após a negociação realizada, acompanhada, se for o caso, dos documentos complementares, quando necessários à confirmação daqueles exigidos neste Edital e já apresentados.

8.29. Após a negociação do preço, o Pregoeiro iniciará a fase de aceitação e julgamento da proposta, podendo desde logo desclassifica-la acaso constatado desatendimento das demais condições de participação ou habilitação.

9. DA ACEITABILIDADE DA PROPOSTA VENCEDORA

9.1. Encerrada a etapa de negociação, o Pregoeiro examinará a proposta classificada em primeiro lugar quanto à adequação ao objeto e à compatibilidade do preço em relação ao máximo estipulado para contratação neste Edital e em seus anexos, observado o disposto no parágrafo único do art. 7º e no § 9º do art. 26 do Decreto n.º 10.024/2019.

9.2. Será desclassificada a proposta ou o lance vencedor, apresentar preço final superior ao preço máximo

fixado (Acórdão nº 1455/2018 -TCU - Plenário), ou que apresentar preço manifestamente inexequível.

9.2.1. Considera-se preço máximo o valor estimado para o item e para o grupo.

9.2.2. Serão consideradas inexequíveis as propostas dos licitantes que sejam inferiores a 70% **do mais baixo entre os valores previstos no art. 48, § 1º, "a" e "b" da Lei 8.666/1993. Isto é: (a) o valor orçado pela administração pública e (b) a média aritmética dos valores das propostas superiores a 50% do valor orçado pela administração.**

9.2.3. Qualquer interessado poderá requerer que se realizem diligências para aferir a exequibilidade e a legalidade das propostas, devendo apresentar as provas ou os indícios que fundamentam a suspeita;

9.2.4. Na hipótese de necessidade de suspensão da sessão pública para a realização de diligências, com vistas ao saneamento das propostas, a sessão pública somente poderá ser reiniciada mediante aviso prévio no sistema com, no mínimo, vinte e quatro horas de antecedência, e a ocorrência será registrada em ata;

9.3. Se a proposta ou lance vencedor for desclassificado, o Pregoeiro examinará a proposta ou lance subsequente, e, assim sucessivamente, na ordem de classificação.

9.4. Havendo necessidade, o Pregoeiro suspenderá a sessão, informando no "*chat*" a nova data e horário para a sua continuidade.

9.5. O Pregoeiro deve encaminhar, por meio do sistema eletrônico, contraproposta ao licitante que apresentou o lance mais vantajoso, com o fim de negociar a obtenção de melhor preço, vedada a negociação em condições diversas das previstas neste Edital.

9.5.1. Também nas hipóteses em que o Pregoeiro não aceitar a proposta e passar à subsequente, poderá negociar com o licitante para que seja obtido preço melhor.

9.5.2. A negociação será realizada por meio do sistema, podendo ser acompanhada pelos demais licitantes.

9.6. Encerrada a análise quanto à aceitação da proposta, o Pregoeiro novamente verificará a habilitação do licitante, observado o disposto neste Edital.

10. DA HABILITAÇÃO

10.1. Como condição prévia ao exame da documentação de habilitação do licitante detentor da proposta classificada em primeiro lugar, o Pregoeiro verificará o eventual descumprimento das condições de participação, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

10.1.1. SICAF;

10.1.2. Consulta Consolidada de Pessoa Jurídica do Tribunal de Contas da União (https://certidoes-apf.apps.tcu.gov.br/).

10.1.3. A consulta aos cadastros será realizada em nome da empresa licitante e também de seu sócio majoritário, por força do artigo 12 da Lei n° 8.429, de 1992, que prevê, dentre as sanções impostas ao responsável pela prática de ato de improbidade administrativa, a proibição de contratar com o Poder Público, inclusive por intermédio de pessoa jurídica da qual seja sócio majoritário.

10.1.3.1. Caso conste na Consulta de Situação do Fornecedor a existência de Ocorrências Impeditivas Indiretas, o gestor diligenciará para verificar se houve fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas.

10.1.3.2. A tentativa de burla será verificada por meio dos vínculos societários, linhas de fornecimento similares, dentre outros.

10.1.3.3. Constatada a existência de ocorrência impeditiva indireta, o licitante será convocado para manifestação previamente à sua desclassificação.

10.1.4. Constatada a existência de sanção, o Pregoeiro reputará o licitante inabilitado, por falta de condição de participação.

10.1.5. No caso de inabilitação, haverá nova verificação, pelo sistema, da eventual ocorrência do empate

ficto, previsto nos arts. 44 e 45 da Lei Complementar nº 123, de 2006, seguindo-se a disciplina antes estabelecida para aceitação da proposta subsequente.

10.2. Caso atendidas as condições de participação, a habilitação dos licitantes será verificada por meio do SICAF, nos documentos por ele abrangidos em relação à habilitação jurídica, à regularidade fiscal e trabalhista, à qualificação econômica financeira e habilitação técnica.

10.2.1. Caso os documentos exigidos para habilitação não estejam contemplados no SICAF devem ser encaminhados.

10.2.2. A consulta aos sítios eletrônicos oficiais emissores de certidões, feita pelo Pregoeiro, constitui meio legal de prova para fins de habilitação, conforme art. 43, §3º, do Decreto 10.024, de 2019.

10.3. Havendo a necessidade de envio de documentos de habilitação complementares, necessários à confirmação daqueles exigidos neste Edital e já apresentados, o licitante será convocado a encaminhá-los, em formato digital, via sistema, no prazo de 2 (duas) horas, sob pena de inabilitação.

10.3.1. Documentos complementares são aqueles que se prestam à confirmação dos já apresentados, vedada a inclusão de documento que deveria ter sido cadastrado para habilitação juntamente com a proposta inicial.

10.3.2. A vedação da inclusão de documento novo não alcança documento ausente, comprobatório de condição atendida pelo licitante quando apresentou sua proposta, e que não foi juntado com os demais documentos de habilitação e/ou proposta, por equivoco ou falha. (Acórdãos TCU - Plenário: 1.211/2021, 2.443/2021, 2.568/2021, 468/2022 e 988/2022).

10.4. Somente haverá a necessidade de comprovação do preenchimento de requisitos mediante apresentação dos documentos originais não-digitais quando houver dúvida em relação à integridade do documento digital.

10.5. Não serão aceitos documentos de habilitação com indicação de CNPJ/CPF diferentes do licitante, salvo aqueles legalmente permitidos.

10.6. Se o licitante for a matriz, todos os documentos deverão estar em nome da matriz, e se o licitante for a filial, todos os documentos deverão estar em nome da filial, exceto aqueles documentos que, pela própria natureza, comprovadamente, forem emitidos somente em nome da matriz.

10.6.1. Serão aceitos registros de CNPJ de licitante matriz e filial com diferenças de números de documentos pertinentes ao CND e ao CRF/FGTS, quando for comprovada a centralização do recolhimento dessas contribuições.

10.7. Ressalvado o disposto no item 6.3, os licitantes deverão encaminhar, exclusivamente por meio do sistema, nos termos deste Edital, a documentação relacionada nos itens a seguir, para fins de habilitação:

10.8. HABILITAÇÃO JURÍDICA:

10.8.1. No caso de empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

10.8.2. Em se tratando de microempreendedor individual – MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio www.portaldoempreendedor.gov.br;

10.8.3. No caso de sociedade empresária ou sociedade limitada unipessoal: ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado na Junta Comercial da respectiva sede, acompanhado de documento comprobatório de seus administradores;

10.8.4. Inscrição no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz, no caso de ser o participante sucursal, filial ou agência;

10.8.5. No caso de sociedade simples: inscrição do ato constitutivo no Registro Civil das Pessoas Jurídicas do local de sua sede, acompanhada de prova da indicação dos seus administradores;

10.8.6. No caso de cooperativa: ata de fundação e estatuto social em vigor, com a ata da assembleia que o

aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, bem como o registro de que trata o art. 107 da Lei nº 5.764, de 1971;

10.8.7. No caso de empresa ou sociedade estrangeira em funcionamento no País: decreto de autorização;

10.8.8. Os documentos acima deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

10.8.9. Cédula de identidade, ou documento equivalente, do representante legal, eleito nos atos constitutivos como administrador, qualquer que seja a modalidade empresária.

10.9. REGULARIDADE FISCAL E TRABALHISTA

10.9.1. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso;

10.9.2. Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02/10/2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.

10.9.3. Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

10.9.4. Prova de inexistência de débitos inadimplidos perante a justiça do trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943;

10.9.5. Prova de regularidade com a Fazenda Estadual e Municipal do domicílio ou sede do licitante, relativa à atividade em cujo exercício contrata ou concorre;

10.9.6. Caso o licitante seja considerado isento dos tributos estaduais relacionados ao objeto licitatório, deverá comprovar tal condição mediante declaração da Fazenda Estadual do seu domicílio ou sede, ou outra equivalente, na forma da lei;

10.10. QUALIFICAÇÃO ECONÔMICO-FINANCEIRA

10.10.1. Certidão negativa de falência expedida pelo distribuidor da sede do licitante;

10.10.2. Balanço Patrimonial acompanhado do resultado do último exercício social, exigível e apresentado na forma da lei, registrado na Junta Comercial do Estado da sede da licitante; ou Balanço Patrimonial via Sistema Público de Escrituração Fiscal Digital - SPED com recibo de entrega, que comprovem a boa situação financeira da empresa, vedada a sua substituição por balancetes ou balanços provisórios, podendo ser atualizados por índices oficiais quando encerrado há mais de 3 (três) meses da data de apresentação da proposta. Na apresentação do Balanço Patrimonial digital, a autenticação será comprovada pelo recibo de entrega emitido pelo Sistema Público de Escrituração Digital – SPED;

10.10.3. No caso de empresa constituída no exercício social vigente, admite-se a apresentação de balanço patrimonial e demonstrações contábeis referentes ao período de existência da sociedade;

10.10.4. É admissível o balanço intermediário, se decorrer de lei ou contrato/estatuto social.

10.10.5. Comprovação da boa situação financeira da empresa mediante obtenção de índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), superiores a 1 (um), obtidos pela aplicação das seguintes fórmulas:

$$LG = \frac{\text{Ativo Circulante + Realizável a Longo Prazo}}{\text{Passivo Circulante + Passivo Não Circulante}}$$

$$SG = \frac{\text{Ativo Total}}{\text{Passivo Circulante + Passivo Não Circulante}}$$

$$LC = \frac{\text{Ativo Circulante}}{\text{Passivo Circulante}}$$

10.10.6. As empresas, que apresentarem resultado inferior ou igual a 1(um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), deverão comprovar patrimônio líquido de 5% (cinco por cento) do valor total estimado da contratação ou do item pertinente.

10.10.7. Para fins de habilitação será considerado como data de validade do balanço patrimonial o dia 30 de abril.

10.10.8. Sendo o participante filial também será aceito balanço patrimonial e atestado de capacidade técnica em nome da matriz, conforme Acórdãos Plenário 3.056/2008 e 1277/2015, TCU.

10.11. QUALIFICAÇÃO TÉCNICA

10.11.1. Caso não conste qualificação técnica junto ao SICAF, ou o atestado ali inserido seja incompatível, deverá o licitante detentor da melhor proposta apresentar cópia de 01 (um) atestado de capacidade técnica ou certidão, expedidos por pessoa jurídica de direito público ou privado, em documento da emitente que conste a razão social, o CNPJ, o objeto contratado que comprove ter a licitante fornecido o bem ou serviço, de maneira satisfatória, compatíveis em características com o objeto desta licitação e dados para contato.

10.11.1.1. Os atestados deverão referir-se ao fornecimento de materiais no âmbito de sua atividade econômica principal ou secundária especificadas no contrato social vigente e compatíveis com o objeto desta licitação.

10.12. DISPOSIÇÕES FINAIS PARA HABILITAÇÃO

10.12.1. O licitante enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar n. 123, de 2006, estará dispensado (a) da prova de inscrição nos cadastros de contribuintes estadual e municipal e (b) da apresentação do balanço patrimonial e das demonstrações contábeis do último exercício.

10.12.2. A existência de restrição relativamente à regularidade fiscal e trabalhista não impede que a licitante qualificada como microempresa ou empresa de pequeno porte seja declarada vencedora, uma vez que atenda a todas as demais exigências do edital.

10.12.3. A declaração do vencedor acontecerá no momento imediatamente posterior à fase de habilitação.

10.12.4. Caso a proposta mais vantajosa seja ofertada por licitante qualificada como microempresa ou empresa de pequeno porte, e uma vez constatada a existência de alguma restrição no que tange à regularidade fiscal e trabalhista, a mesma será convocada para, no prazo de 5 (cinco) dias úteis, após a declaração do vencedor, comprovar a regularização. O prazo poderá ser prorrogado por igual período, a critério da administração pública, quando requerida pelo licitante, mediante apresentação de justificativa.

10.12.5. A não regularização fiscal e trabalhista no prazo previsto no subitem anterior acarretará a inabilitação do licitante, sem prejuízo das sanções previstas neste Edital, sendo facultada a convocação dos licitantes remanescentes, na ordem de classificação.

10.12.6. Havendo necessidade de analisar minuciosamente os documentos exigidos, o Pregoeiro suspenderá a sessão, informando no "chat" a nova data e horário para a continuidade da mesma.

10.12.7. Será inabilitado o licitante que não comprovar sua habilitação, seja por não apresentar quaisquer dos documentos exigidos, ou apresentá-los em desacordo com o estabelecido neste Edital.

10.12.8. Constatado o atendimento às exigências de habilitação fixadas no Edital, o licitante será declarado vencedor.

11. DO ENCAMINHAMENTO DA PROPOSTA VENCEDORA

11.1. A proposta final do licitante declarado vencedor deverá ser encaminhada no prazo de 2 (duas) horas, a contar da solicitação do Pregoeiro no sistema eletrônico e deverá:

11.1.1. Ser redigida em língua portuguesa, datilografada ou digitada, em uma via, sem emendas, rasuras, entrelinhas ou ressalvas, devendo a última folha ser assinada e as demais rubricadas pelo licitante ou seu representante legal.

11.1.2. Conter a indicação do banco, número da conta e agência do licitante vencedor, para fins de pagamento.

11.1.3. A proposta final deverá ser documentada nos autos e será levada em consideração no decorrer da execução do objeto e aplicação de eventual sanção ao fornecedor registrado, se for o caso.

11.1.4. Todas as especificações do objeto contidas na proposta vinculam a Contratada.

11.2. Os preços deverão ser expressos em moeda corrente nacional, o valor unitário em algarismos e o valor global em algarismos e por extenso (art. 5º da Lei nº 8.666/93).

11.3. Ocorrendo divergência entre os preços unitários e o preço global, prevalecerão os primeiros; no caso de divergência entre os valores numéricos e os valores expressos por extenso, prevalecerão estes últimos.

11.4. A oferta deverá ser firme e precisa, limitada, rigorosamente, ao objeto deste Edital, sem conter alternativas de preço ou de qualquer outra condição que induza o julgamento a mais de um resultado, sob pena de desclassificação.

11.5. A proposta deverá obedecer aos termos deste Edital e seus Anexos, não sendo considerada aquela que não corresponda às especificações ali contidas ou que estabeleça vínculo à proposta de outro licitante.

12. DOS RECURSOS

12.1. Declarado o vencedor e decorrida a fase de regularização fiscal e trabalhista da licitante qualificada como microempresa ou empresa de pequeno porte, se for o caso, será concedido o prazo de no mínimo trinta minutos, para que qualquer licitante manifeste a intenção de recorrer, de forma motivada, isto é, indicando contra qual(is) decisão(ões) pretende recorrer e por quais motivos, em campo próprio do sistema.

12.2. Havendo quem se manifeste, caberá ao Pregoeiro verificar a tempestividade e a existência de motivação da intenção de recorrer, para decidir se admite ou não o recurso, fundamentadamente.

12.2.1. Nesse momento o Pregoeiro não adentrará no mérito recursal, mas apenas verificará as condições de admissibilidade do recurso.

12.2.2. A falta de manifestação motivada do licitante quanto à intenção de recorrer importará a decadência desse direito.

12.2.3. Uma vez admitido o recurso, o recorrente terá, a partir de então, o prazo de três dias para apresentar as razões, pelo sistema eletrônico, ficando os demais licitantes, desde logo, intimados para, querendo, apresentarem contrarrazões também pelo sistema eletrônico, em outros três dias, que começarão a contar do término do prazo do recorrente, sendo-lhes assegurada vista imediata dos elementos indispensáveis à defesa de seus interesses.

12.3. O acolhimento do recurso invalida tão somente os atos insuscetíveis de aproveitamento.

12.4. Para efeito do disposto no § 5º do artigo 109 da Lei nº 8.666/1993, os autos do processo administrativo eletrônico permanecerão com vista franqueada aos interessados, que deverão solicitá-la pelo e-mail: **cpl@defensoria.to.def.br,** ou diretamente na CPL.

13. DA REABERTURA DA SESSÃO PÚBLICA

13.1. A sessão pública poderá ser reaberta:

13.1.1. Nas hipóteses de provimento de recurso que leve à anulação de atos anteriores à realização da sessão pública precedente ou em que seja anulada a própria sessão pública, situação em que serão repetidos os atos anulados e os que dele dependam.

13.1.2. Quando houver erro na aceitação do preço melhor classificado, habilitação, ou quando o licitante declarado vencedor não assinar o contrato, não retirar o instrumento equivalente ou não comprovar a regularização fiscal e trabalhista, nos termos do art. 43, §1º da LC nº 123/2006. Nessas hipóteses, serão adotados os procedimentos imediatamente posteriores ao encerramento da etapa de lances.

13.2. Todos os licitantes remanescentes deverão ser convocados para acompanhar a sessão reaberta.

13.2.1. A convocação se dará por meio do sistema eletrônico ("chat"), e-mail, ou, ainda, de acordo com a fase do procedimento licitatório.

13.2.2. A convocação feita por e-mail dar-se-á de acordo com os dados contidos no SICAF, sendo responsabilidade do licitante manter seus dados cadastrais atualizados.

14. DA ADJUDICAÇÃO E HOMOLOGAÇÃO

14.1. O objeto da licitação será adjudicado ao licitante declarado vencedor, por ato do Pregoeiro, caso não haja interposição de recurso, ou pela autoridade competente, após a regular decisão dos recursos apresentados.

14.2. Após a fase recursal, constatada a regularidade dos atos praticados, a autoridade competente homologará o procedimento licitatório.

15. DAS CONDIÇÕES DE ASSINATURA DA ATA DE REGISTRO DE PREÇOS, DA VIGÊNCIA E DA ADESÃO À ATA DE REGISTRO DE PREÇOS

15.1. Homologado o resultado da licitação, terá o adjudicatário o prazo de 05 (cinco) dias úteis, contados a partir da data de sua convocação, para assinar a Ata de Registro de Preços, cujo prazo de validade encontra-se nela fixado, sob pena de decair do direito à contratação, sem prejuízo das sanções previstas neste Edital.

15.2. A assinatura da Ata de Registro de Preços se dará na modalidade eletrônica, devendo o representante legal do licitante vencedor providenciar seu cadastro no Sistema Eletrônico de Informações – SEI da DPE-TO, através do banner correspondente no sitio da DPE-TO.

15.3. Na assinatura da ata de registro de preços, será exigida a comprovação das condições de habilitação consignadas no edital, que deverão ser mantidas pelo licitante durante a vigência da ata de registro de preços.

15.4. Na hipótese de o vencedor da licitação não comprovar as condições de habilitação consignadas no edital ou se recusar a assinar a ata de registro de preços, a Administração, sem prejuízo da aplicação das sanções das demais cominações legais cabíveis a esse licitante, poderá convocar outro licitante, respeitada a ordem de classificação, para, após a comprovação dos requisitos para habilitação, analisada a proposta e eventuais documentos complementares e, feita a negociação, assinar a ata de registro de preços.

15.5. Firmada a Ata de Registro de Preços entre o licitante vencedor e a Defensoria Pública do Estado do Tocantins, seus signatários passarão a denominar-se: Fornecedor Registrado e Órgão Gerenciador, respectivamente.

15.6. A Ata poderá ser firmada por representante legal, diretor ou sócio da empresa, devidamente munido, respectivamente, de procuração ou contrato social e cédula de identificação do licitante vencedor.

15.7. Ao firmar a Ata, o Licitante vencedor, quando solicitado pelo Órgão Gerenciador, obriga-se a fornecer os bens a ele adjudicados.

15.8. O prazo de validade da Ata de Registro de Preços será de 12 (doze) meses contados a partir da data da publicação do respectivo extrato no Diário Oficial da Defensoria Pública do Estado do Tocantins.

15.9. Em atendimento ao disposto no § 4º do art. 22 do Decreto nº 7.892/2013, **o quantitativo decorrente das adesões à Ata de Registro de Preços, não excederá, na totalidade, ao dobro do quantitativo de cada item registrado** para o órgão gerenciador e órgãos participantes.

15.10. Após a autorização do órgão gerenciador, o órgão não participante deverá efetivar a aquisição ou contratação solicitada em até noventa dias, observado o prazo de vigência da ata.

15.11. Para fins de autorização, **só serão aceitos pedidos de adesões às atas que não excedam**, por órgão ou entidade solicitante, **a cinquenta por cento** dos quantitativos **dos itens** registrados na Ata de Registro de Preços.

16. DA FORMAÇÃO DO CADASTRO DE RESERVA

16.1. Após o encerramento da etapa competitiva, os licitantes poderão reduzir seus preços ao valor da proposta do licitante melhor classificado.

16.2. A apresentação de novas propostas na forma deste item não prejudicará o resultado do certame em relação ao licitante melhor classificado.

16.3. Havendo um ou mais licitantes que aceitem cotar suas propostas em valor igual ao do licitante vencedor, estes serão classificados segundo a ordem da última proposta individual apresentada durante a fase competitiva.

16.4. Esta ordem de classificação dos licitantes registrados deverá ser respeitada nas contratações e somente será utilizada acaso o melhor colocado no certame não assine a ata ou tenha seu registro cancelado nas hipóteses previstas nos artigos 20 e 21 do Decreto n° 7.892/2013.

17. DO CANCELAMENTO DO REGISTRO DE PREÇOS

17.1. O fornecedor registrado poderá ter o seu registro de preços cancelado mediante processo administrativo específico, assegurado o contraditório e a ampla defesa.

17.2. O cancelamento do seu registro poderá ser:

17.2.1. A pedido do próprio Fornecedor Registrado, quando comprovar estar impossibilitado de cumprir as exigências da Ata, por ocorrência de casos fortuitos ou de força maior;

17.2.2. Por iniciativa do Órgão Gerenciador, quando:

a) O fornecedor registrado não aceitar reduzir o preço registrado, na hipótese deste se tornar superior àqueles praticados no mercado:

b) O fornecedor registrado perder qualquer condição de habilitação ou qualificação técnica exigida no processo licitatório;

c) Por razões de interesse público, devidamente motivadas e justificadas;

d) O fornecedor registrado não cumprir as obrigações decorrentes da Ata de Registro de Preços;

e) O fornecedor registrado não comparecer ou se recusar a retirar, no prazo estabelecido, as solicitações decorrentes da Ata de Registro de Preços;

f) Caracterizada qualquer hipótese de inexecução total ou parcial das condições estabelecidas na Ata de Registro de Preços ou nas solicitações dela decorrentes.

17.3. Em qualquer das hipóteses acima, concluído o processo, o Órgão Gerenciador fará o devido

apostilamento na Ata de Registro de Preços e informará aos proponentes a nova ordem de registro.

18. DO RECEBIMENTO DO OBJETO E DA FISCALIZAÇÃO

18.1. Os critérios de recebimento e aceitação do objeto e de fiscalização estão previstos no Termo de Referência, ANEXO I a este Edital.

19. DAS OBRIGAÇÕES DO ÓRGÃO GERENCIADOR E DO FORNECEDOR REGISTRADO

19.1. As obrigações do Órgão Gerenciador e do Fornecedor Registrado são as estabelecidas no Termo de Referência, ANEXO I a este Edital.

20. DO TERMO DE CONTRATO OU INSTRUMENTO EQUIVALENTE

20.1. Após a homologação da licitação e assinada a respectiva Ata de Registro de Preços, em sendo realizada a contratação, será firmado Termo de Contrato.

20.2. O Fornecedor Registrado terá o prazo de 05 (cinco) dias úteis, contados a partir da data de sua convocação, para assinar o Termo de Contrato, sob pena de decair do direito à contratação, sem prejuízo das sanções previstas neste Edital.

20.3. Na assinatura do contrato, será exigida a comprovação das condições de habilitação consignadas no edital, que deverão ser mantidas pelo licitante durante a vigência do contrato.

20.4. Na hipótese de o vencedor da licitação não comprovar as condições de habilitação consignadas no edital ou se recusar a assinar o contrato, a Administração, sem prejuízo da aplicação das sanções das demais cominações legais cabíveis a esse licitante, poderá convocar outro licitante, respeitada a ordem de classificação, para, após a comprovação dos requisitos para habilitação, analisada a proposta e eventuais documentos complementares e, feita a negociação, assinar o contrato.

21. DO PAGAMENTO

21.1. As regras acerca do pagamento são as estabelecidas no Termo de Referência, ANEXO I a este Edital.

22. DAS SANÇÕES ADMINISTRATIVAS

22.1. A licitante ficará impedida de licitar e contratar com a União, Estados, Distrito Federal ou Município pelo prazo de até 05 (cinco) anos, sem prejuízo da multa de 20% do valor estimado/contratado e das demais cominações legais, garantidos o contraditório e a ampla defesa, que deverá ser apresentada no prazo de 05 (cinco) dias úteis a contar da sua notificação, nos seguintes casos:

a) Não apresentar documentação exigida para o certame;

b) Apresentar documentação falsa;

c) Não assinar a ata de registro de Preços ou o Contrato dentro do prazo de validade da sua proposta;

d) Ensejar o retardamento da execução de seu objeto;

e) Não manter as condições ofertadas na proposta;

f) Falhar ou fraudar na execução do ajustado;

g) Comportar-se de modo inidôneo, nos termos da Lei;

h) Cometer fraude fiscal.

22.2. Pela inexecução total ou parcial das condições estabelecidas no instrumento convocatório, a Defensoria Pública do Estado do Tocantins poderá aplicar, sem prejuízo das responsabilidades penal e cível, as seguintes sanções:

a) Advertência, por escrito, quando o FORNECEDOR REGISTRADO/CONTRATADA deixar de atender quaisquer indicações aqui constantes;

b) Multa compensatória / indenizatória no percentual de até 20% (vinte por cento) calculado sobre o valor contratado;

c) Suspensão temporária de participação de licitação e impedimento de contratar com a Defensoria Pública do Estado do Tocantins, pelo prazo de até 02 (dois) anos;

d) Declaração de inidoneidade para licitar e contratar com Administração Pública enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação, na forma da Lei, perante a própria autoridade que aplicou a penalidade.

22.3. Na hipótese de atraso no cumprimento de quaisquer obrigações assumidas pelo FORNECEDOR REGISTRADO/CONTRATADA será aplicada multa moratória de 0,5% (zero vírgula cinco por cento) sobre o valor do contrato ou instrumento equivalente, por dia de atraso, limitada a 10 % (dez por cento) do valor inadimplido;

22.4. O valor da multa aplicada, tanto compensatória quanto moratória, deverá ser recolhida em conta da Defensoria Pública do Estado do Tocantins a ser indicada, dentro do prazo de 05 (cinco) dias úteis após a respectiva notificação;

22.5. Caso não seja paga na forma do subitem anterior, a multa será descontada por ocasião do pagamento posterior a ser efetuado ao FORNECEDOR REGISTRADO/CONTRATADA ou cobrada judicialmente;

22.6. Além das penalidades citadas, o FORNECEDOR REGISTRADO/CONTRATADA ficará sujeito, ainda, no que couber, às demais penalidades referidas no Capítulo IV da Lei n° 8.666/93;

22.7. Na aplicação de quaisquer sanções previstas, será garantido o contraditório e a ampla defesa.

23. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

23.1. Até 03 (três) dias úteis antes da data designada para a abertura da sessão pública, qualquer pessoa poderá impugnar este Edital.

23.2. A impugnação poderá ser realizada por forma eletrônica, pelo e-mail cpl@defensoria.to.def.br ou por petição dirigida ou protocolada no endereço Quadra 502 Sul, Avenida Teotônio Segurado, Palmas – TO, CEP: 77021-654, seção de protocolo da Defensoria Pública do Estado do Tocantins.

23.3. Caberá o Pregoeiro, auxiliado pelos responsáveis pela elaboração deste Edital e seus anexos, decidir sobre a impugnação no prazo de até dois dias úteis contados da data de recebimento da impugnação.

23.4. Acolhida a impugnação, será definida e publicada nova data para a realização do certame.

23.5. Os pedidos de esclarecimentos referentes a este processo licitatório deverão ser enviados o Pregoeiro, até 03 (três) dias úteis anteriores à data designada para abertura da sessão pública, exclusivamente por meio eletrônico via internet, no endereço indicado no Edital.

23.6. O Pregoeiro responderá aos pedidos de esclarecimentos no prazo de dois dias úteis, contado da data de recebimento do pedido, e poderá requisitar subsídios formais aos responsáveis pela elaboração do edital e dos anexos.

23.7. As impugnações e pedidos de esclarecimentos não suspendem os prazos previstos no certame.

23.7.1. Concessão de efeito suspensivo à impugnação é medida excepcional e deverá ser motivada pelo Pregoeiro, nos autos do processo de licitação.

23.8. As respostas aos pedidos de esclarecimentos serão divulgadas pelo sistema, bem como publicadas na página da DPE-TO e vincularão os participantes e a administração.

24. DAS DISPOSIÇÕES GERAIS

24.1. Da sessão pública do Pregão divulgar-se-á Ata no sistema eletrônico.

24.2. Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a realização do certame na data marcada, a sessão será automaticamente transferida para o primeiro dia útil subsequente, no mesmo horário anteriormente estabelecido, desde que não haja comunicação em contrário, pelo Pregoeiro.

24.3. Todas as referências de tempo no Edital, no aviso e durante a sessão pública observarão o horário de Brasília – DF.

24.4. No julgamento das propostas e da habilitação, o Pregoeiro poderá sanar erros ou falhas que não alterem a substância das propostas, dos documentos e sua validade jurídica, mediante despacho fundamentado, registrado em ata e acessível a todos, atribuindo-lhes validade e eficácia para fins de habilitação e classificação.

24.5. A homologação do resultado desta licitação não implicará direito à contratação.

24.6. As normas disciplinadoras da licitação serão sempre interpretadas em favor da ampliação da disputa entre os interessados, desde que não comprometam o interesse da Administração, o princípio da isonomia, a finalidade e a segurança da contratação.

24.7. Os licitantes assumem todos os custos de preparação e apresentação de suas propostas e a Administração não será, em nenhum caso, responsável por esses custos, independentemente da condução ou do resultado do processo licitatório.

24.8. Na contagem dos prazos estabelecidos neste Edital e seus Anexos, excluir-se-á o dia do início e incluir-se-á o do vencimento. Só se iniciam e vencem os prazos em dias de expediente na Administração.

24.8.1. Para os fins do disposto no subitem anterior, em dias em que eventualmente venha a ser estabelecido como ponto facultativo considerar-se-á como dia não útil.

24.9. O desatendimento de exigências formais não essenciais não importará o afastamento do licitante, desde que seja possível o aproveitamento do ato, observados os princípios da isonomia e do interesse público.

24.10. Em caso de divergência entre disposições deste Edital e de seus anexos ou demais peças que compõem o processo, prevalecerá as deste Edital.

24.11. Fica assegurado à DPE-TO, mediante justificativa, o direito de, a qualquer tempo, e no interesse da Administração, revogar a presente licitação no todo ou em parte.

24.12. Qualquer modificação no Edital exige divulgação pela mesma forma que se deu o texto original, reabrindo-se o prazo inicialmente estabelecido, **exceto quando, inquestionavelmente, a alteração não afetar a formulação da proposta**.

24.13. As certidões que não possuírem prazo de validade, somente serão aceitas com data de emissão não superior a 60 (sessenta) dias.

24.14. É responsabilidade da licitante o acompanhamento das publicações oficiais referentes ao presente procedimento licitatório, inclusive o acompanhamento da situação do certame no site da Defensoria Pública do Estado do Tocantins independentemente dos dados constantes do sistema Comprasnet.

24.15. Em caso de indisponibilidade do sistema Comprasnet para o licitante é dever deste comunicar imediatamente o Pregoeiro via telefone no nº (063) 3218-3775, sob pena de assumir o ônus disposto no subitem 6.5 deste Edital.

24.16. São válidas todas as comunicações ou notificações encaminhadas aos licitantes via correio eletrônico nos endereços por eles indicados em suas propostas ou constantes do SICAF, contando-se os prazos a partir da data do envio.

24.17. O Edital está disponibilizado, na íntegra, no endereço eletrônico https://www.defensoria.to.def.br/ e https://www.compras.gov.br/ (UASG: 926040), permanecendo os autos do processo administrativo com vista franqueada aos interessados que a solicitarem.

24.18. Os casos omissos serão resolvidos pelo Pregoeiro em conformidade com a legislação

preambularmente indicada.

24.19. Para dirimir as questões relativas ao presente Edital, elege-se como foro competente o de Palmas-TO, com exclusão de qualquer outro.

Palmas, 21 de outubro de 2022.

Pedro Alexandre Conceição A. Gonçalves

Subdefensor Público-Geral

Dulcirene Pereira Oliveira

Pregoeira

Documento assinado eletronicamente por **Pedro Alexandre Conceição A Gonçalves**, **Subdefensor Público-Geral**, em 21/10/2022, às 09:31, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **DULCIRENE PEREIRA OLIVEIRA**, **Pregoeiro (a)**, em 21/10/2022, às 11:27, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site http://sei.defensoria.to.def.br/sei/verifica.php informando o código verificador **0698999** e o código CRC **35E64519**.

ANEXO I -TERMO DE REFERÊNCIA

1. DO OBJETO

O presente Termo de Referência tem como finalidade promover o REGISTRO DE PREÇOS para eventual contratação de empresa fornecedora de *switches* gerenciáveis, cordões ópticos, *access points*, *sofware* de gerencia, serviços de instalação e treinamento especializados, para atender as necessidades da Defensoria Pública do Estado do Tocantins.

2. DA JUSTIFICATIVA

As atividades desenvolvidas por esta Instituição consistem na assistência jurídica aos que necessitam da tutela jurisdicional. Dessa forma, para que a Defensoria Pública do Estado do Tocantins ofereça um serviço de qualidade é necessário propiciar aos servidores e Defensores Públicos condições e estrutura física. Para tanto, alguns itens se faz necessário para atender a execução das atividades das áreas meio e fim pensando no aprimoramento, ampliação e agilidade do Atendimento ao Assistido.

Atualmente a estrutura de rede da Defensoria Pública do Estado do Tocantins, tanto em sua Sede como nas Diretorias Regionais e Comarcas, vem demandando melhorias, tendo em vista: a implantação da Telefonia VOIP, que é tendência para as próximas licitações de telefonia e para alguns ramais já em operação; e a necessidade de maior conectividade, demandados pela crescente utilização dos serviços institucionais e ampliação dos mesmos ao atendimento aos públicos remotos. Para que se consigam suprir

essas necessidades crescentes, se faz necessária a aquisição de ativos a serem utilizados em todo o estado.

Switches são equipamentos de rede de dados essenciais em qualquer sistema de cabeamento estruturado – como os implantados nas unidades da Defensoria Pública do Estado do Tocantins –, sendo responsáveis por interligar computadores e outros equipamentos de rede, realizando a comunicação de dados de maneira inteligente, criando um canal exclusivo entre a origem e o destino, aumentando o desempenho e diminuindo a ocorrência de erros. Com a implantação do Data Center na Sede, dos circuitos MPLS e futura expansão de telefonia VOIP nas unidades desta instituição no estado, é imprescindível a aquisição de Switches que permitam o maior fluxo de dados trocados entre a intranet, rede do Data Center e Internet, bem como, de gerenciamento remoto e centralizado, o que hoje não é possível executar com os equipamentos atualmente instalados nesses locais.

Access Points são equipamentos destinados na disponibilização de rede de dados sem fio aos dispositivos por meio de ondas de rádio – como os implantados nas unidades da Defensoria Pública do Estado do Tocantins –, sendo responsáveis por interligar notebooks e outros dispositivos, realizando a comunicação de dados por meio de rede sem fio. Com a adoção de aplicativos de mensagens instantâneas e de redes sociais, algumas integradas aos sistemas institucionais de atendimento, utilizados de forma crescente na comunicação institucional com assistidos, acréscimos de equipamentos na rede onde os pontos lógicos de dados são limitados, remoção dos roteadores Wi-Fi em comodato com a prestadora de serviços das Comarcas onde o serviço ADSL foi desativado e, execuções de projetos e atividades institucionais externas, é imprescindível a aquisição de Access Points para uma solução de rede Wi-Fi corporativa que permita o maior fluxo de dados e dispositivos conectados simultaneamente, equipamentos homogêneos de forma a garantir a interoperabilidade plena entre si e aumento da área de cobertura, de gerenciamento remoto e centralizado, :executar com os equipamentos atualmente instalados nesses locais, os quais na atualidade são considerados de uso comum.

Vale ressaltar que equipamentos defasados e fora de garantia e suporte técnico podem ocasionar falhas inesperadas causando indisponibilidade ou interrupção dos serviços da Defensoria Pública do Estado do Tocantins e que pode acarretar prejuízos aos trabalhos desenvolvidos, de acordo com a criticidade de cada um. Serviços como SOLAR, SEI, ATHENAS (Diárias, Patrimônio, Recursos Humanos) e correio eletrônico, por exemplo, tornaram-se de tal modo críticos que a sua breve interrupção causa inúmeros transtornos e atrasos nos serviços normais desta instituição.

Os equipamentos de rede, switches e Access Points/Roteadores, atualmente instalados nas unidades desta instituição não possuem padronização de fabricantes e, em alguns casos, não há interoperabilidade entre esses equipamentos o que dificulta a gestão e em muitos casos inviabiliza a conexão e utilização de funcionalidades e dispositivos entre eles devido à incompatibilidade existente.

Desta forma, os itens foram agrupados conforme suas características a fim de garantir total integração da infraestrutura de rede, conectividade e interoperabilidade plena entre si e, desses equipamentos com o software de gerenciamento, o qual só é possível de utilização com equipamentos de mesmo fabricante. Ademais, a divisão em grupos não restringe a participação ou competitividade, pois há no mercado de ativos de rede diversos fabricantes e empresas fornecedoras de soluções objeto desse instrumento, pode-se citar a Alcatel, Aruba, Cisco, Dell, Extreme Networks, Rukus, Juniper, entre outros potenciais fornecedores.

A opção pelo registro de preços no processo licitatório em epígrafe visa planejar a aquisição dos objetos de forma parcelada, quando houver necessidade, por se tratar de contratação de considerável extensão, que não se pode precisar com exatidão o quantitativo a ser utilizado de imediato, conforme demanda e disponibilidade orçamentária.

Logo, visando manter e expandir os serviços de rede e telefonia da Defensoria Pública do Estado do Tocantins, de modo que esta possa continuar prestando serviços públicos de qualidade à população em todo o Estado do Tocantins, planeja-se contratação de pessoa jurídica para eventual fornecimento dos equipamentos supracitados.

3. ESPECIFICAÇÕES, DAS QUANTIDADES E DOS VALORES ESTIMADOS

GRUPO	ITEM	CATMAT/ CATSER	QTD	UND	DESCRIÇÃO	Valor Unit. (R$)
1	1	393274	100	UND	Switch de Acesso Tipo I	R$ 10.587,84
	2	393274	60	UND	Switch de Acesso Tipo II	R$ 17.903,19
	3	393274	30	UND	Switch de Acesso Tipo III	R$ 21.506,79
	4	394004	20	UND	Switch de Acesso Tipo IV	R$ 23.443,78
	5	393274	20	UND	Switch de Acesso Tipo V	R$ 42.719,94
	6	485140	2	UND	Switch de Distribuição	R$ 98.981,50
	7	295671	80	UND	Transceiver 1000BASE-X	R$ 715,32
	8	462024	60	UND	Transceiver 10GBASE-X	R$ 1.608,23
	9	27464	232	UND	Licenças Software de Gerência LAN	R$ 1.645,31
	10	26972	232	SERV	Serviço de instalação especializada LAN	R$ 993,00
	11	20052	1	SERV	Serviço de treinamento especializado LAN	R$ 29.383,33
	TOTAL GRUPO 1					**R$ 5.094**

GRUPO	ITEM	CATMAT/ CATSER	QTD	UND	DESCRIÇÃO	Valor Unit. (R$)
2	12	393277	80	UND	Access Point Indoor	R$ 6.237,08
	13	393277	6	UND	Access Point Outdoor	R$ 12.263,39
	14	27464	86	UND	Licenças Software de Gerência WLAN	R$ 1.054,02
	15	26972	86	SERV	Serviço de instalação especializada WLAN	R$ 975,00
	16	20052	1	SERV	Serviço de treinamento especializado WLAN	R$ 21.388,80
	TOTAL GRUPO 2					**R$ 76**

ITEM	CATMAT/ CATSER	QTD	UND	DESCRIÇÃO	Valor Unit. (R$)	Valor Total (R$)

17	432081	100	UND	Cordão Óptico 2 metros	R$ 87,65	R$ 8.765,00

ITEM	CATMAT/ CATSER	QTD	UND	DESCRIÇÃO	Valor Unit. (R$)	Valor Total (R$)
18	420396	20	UND	Cordão Óptico 20 metros	R$ 511,47	R$ 10.229,40

3.1. Switch de Acesso Tipo I

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

3.1.2. A solução deve ser composta de um único equipamento, montável em rack 19" devendo este vir acompanhado dos devidos acessórios para tal e possuir altura máxima de 1RU;

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

3.1.4. Possuir LEDS indicativos de funcionamento da fonte de alimentação e status das portas;

3.1.5. Deve possuir homologação ANATEL, de acordo com a resolução vigente;

3.1.6. Deve possuir pelo menos 24 portas 10/100/1000BASE-T;

3.1.7. Deve possuir pelo menos 04 portas 1000/2500BASE-X baseadas em SFP;

3.1.8. Deve possuir uma porta USB para transferência de arquivos;

3.1.9. Possuir uma porta console com conector RJ-45 ou DB9 macho;

3.1.10. Possuir uma porta 10/100/1000Base-T do tipo out-of-band para gerência do equipamento;

3.1.11. Todas as interfaces ofertadas devem ser non-blocking;

3.1.12. Deve possuir detecção automática MDI/MDIX em todas as portas 10/100/1000BASE-T;

3.1.13. Deve possuir capacidade de processamento de pelo menos 68Gbps;

3.1.14. Deve possuir capacidade de encaminhamento de pelo menos 50Mpps;

3.1.15. A memória Flash instalada deve ser suficiente para comportar no mínimo duas imagens do SO simultaneamente, permitindo que seja feito um upgrade de Software e a imagem anterior seja mantida;

3.1.16. Implementar agregação de links conforme padrão IEEE 802.3ad com, no mínimo, 8 grupos, sendo 8 links agregados por grupo;

3.1.17. Implementar agregação de links conforme padrão IEEE 802.3ad com suporte a LACP;

3.1.18. Implementar jumbo frames em todas as portas ofertadas, com suporte a pacotes de até 9216 Bytes;

3.1.19. Implementar Proxy-ARP (RFC 1027);

3.1.20. Implementar IGMP v1, v2 e v3 Snooping;

3.1.21. Implementar IGMPv1 (RFC 1112), IGMP v2 (RFC 2236) e IGMPv3 (RFC 3376);

3.1.22. Implementar MVR (Multicast VLAN Registration);

3.1.23. Implementar DHCP/Bootp relay configurável por VLAN para IPv4 e IPv6;

3.1.24. Implementar servidor DHCP interno que permita a configuração de um intervalo de endereços IP a serem atribuídos os clientes DHCP e possibilite ainda a atribuição de, no mínimo, default-gateway, servidor DNS e servidor WINS;

3.1.25. Implementar DHCP Option 82, de acordo com a RFC 3046, com identificação de porta e VLAN, configurável por VLAN;

3.1.26. Implementar DHCP Client para IPv4 e IPv6;

3.1.27. Implementar Spanning-Tree (IEEE 802.1d), Rapid Spanning Tree (IEEE 802.1w), Multiple Instance STP (802.1s) e PVST+;

3.1.28. Implementar a configuração de Multiple Spanning Tree Protocol, com suporte a, pelo menos, 16 domínios;

3.1.29. Implementar funcionalidade vinculada ao Spanning-tree onde é possível designar portas de acesso (por exemplo onde estações estão conectadas) que não sofram o processo de Listening-Learning, passando direto para o estado de Forwarding. No entanto, as portas configuradas com esta funcionalidade devem detectar loops na rede normalment;

3.1.30. Implementar funcionalidade vinculada ao Spanning-tree que evite a eleição de outros switches da rede como Root;

3.1.31. Implementar funcionalidade vinculada ao Spanning-tree que permita desabilitar uma porta de acesso assim que a mesma receba uma BPDU;

3.1.32. Implementar 4000 VLANs por porta, ativas simultaneamente, através do protocolo 802.1Q;

3.1.33. Deverá permitir a criação, remoção, gerenciamento e distribuição de VLANs de forma dinâmica através de portas configuradas como tronco IEEE 802.1Q utilizando o protocolo MVRP segundo o padrão IEEE802.1ak;

3.1.34. Possibilitar a coleta de estatísticas de tráfego baseada em VLANs IEEE 802.1Q e double-tagged VLANs IEEE 802.1ad;

3.1.35. Implementar MAC Based VLAN;

3.1.36. Implementar VLAN Translation;

3.1.37. Implementar VLAN Aggregation ou funcionalidade que permita o compartilhamento de uma mesma subnet e de um mesmo endereço IPv4 utilizado como default-gateway por hosts de diferentes VLANs;

3.1.38. Implementar Private VLANs;

3.1.39. Implementar Port Isolation ou funcionalidade que permita isolamento de portas específicas do switch. As portas isoladas não devem se comunicar entre si, porém podem se comunicar com qualquer outra porta no equipamento que não esteja isolada;

3.1.40. Implementar IEEE 802.1ad com a possibilidade de associar CVIDs específicos para diferentes SVIDs (selective Q-in-Q ou 802.1ad CEP). A implementação deverá permitir a tradução do CVID;

3.1.41. Implementar IEEE 802.1ag (Connectivity Fault Management);

3.1.42. Implementar funcionalidade baseada na recomendação do ITU-T Y.1731 com medição de, no mínimo, Frame Delay;

3.1.43. Implementar o protocolo ITU-T G.8032 ERPS;

3.1.44. Implementar protocolo de resiliência em camada 2, específico para topologias em anel, que permita tempo de convergência inferior a 200 ms;

3.1.45. Implementar IEEE 802.1ab Link Layer Discovery Protocol (LLDP);

3.1.46. Implementar LLDP-MED (Media Endpoint Discovery);

3.1.47. Implementar roteamento estático com suporte a, no mínimo, 32 rotas;

3.1.48. Implementar, no mínimo, 30 interfaces IP (IPv4 ou IPv6);

3.1.49. Implementar PIM Snooping;

3.1.50. Deve implementar Dual Stack, ou seja, IPv6 e IPv4, com suporte as seguintes

funcionalidades/RFCs:

3.1.50.1. RFC 1981, Path MTU Discovery for IPv6, August 1996 - Host Requirements;

3.1.50.2. RFC 5095, Internet Protocol, Version 6 (IPv6) Specification;

3.1.50.3. RFC 4861, Neighbor Discovery for IP Version 6, (IPv6);

3.1.50.4. RFC 2462, IPv6 Stateless Address Auto configuration - Host Requirements;

3.1.50.5. RFC 2463, Internet Control Message Protocol (ICMPv6) for the IPv6 Specification;

3.1.50.6. RFC 2464, Transmission of IPv6 Packets over Ethernet Networks;

3.1.50.7. RFC 2465, IPv6 MIB, General Group and Textual Conventions;

3.1.50.8. RFC 2466, MIB for ICMPv6;

3.1.50.9. RFC 3513, Internet Protocol Version 6 (IPv6) Addressing Architecture;

3.1.50.10. RFC 3587, Global Unicast Address Format;

3.1.51. Implementar os seguintes protocolos em IPv6: Ping, Traceroute, Telnet, SSHv2, SNMP, Syslog, SNTP e DNS;

3.1.52. Deve implementar IPv6 de acordo com as seguintes RFCs:

3.1.52.1. RFC 1981, Path MTU Discovery for IPv6, August 1996 - Router Requirements;

3.1.52.2. RFC 2462, IPv6 Stateless Address Auto configuration - Router Requirements;

3.1.52.3. RFC 2462, IPv6 Stateless Address Auto configuration - Router Requirements;

3.1.52.4. RFC 2710, IPv6 Multicast Listener Discovery v1 (MLDv1) Protocol;

3.1.52.5. RFC 3810, IPv6 Multicast Listener Discovery v2 (MLDv2) Protocol;

3.1.52.6. RFC 6106, IPv6 Router Advertisement Options for DNS Configuration;

3.1.53. Implementar Policy Based Routing;

3.1.54. Implementar upload e download de configuração em formato ASCII ou XML, permitindo a edição do arquivo de configuração e, posteriormente, o download do arquivo editado para o equipamento;

3.1.55. Implementar TACACS+ segundo a RFC 1492;

3.1.56. Implementar autenticação RADIUS com suporte a:

3.1.56.1. RFC 2865 RADIUS Authentication;

3.1.56.2. RFC 2866 RADIUS Accounting;

3.1.56.3. RFC 3579 RADIUS EAP support for 802.1X;

3.1.57. A implementação de RADIUS deve suportar alteração dinâmica de parâmetros de autorização de uma sessão que já esteja ativa;

3.1.58. A implementação de RADIUS e TACACS+ deve estar disponível para autenticação de usuários via Telnet e Console serial;

3.1.59. Implementar per-command authorization para RADIUS e TACACS+;

3.1.60. Possuir DNS Client para IPv4 segundo a RFC 1591 e DNS Client para IPv6;

3.1.61. Possuir Telnet client and server segundo a RFC 854;

3.1.62. Implementar os seguintes grupos de RMON através da RFC 1757: History, Statistics, Alarms e Events;

3.1.63. Deve implementar RMON2-probe configuration segundo a RFC 2021, podendo ser implementada internamente no switch ou externamente, por meio de probe em hardware utilizando uma porta 1000BaseTX;

3.1.64. Implementar sFlow ou Netflow, em hardware;

3.1.65. Implementar a atualização de imagens de software e configuração através de um servidor TFTP;

3.1.66. Suportar múltiplos servidores Syslog;

3.1.67. Implementar Port Mirroring, permitindo espelhar portas físicas ou VLANs para portas de destino (portas de análise);

3.1.68. Implementar RSPAN (Remote Mirroring), permitindo espelhar o tráfego de uma porta ou VLAN de um switch remoto para uma porta de um switch local (porta de análise);

3.1.69. Implementar gerenciamento através de SNMPv1 (RFC 1157), v2c (RFCs 1901 a 1908), v3 (RFCs 3410 a 3415) e SNMP para IPv6;

3.1.70. Implementar SMON de acordo com a RFC 2613;

3.1.71. Implementar cliente e servidor SSHv2;

3.1.72. Implementar cliente e servidor SCP e servidor SFTP;

3.1.73. Implementar gerenciamento via web com suporte a HTTP e HTTPS/SSL, permitindo visualização gráfica da utilização (em percentual, bytes e pacotes) das portas;

3.1.74. A interface gráfica deve permitir visualização de informações do sistema (VLAN, Portas, Fonte e Fans), monitoramento de Log, utilização de portas, QoS e configuração de portas, VLANs e ACLs;

3.1.75. O equipamento ofertado deve possuir um sistema operacional modular;

3.1.76. O sistema operacional deve possuir função grep/pipe para filtrar a saída de determinado comando;

3.1.77. O sistema operacional deve possuir comandos para visualização e monitoração de cada processo, sendo possível verificar por processo qual o consumo de cpu, process-id e qual o consumo de memória por processo;

3.1.78. O sistema operacional deve possuir comandos para que processos sejam terminados ou reiniciados sem que seja necessário a reinicialização do equipamento. Esta funcionalidade deve estar disponível pelo menos para Telnet, TFTP, HTTP e LLDP na versão atual;

3.1.79. Implementar linguagem de scripting baseada em Python, permitindo a automatização de tarefas. A linguagem deve implementar estruturas de controle como loops e execução condicional e permitir a definição de variáveis;

3.1.80. Implementar protocolo de monitoramento de status de comunicação entre dois switches, que possibilite que uma porta seja desabilitada caso seja detectada uma falha de comunicação entre os dois peers;

3.1.81. Implementar funcionalidade que permita sua auto-configuração através dos protocolos DHCP e TFTP, permitindo o provisionamento em massa com o mínimo de intervenção humana;

3.1.82. Deve disponibilizar API (Aplication Programming Interface) aberta para integração com aplicações;

3.1.83. Implementar Rate limiting de entrada em todas as portas. A granularidade deve ser configurável em intervalos de 64Kbps para portas de até 1Gbps. Caso o equipamento ofertado possua suporte a portas 10Gbps, a granularidade para este tipo de interface deve ser configurável em intervalos de 1Mbps. A implementação de Rate Limiting deve permitir a classificação do tráfego utilizando-se ACLs e parâmetros, MAC origem e destino (simultaneamente) IP origem e destino (simultaneamente), portas TCP, portas UDP e campo 802.1p;

3.1.84. Implementar Rate Shaping de saída em todas as portas. A granularidade deve ser configurável em intervalos de 64Kbps para portas de até 1Gbps. Caso o equipamento ofertado possua suporte a portas 10Gbps, a granularidade para este tipo de interface deve ser configurável em intervalos de 1Mbps;

3.1.85. A funcionalidade de Rate Shaping deve permitir a configuração de CIR (Commited Rate), banda máxima, banda mínima e peak rate;

3.1.86. Implementar a leitura, classificação e remarcação de QoS (802.1p e DSCP);

3.1.87. Implementar remarcação de prioridade de pacotes Layer 3, remarcando o campo DiffServ para grupos de tráfego classificados segundo portas TCP e UDP, endereço/subrede IP, VLAN e MAC origem e destino;

3.1.88. Implementar 8 filas de prioridade em hardware por porta;

3.1.89. Implementar os algoritmos de gerenciamento de filas WRR (Weighted Round Robin), WDRR (Weighted Deficit Round Robin) e SP (Strict Priority);

3.1.90. Deve implementar, ao menos dois dos algoritimos acima, simultaneamente em uma mesma porta;

3.1.91. Implementar as seguintes RFCs:

3.1.91.1. RFC 2474 DiffServ Precedence;

3.1.91.2. RFC 2598 DiffServ Expedited Forwarding (EF);

3.1.91.3. RFC 2597 DiffServ Assured Forwarding (AF);

3.1.91.4. RFC 2475 DiffServ Core and Edge Router Functions;

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

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

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

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

3.1.96. Implementar Gratuitous ARP Protection;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3.1.111. Implementar Policy Based Switching, ou seja, possibilitar que o tráfego classificado por uma ACL seja redirecionado para uma porta física específica;

3.1.112. Implementar funcionalidade que permita o mapeamento de usuários identificados via Kerberos (com a credencial de usuário no domínio), IEEE 802.1x e LLDP, provendo informações como endereço MAC, VLAN e porta física. Estas informações devem estar disponíveis na linha de comando (CLI) do equipamento;

3.1.113. O equipamento ofertado deve permitir que ele faça parte de uma malha ethernet (Fabric Ethernet) descrito nos switches distribuição com as seguintes funcionalidades:

3.1.114. O equipamento ofertado deve permitir a configuração como elemento anexo à malha ethernet;

3.1.115. O equipamento ofertado deve permitir a criação de VLANS mapeadas a serviços virtuais de rede, de que forma os serviços sejam criados automaticamente no elemento de borda da malha e propagados de maneira automática nos demais equipamentos que compõem a malha ethernet;

3.1.116. Deve permitir o gerenciamento do equipamento através de software de gerência do Fabric;

3.1.117. Deve possuir garantia do fabricante ou da revenda, desde que essa seja autorizada por carta pelo fabricante dos equipamentos a prestar o suporte e garantia, pelo período de 60 meses;

3.1.118. Marca/Modelo/Séries de Referencia: Extreme Networks X435, Alcatel Lucent 6360, Ruckus 7150, Juniper EX2300, Cisco 9200 e Aruba 2930F.

3.2. Switch de Acesso Tipo II

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

3.2.2. A solução deve ser composta de um único equipamento, montável em rack 19” devendo este vir acompanhado dos devidos acessórios para tal e possuir altura máxima de 1RU;

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

3.2.4. Implementar Power over Ethernet Plus (PoE+) segundo o padrão IEEE 802.3at em todas as portas 1000Base-T, com no mínimo 370W de potência disponível para dispositivos PoE através de fonte interna;

3.2.5. Possuir LEDS indicativos de funcionamento da fonte de alimentação e status das portas;

3.2.6. Deve possuir homologação ANATEL, de acordo com a resolução vigente;

3.2.7. Deve possuir pelo menos 24 portas 10/100/1000BASE-T;

3.2.8. Deve possuir pelo menos 04 portas 1000/2500BASE-X baseadas em SFP;

3.2.9. Deve possuir uma porta USB para transferência de arquivos;

3.2.10. Possuir uma porta console com conector RJ-45 ou DB9 macho;

3.2.11. Possuir uma porta 10/100/1000Base-T do tipo out-of-band para gerência do equipamento;

3.2.12. Todas as interfaces ofertadas devem ser non-blocking;

3.2.13. Deve possuir detecção automática MDI/MDIX em todas as portas 10/100/1000BASE-T;

3.2.14. Deve possuir capacidade de processamento de pelo menos 68Gbps;

3.2.15. Deve possuir capacidade de encaminhamento de pelo menos 50Mpps;

3.2.16. A memória Flash instalada deve ser suficiente para comportar no mínimo duas imagens do SO simultaneamente, permitindo que seja feito um upgrade de Software e a imagem anterior seja mantida;

3.2.17. Implementar agregação de links conforme padrão IEEE 802.3ad com, no mínimo, 8 grupos, sendo 8 links agregados por grupo;

3.2.18. Implementar agregação de links conforme padrão IEEE 802.3ad com suporte a LACP;

3.2.19. Implementar jumbo frames em todas as portas ofertadas, com suporte a pacotes de até 9216 Bytes;

3.2.20. Implementar Proxy-ARP (RFC 1027);

3.2.21. Implementar IGMP v1, v2 e v3 Snooping;

3.2.22. Implementar IGMPv1 (RFC 1112), IGMP v2 (RFC 2236) e IGMPv3 (RFC 3376);

3.2.23. Implementar MVR (Multicast VLAN Registration);

3.2.24. Implementar DHCP/Bootp relay configurável por VLAN para IPv4 e IPv6;

3.2.25. Implementar servidor DHCP interno que permita a configuração de um intervalo de endereços IP a serem atribuídos os clientes DHCP e possibilite ainda a atribuição de, no mínimo, default-gateway, servidor DNS e servidor WINS;

3.2.26. Implementar DHCP Option 82, de acordo com a RFC 3046, com identificação de porta e VLAN, configurável por VLAN;

3.2.27. Implementar DHCP Client para IPv4 e IPv6;

3.2.28. Implementar Spanning-Tree (IEEE 802.1d), Rapid Spanning Tree (IEEE 802.1w), Multiple Instance STP (802.1s) e PVST+;

3.2.29. Implementar a configuração de Multiple Spanning Tree Protocol, com suporte a, pelo menos, 16 domínios;

3.2.30. Implementar funcionalidade vinculada ao Spanning-tree onde é possível designar portas de acesso (por exemplo onde estações estão conectadas) que não sofram o processo de Listening-Learning, passando direto para o estado de Forwarding. No entanto, as portas configuradas com esta funcionalidade devem detectar loops na rede normalment;

3.2.31. Implementar funcionalidade vinculada ao Spanning-tree que evite a eleição de outros switches da rede como Root;

3.2.32. Implementar funcionalidade vinculada ao Spanning-tree que permita desabilitar uma porta de acesso assim que a mesma receba uma BPDU;

3.2.33. Implementar 4000 VLANs por porta, ativas simultaneamente, através do protocolo 802.1Q;

3.2.34. Deverá permitir a criação, remoção, gerenciamento e distribuição de VLANs de forma dinâmica através de portas configuradas como tronco IEEE 802.1Q utilizando o protocolo MVRP segundo o padrão IEEE802.1ak;

3.2.35. Possibilitar a coleta de estatísticas de tráfego baseada em VLANs IEEE 802.1Q e double-tagged VLANs IEEE 802.1ad;

3.2.36. Implementar MAC Based VLAN;

3.2.37. Implementar VLAN Translation;

3.2.38. Implementar VLAN Aggregation ou funcionalidade que permita o compartilhamento de uma mesma subnet e de um mesmo endereço IPv4 utilizado como default-gateway por hosts de diferentes VLANs;

3.2.39. Implementar Private VLANs;

3.2.40. Implementar Port Isolation ou funcionalidade que permita isolamento de portas específicas do switch. As portas isoladas não devem se comunicar entre si, porém podem se comunicar com qualquer outra porta no equipamento que não esteja isolada;

3.2.41. Implementar IEEE 802.1ad com a possibilidade de associar CVIDs específicos para diferentes SVIDs (selective Q-in-Q ou 802.1ad CEP). A implementação deverá permitir a tradução do CVID;

3.2.42. Implementar IEEE 802.1ag (Connectivity Fault Management);

3.2.43. Implementar funcionalidade baseada na recomendação do ITU-T Y.1731 com medição de, no mínimo, Frame Delay;

3.2.44. Implementar o protocolo ITU-T G.8032 ERPS;

3.2.45. Implementar protocolo de resiliência em camada 2, específico para topologias em anel, que permita tempo de convergência inferior a 200 ms;

3.2.46. Implementar IEEE 802.1ab Link Layer Discovery Protocol (LLDP);

3.2.47. Implementar LLDP-MED (Media Endpoint Discovery);

3.2.48. Implementar roteamento estático com suporte a, no mínimo, 32 rotas;

3.2.49. Implementar, no mínimo, 30 interfaces IP (IPv4 ou IPv6);

3.2.50. Implementar PIM Snooping;

3.2.51. Deve implementar Dual Stack, ou seja, IPv6 e IPv4, com suporte as seguintes funcionalidades/RFCs:

3.2.51.1. RFC 1981, Path MTU Discovery for IPv6, August 1996 - Host Requirements;

3.2.51.2. RFC 5095, Internet Protocol, Version 6 (IPv6) Specification;

3.2.51.3. RFC 4861, Neighbor Discovery for IP Version 6, (IPv6);

3.2.51.4. RFC 2462, IPv6 Stateless Address Auto configuration - Host Requirements;

3.2.51.5. RFC 2463, Internet Control Message Protocol (ICMPv6) for the IPv6 Specification;

3.2.51.6. RFC 2464, Transmission of IPv6 Packets over Ethernet Networks;

3.2.51.7. RFC 2465, IPv6 MIB, General Group and Textual Conventions;

3.2.51.8. RFC 2466, MIB for ICMPv6;

3.2.51.9. RFC 3513, Internet Protocol Version 6 (IPv6) Addressing Architecture;

3.2.51.10. RFC 3587, Global Unicast Address Format;

3.2.52. Implementar os seguintes protocolos em IPv6: Ping, Traceroute, Telnet, SSHv2, SNMP, Syslog, SNTP e DNS;

3.2.53. Deve implementar IPv6 de acordo com as seguintes RFCs:

3.2.53.1. RFC 1981, Path MTU Discovery for IPv6, August 1996 - Router Requirements;

3.2.53.2. RFC 2462, IPv6 Stateless Address Auto configuration - Router Requirements;

3.2.53.3. RFC 2462, IPv6 Stateless Address Auto configuration - Router Requirements;

3.2.53.4. RFC 2710, IPv6 Multicast Listener Discovery v1 (MLDv1) Protocol;

3.2.53.5. RFC 3810, IPv6 Multicast Listener Discovery v2 (MLDv2) Protocol;

3.2.53.6. RFC 6106, IPv6 Router Advertisement Options for DNS Configuration;

3.2.54. Implementar Policy Based Routing;

3.2.55. Implementar upload e download de configuração em formato ASCII ou XML, permitindo a edição do arquivo de configuração e, posteriormente, o download do arquivo editado para o equipamento;

3.2.56. Implementar TACACS+ segundo a RFC 1492;

3.2.57. Implementar autenticação RADIUS com suporte a:

3.2.57.1. RFC 2865 RADIUS Authentication;

3.2.57.2. RFC 2866 RADIUS Accounting;

3.2.57.3. RFC 3579 RADIUS EAP support for 802.1X;

3.2.58. A implementação de RADIUS deve suportar alteração dinâmica de parâmetros de autorização de uma sessão que já esteja ativa;

3.2.59. A implementação de RADIUS e TACACS+ deve estar disponível para autenticação de usuários via Telnet e Console serial;

3.2.60. Implementar per-command authorization para RADIUS e TACACS+;

3.2.61. Possuir DNS Client para IPv4 segundo a RFC 1591 e DNS Client para IPv6;

3.2.62. Possuir Telnet client and server segundo a RFC 854;

3.2.63. Implementar os seguintes grupos de RMON através da RFC 1757: History, Statistics, Alarms e Events;

3.2.64. Deve implementar RMON2-probe configuration segundo a RFC 2021, podendo ser implementada internamente no switch ou externamente, por meio de probe em hardware utilizando uma porta 1000BaseTX;

3.2.65. Implementar sFlow ou Netflow, em hardware;

3.2.66. Implementar a atualização de imagens de software e configuração através de um servidor TFTP;

3.2.67. Suportar múltiplos servidores Syslog;

3.2.68. Implementar Port Mirroring, permitindo espelhar portas físicas ou VLANs para portas de destino (portas de análise);

3.2.69. Implementar RSPAN (Remote Mirroring), permitindo espelhar o tráfego de uma porta ou VLAN de um switch remoto para uma porta de um switch local (porta de análise);

3.2.70. Implementar gerenciamento através de SNMPv1 (RFC 1157), v2c (RFCs 1901 a 1908), v3 (RFCs 3410 a 3415) e SNMP para IPv6;

3.2.71. Implementar SMON de acordo com a RFC 2613;

3.2.72. Implementar cliente e servidor SSHv2;

3.2.73. Implementar cliente e servidor SCP e servidor SFTP;

3.2.74. Implementar gerenciamento via web com suporte a HTTP e HTTPS/SSL, permitindo visualização gráfica da utilização (em percentual, bytes e pacotes) das portas;

3.2.75. A interface gráfica deve permitir visualização de informações do sistema (VLAN, Portas, Fonte e Fans), monitoramento de Log, utilização de portas, QoS e configuração de portas, VLANs e ACLs;

3.2.76. O equipamento ofertado deve possuir um sistema operacional modular;

3.2.77. O sistema operacional deve possuir função grep/pipe para filtrar a saída de determinado comando;

3.2.78. O sistema operacional deve possuir comandos para visualização e monitoração de cada processo, sendo possível verificar por processo qual o consumo de cpu, process-id e qual o consumo de memória por processo;

3.2.79. O sistema operacional deve possuir comandos para que processos sejam terminados ou reiniciados sem que seja necessário a reinicialização do equipamento. Esta funcionalidade deve estar disponível pelo menos para Telnet, TFTP, HTTP e LLDP na versão atual;

3.2.80. Implementar linguagem de scripting baseada em Python, permitindo a automatização de tarefas. A linguagem deve implementar estruturas de controle como loops e execução condicional e permitir a definição de variáveis;

3.2.81. Implementar protocolo de monitoramento de status de comunicação entre dois switches, que possibilite que uma porta seja desabilitada caso seja detectada uma falha de comunicação entre os dois peers;

3.2.82. Implementar funcionalidade que permita sua auto-configuração através dos protocolos DHCP e TFTP, permitindo o provisionamento em massa com o mínimo de intervenção humana;

3.2.83. Deve disponibilizar API (Aplication Programming Interface) aberta para integração com aplicações;

3.2.84. Implementar Rate limiting de entrada em todas as portas. A granularidade deve ser configurável em intervalos de 64Kbps para portas de até 1Gbps. Caso o equipamento ofertado possua suporte a portas 10Gbps, a granularidade para este tipo de interface deve ser configurável em intervalos de 1Mbps. A implementação de Rate Limiting deve permitir a classificação do tráfego utilizando-se ACLs e parâmetros, MAC origem e destino (simultaneamente) IP origem e destino (simultaneamente), portas TCP, portas UDP e campo 802.1p;

3.2.85. Implementar Rate Shaping de saída em todas as portas. A granularidade deve ser configurável em intervalos de 64Kbps para portas de até 1Gbps. Caso o equipamento ofertado possua suporte a portas 10Gbps, a granularidade para este tipo de interface deve ser configurável em intervalos de 1Mbps;

3.2.86. A funcionalidade de Rate Shaping deve permitir a configuração de CIR (Commited Rate), banda máxima, banda mínima e peak rate;

3.2.87. Implementar a leitura, classificação e remarcação de QoS (802.1p e DSCP);

3.2.88. Implementar remarcação de prioridade de pacotes Layer 3, remarcando o campo DiffServ para grupos de tráfego classificados segundo portas TCP e UDP, endereço/subrede IP, VLAN e MAC origem e destino;

3.2.89. Implementar 8 filas de prioridade em hardware por porta;

3.2.90. Implementar os algoritmos de gerenciamento de filas WRR (Weighted Round Robin), WDRR (Weighted Deficit Round Robin) e SP (Strict Priority);

3.2.91. Deve implementar, ao menos dois dos algoritimos acima, simultaneamente em uma mesma porta;

3.2.92. Implementar as seguintes RFCs:

3.2.92.1. RFC 2474 DiffServ Precedence;

3.2.92.2. RFC 2598 DiffServ Expedited Forwarding (EF);

3.2.92.3. RFC 2597 DiffServ Assured Forwarding (AF);

3.2.92.4. RFC 2475 DiffServ Core and Edge Router Functions;

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

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

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

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

3.2.97. Implementar Gratuitous ARP Protection;

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

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

3.2.100. Implementar travamento de endereços MAC, permitindo a adição estática de endereços para uma

determinada porta ou utilizando os endereços existentes na tabela MAC. O acesso de qualquer outro endereço que não esteja previamente autorizado deve ser negado;

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

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

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

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

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

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

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

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

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

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

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

3.2.112. Implementar Policy Based Switching, ou seja, possibilitar que o tráfego classificado por uma ACL seja redirecionado para uma porta física específica;

3.2.113. Implementar funcionalidade que permita o mapeamento de usuários identificados via Kerberos (com a credencial de usuário no domínio), IEEE 802.1x e LLDP, provendo informações como endereço MAC, VLAN e porta física. Estas informações devem estar disponíveis na linha de comando (CLI) do equipamento;

3.2.114. O equipamento ofertado deve permitir que ele faça parte de uma malha ethernet (Fabric Ethernet) descrito nos switches distribuição com as seguintes funcionalidades:

3.2.115. O equipamento ofertado deve permitir a configuração como elemento anexo à malha ethernet;

3.2.116. O equipamento ofertado deve permitir a criação de VLANS mapeadas a serviços virtuais de rede, de que forma os serviços sejam criados automaticamente no elemento de borda da malha e propagados de maneira automática nos demais equipamentos que compõem a malha ethernet;

3.2.117. Deve permitir o gerenciamento do equipamento através de software de gerência do Fabric;

3.2.118. Deve possuir garantia do fabricante ou da revenda, desde que essa seja autorizada por carta pelo fabricante dos equipamentos a prestar o suporte e garantia, pelo período de 60 meses;

3.2.118. Marca/Modelo/Séries de Referencia: Extreme Networks X435, Alcatel Lucent 6360, Ruckus 7150, Juniper EX2300, Cisco 9200 e Aruba 2930F.

3.3. Switch de Acesso Tipo III

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

3.3.2. A solução deve ser composta de um único equipamento, montável em rack 19” devendo este vir acompanhado dos devidos acessórios para tal e possuir altura máxima de 1RU;

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

3.3.4. Possuir LEDS indicativos de funcionamento da fonte de alimentação e status das portas;

3.3.5. Deve possuir homologação ANATEL, de acordo com a resolução vigente;

3.3.6. Deve possuir pelo menos 48 portas 10/100/1000BASE-T;

3.3.7. Deve possuir pelo menos 04 portas 1000BASE-X baseadas em SFP;

3.3.8. Deve possuir uma porta USB ou micro-USB para transferência de arquivos;

3.3.9. Possuir uma porta console com conector RJ-45 ou DB9 macho;

3.3.10. Todas as interfaces Gigabit Ethernet solicitadas neste termo de referência devem funcionar simultaneamente;

3.3.11. Todas as interfaces ofertadas devem ser non-blocking;

3.3.12. Deve possuir detecção automática MDI/MDIX em todas as portas 10/100/1000BASE-T;

3.3.13. Deve possuir capacidade de processamento de pelo menos 256Gbps;

3.3.14. Deve possuir capacidade de encaminhamento de pelo menos 190Mpps;

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

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

3.3.17. O equipamento deve suportar o agrupamento lógico (gerência por um único IP) de unidades remotamente instaladas;

3.3.18. O empilhamento deve possuir velocidade de pelo menos 20Gbps cada (ou 10Gbps Full Duplex), totalizando 40 Gbps (ou 20 Gbps full-duplex). Este empilhamento poderá ser feito através de portas SFP+, X2, XENPAK ou XFP, sendo essas portas adicionais às solicitadas anteriormente;

3.3.19. O empilhamento deve possuir arquitetura de anel para prover resiliência.;

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

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

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

3.3.23. Deve armazenar, no mínimo, 32.000 (trinta e dois mil) endereços MAC;

3.3.24. Implementar, no mínimo, 4.000 (quatro mil) regras de ACL de entrada (ingress ACLs);

3.3.25. Implementar, no mínimo, 500 (quinhentas mil) regras de ACL de saída (egress ACLs);

3.3.26. Implementar 4000 VLANs por porta, ativas simultaneamente, através do protocolo 802.1Q;

3.3.27. Implementar agregação de links conforme padrão IEEE 802.3ad com suporte a LACP;

3.3.28. Em conjunto com outro equipamento de mesmo modelo, deverá permitir que um switch conectado aos dois, tenha a possibilidade de agregação de links (IEEE 802.3ad) com suporte a LACP com os mesmos, de forma a simular a existência de apenas um único link lógico entre este equipamento e os dois

switches do modelo aqui especificado (Multi-Chassis Trunking, por exemplo). O único link lógico entre as camadas deve eliminar convergência do Spanning Tree, possibilitando o tráfego simultâneo por mais de uma conexão;

3.3.29. Implementar Proxy-ARP (RFC 1027);

3.3.30. Implementar IGMP v1, v2 e v3 Snooping;

3.3.31. Implementar IGMPv1 (RFC 1112), IGMP v2 (RFC 2236) e IGMPv3 (RFC 3376);

3.3.32. Implementar MVR (Multicast VLAN Registration);

3.3.33. Implementar DHCP/Bootp relay configurável por VLAN para IPv4 e IPv6;

3.3.34. Implementar servidor DHCP interno que permita a configuração de um intervalo de endereços IP a serem atribuídos os clientes DHCP e possibilite ainda a atribuição de, no mínimo, default-gateway, servidor DNS e servidor WINS;

3.3.35. Implementar DHCP Option 82, de acordo com a RFC 3046, com identificação de porta e VLAN, configurável por VLAN;

3.3.36. Implementar DHCP Client para IPv4 e IPv6;

3.3.37. Implementar RFC 3021 - Using 31-Bit Prefixes on IPv4 Point-to-Point Links;

3.3.38. Implementar Spanning-Tree (IEEE 802.1d), Rapid Spanning Tree (IEEE 802.1w), Multiple Instance STP (802.1s) e PVST+;

3.3.39. Implementar a configuração de Multiple Spanning Tree Protocol, com suporte a, pelo menos, 32 domínios;

3.3.40. Implementar funcionalidade vinculada ao Spanning-tree onde é possível designar portas de acesso (por exemplo onde estações estão conectadas) que não sofram o processo de Listening-Learning, passando direto para o estado de Forwarding. No entanto, as portas configuradas com esta funcionalidade devem detectar loops na rede normalmente;

3.3.41. Implementar funcionalidade vinculada ao Spanning-tree que evite a eleição de outros switches da rede como Root;

3.3.42. Implementar funcionalidade vinculada ao Spanning-tree que permita desabilitar uma porta de acesso assim que a mesma receba uma BPDU;

3.3.43. Deverá permitir a criação, remoção, gerenciamento e distribuição de VLANs de forma dinâmica através de portas configuradas como tronco IEEE 802.1Q utilizando o protocolo MVRP segundo o padrão IEEE802.1ak;

3.3.44. Possibilitar a coleta de estatísticas de tráfego baseada em VLANs IEEE 802.1Q e double-tagged VLANs IEEE 802.1ad;

3.3.45. Implementar MAC Based VLAN;

3.3.46. Implementar VLAN Translation;

3.3.47. Implementar Private VLANs;

3.3.48. Implementar Port Isolation ou funcionalidade que permita isolamento de portas específicas do switch. As portas isoladas não devem se comunicar entre si, porém podem se comunicar com qualquer outra porta no equipamento que não esteja isolada;

3.3.49. Implementar Private VLANs;

3.3.50. Implementar Port Isolation ou funcionalidade que permita isolamento de portas específicas do switch. As portas isoladas não devem se comunicar entre si, porém podem se comunicar com qualquer outra porta no equipamento que não esteja isolada;

3.3.51. Implementar IEEE 802.1ad com a possibilidade de associar CVIDs específicos para diferentes SVIDs (selective Q-in-Q ou 802.1ad CEP). A implementação deverá permitir a tradução do CVID;

3.3.52. Implementar IEEE 802.1ag (Connectivity Fault Management);

3.3.53. Implementar IEEE 802.3ah Ethernet OAM – Unidirectional Link Fault Management;

3.3.54. Implementar funcionalidade baseada na recomendação do ITU-T Y.1731 com medição de, no mínimo, Frame Delay;

3.3.55. Implementar o protocolo ITU-T G.8032 ERPS;

3.3.56. Implementar protocolo de resiliência em camada 2, específico para topologias em anel, que permita tempo de convergência inferior a 200 ms;

3.3.57. Implementar IEEE 802.1ab Link Layer Discovery Protocol (LLDP);

3.3.58. Implementar LLDP-MED (Media Endpoint Discovery);

3.3.59. Implementar os protocolos de roteamento IP: RFC 1058 – RIP v1 e RFC 2453 – RIP v2;

3.3.60. Suportar o protocolo de roteamento OSPFv2, incluindo autenticação MD5;

3.3.61. Suportar o protocolo de roteamento OSPFv2 (RFC 2328), incluindo autenticação MD5;

3.3.62. A implementação de OSPF deve estar de acordo com as seguintes RFCs:

3.3.62.1. RFC 1587 The OSPF NSSA Option;

3.3.62.2. RFC 1765 OSPF Database Overflow;

3.3.62.3. RFC 2370 The OSPF Opaque LSA Option;

3.3.62.4. RFC 3623 Graceful OSPF Restart;

3.3.63. Implementar PIM Snooping;

3.3.64. Suportar protocolo de multicast PIM-SM para IPv4 e IPv6;

3.3.65. Suportar PIM-DM para IPv4 e IPv6;

3.3.66. Suportar PIM-SSM segundo a RFC 3569;

3.3.67. Suportar MSDP (Multicast Source Discovery Protocol), de acordo com a RFC 3618;

3.3.68. Suportar VRRPv3 (RFC 5798);

3.3.69. Deve suportar BGPv4 de acordo com as seguintes RFCs:

3.3.69.1. RFC 4271, Border Gateway Protocol 4;

3.3.69.2. RFC 5065, Autonomous System Confederations for BGP;

3.3.69.3. RFC 4456, BGP Route Reflection;

3.3.69.4. RFC 1997, BGP Communities Attribute;

3.3.69.5. RFC 1745, BGP4/IDRP for IP-OSPF Interaction;

3.3.69.6. RFC 2439, BGP Route Flap Damping;

3.3.69.7. RFC 5492, Capabilities Advertisement with BGP-4;

3.3.69.8. RFC 2918, Route Refresh Capability for BGP-4;

3.3.69.9. RFC 4360, BGP Extended Communities Attribute;

3.3.69.10. RFC 4760, Multiprotocol Extensions for BGP4;

3.3.69.11. RFC 4724, Graceful Restart Mechanism for BGP;

3.3.69.12. RFC 6793, BGP Support for four-octet AS number space;

3.3.70. Deve implementar Dual Stack, ou seja, IPv6 e IPv4, com suporte as seguintes funcionalidades/RFCs:

3.3.70.1. RFC 1981, Path MTU Discovery for IPv6, August 1996 - Host Requirements;

3.3.70.2. RFC 5095, Internet Protocol, Version 6 (IPv6) Specification;

3.3.70.3. RFC 4861, Neighbor Discovery for IP Version 6, (IPv6);

3.3.70.4. RFC 2462, IPv6 Stateless Address Auto configuration - Host Requirements;

3.3.70.5. RFC 2463, Internet Control Message Protocol (ICMPv6) for the IPv6 Specification;

3.3.70.6. RFC 2464, Transmission of IPv6 Packets over Ethernet Networks;

3.3.70.7. RFC 2465, IPv6 MIB, General Group and Textual Conventions;

3.3.70.8. RFC 2466, MIB for ICMPv6;

3.3.70.9. RFC 3513, Internet Protocol Version 6 (IPv6) Addressing Architecture;

3.3.70.10. RFC 3587, Global Unicast Address Format;

3.3.71. Implementar os seguintes protocolos em IPv6: Ping, Traceroute, Telnet, SSHv2, SNMP, Syslog, SNTP e DNS;

3.3.72. Deve implementar IPv6 de acordo com as seguintes RFCs:

3.3.72.1. RFC 1981, Path MTU Discovery for IPv6, August 1996 - Router Requirements;

3.3.72.2. RFC 2462, IPv6 Stateless Address Auto configuration - Router Requirements;

3.3.72.3. RFC 2080, RIPng;

3.3.72.4. RFC 2462, IPv6 Stateless Address Auto configuration - Router Requirements;

3.3.72.5. RFC 2710, IPv6 Multicast Listener Discovery v1 (MLDv1) Protocol;

3.3.72.6. RFC 3810, IPv6 Multicast Listener Discovery v2 (MLDv2) Protocol;

3.3.72.7. RFC 6106, IPv6 Router Advertisement Options for DNS Configuration;

3.3.73. Suportar OSPFv3 conforme a RFC 5340;

3.3.74. Suportar OSPFv3 Graceful Restart conforme RFC 5187;

3.3.75. Suportar IS-IS, de acordo com as seguintes RFCs:

3.3.75.1. RFC 1195, Use of OSI IS-IS for Routing in TCP/IP and Dual Environments (TCP/IP transport only);

3.3.75.2. RFC 2763, Dynamic Hostname Exchange Mechanism for IS-IS;

3.3.75.3. RFC 2966, Domain-wide Prefix Distribution with Two-Level IS-IS;

3.3.75.4. RFC 2973, IS-IS Mesh Groups;

3.3.75.5. Draft-ietf-isis-restart-02, Restart Signaling for IS-IS;

3.3.75.6. Draft-ietf-isis-ipv6-06, Routing IPv6 with IS-IS;

3.3.75.7. Draft-ietf-isis-wg-multi-topology-11, Multi Topology (MT) Routing in IS-IS;

3.3.76. Implementar upload e download de configuração em formato ASCII ou XML, permitindo a edição do arquivo de configuração e, posteriormente, o download do arquivo editado para o equipamento;

3.3.77. Implementar TACACS+ segundo a RFC 1492;

3.3.78. Implementar autenticação RADIUS com suporte a:

3.3.79. RFC 2865 RADIUS Authentication;

3.3.80. RFC 2866 RADIUS Accounting;

3.3.81. RFC 3579 RADIUS EAP support for 802.1X;

3.3.82. A implementação de RADIUS deve suportar alteração dinâmica de parâmetros de autorização de uma sessão que já esteja ativa;

3.3.83. A implementação de RADIUS e TACACS+ deve estar disponível para autenticação de usuários via Telnet e Console serial;

3.3.84. Implementar per-command authorization para RADIUS e TACACS+;

3.3.85. Possuir DNS Client para IPv4 segundo a RFC 1591 e DNS Client para IPv6;

3.3.86. Possuir Telnet client and server segundo a RFC 854;

3.3.87. Implementar os seguintes grupos de RMON através da RFC 1757: History, Statistics, Alarms e Events;

3.3.88. Deve implementar RMON2-probe configuration segundo a RFC 2021, podendo ser implementada internamente no switch ou externamente, por meio de probe em hardware utilizando uma porta 1000BaseTX;

3.3.89. Implementar sFlow ou Netflow, em hardware;

3.3.90. Implementar a atualização de imagens de software e configuração através de um servidor TFTP;

3.3.91. Suportar múltiplos servidores Syslog;

3.3.92. Implementar ajuste de clock do equipamento utilizando NTP com autenticação MD5 e SNTP;

3.3.93. Implementar Port Mirroring, permitindo espelhar até 128 portas físicas ou 16 VLANs para até 16 portas de destino (portas de análise). Deve ser possível configurar mais de uma sessão de espelhamento simultânea;

3.3.94. Implementar RSPAN (Remote Mirroring), permitindo espelhar o tráfego de uma porta ou VLAN de um switch remoto para uma porta de um switch local (porta de análise);

3.3.95. Implementar gerenciamento através de SNMPv1 (RFC 1157), v2c (RFCs 1901 a 1908), v3 (RFCs 3410 a 3415) e SNMP para IPv6;

3.3.96. Implementar SMON de acordo com a RFC 2613;

3.3.97. Implementar cliente e servidor SSHv2;

3.3.98. Implementar cliente e servidor SCP e servidor SFTP;

3.3.99. Implementar gerenciamento via web com suporte a HTTP e HTTPS/SSL, permitindo visualização gráfica da utilização (em percentual, bytes e pacotes) das portas;

3.3.100. A interface gráfica deve permitir visualização de informações do sistema (VLAN, Portas, Fonte e Fans), monitoramento de Log, utilização de portas, QoS e configuração de portas, VLANs e ACLs;

3.3.101. O equipamento ofertado deve possuir um sistema operacional modular;

3.3.102. O sistema operacional deve possuir função grep/pipe para filtrar a saída de determinado comando;

3.3.103. O sistema operacional deve possuir comandos para visualização e monitoração de cada processo, sendo possível verificar por processo qual o consumo de cpu, process-id e qual o consumo de memória por processo;

3.3.104. O sistema operacional deve possuir comandos para que processos sejam terminados ou reiniciados sem que seja necessário a reinicialização do equipamento. Esta funcionalidade deve estar disponível pelo menos para Telnet, TFTP, HTTP e LLDP na versão atual;

3.3.105. O sistema operacional deve possuir comandos para que processos sejam terminados ou reiniciados sem que seja necessário a reinicialização do equipamento. Esta funcionalidade deve estar disponível pelo menos para Telnet, TFTP, HTTP, LLDP, OSPF e BGP na versão atual;

3.3.106. Implementar linguagem de scripting baseada em Python, permitindo a automatização de tarefas. A linguagem deve implementar estruturas de controle como loops e execução condicional e permitir a definição de variáveis;

3.3.107. Implementar protocolo de monitoramento de status de comunicação entre dois switches, que possibilite que uma porta seja desabilitada caso seja detectada uma falha de comunicação entre os dois peers;

3.3.108. Implementar funcionalidade que permita sua auto-configuração através dos protocolos DHCP e TFTP, permitindo o provisionamento em massa com o mínimo de intervenção humana;

3.3.109. Deve disponibilizar API (Aplication Programming Interface) aberta para integração com aplicações;

3.3.110. Implementar Rate limiting de entrada em todas as portas. A granularidade deve ser configurável em intervalos de 64Kbps para portas de até 1Gbps. Caso o equipamento ofertado possua suporte a portas 10Gbps, a granularidade para este tipo de interface deve ser configurável em intervalos de 1Mbps. A implementação de Rate Limiting deve permitir a classificação do tráfego utilizando-se ACLs e parâmetros, MAC origem e destino (simultaneamente) IP origem e destino (simultaneamente), portas TCP, portas UDP e campo 802.1p;

3.3.111. Implementar Rate Shaping de saída em todas as portas. A granularidade deve ser configurável em intervalos de 64Kbps para portas de até 1Gbps. Caso o equipamento ofertado possua suporte a portas 10Gbps, a granularidade para este tipo de interface deve ser configurável em intervalos de 1Mbps;

3.3.112. A funcionalidade de Rate Shaping deve permitir a configuração de CIR (Commited Rate), banda máxima, banda mínima e peak rate;

3.3.113. Implementar a leitura, classificação e remarcação de QoS (802.1p e DSCP);

3.3.114. Implementar remarcação de prioridade de pacotes Layer 3, remarcando o campo DiffServ para grupos de tráfego classificados segundo portas TCP e UDP, endereço/subrede IP, VLAN e MAC origem e destino;

3.3.115. Implementar 8 filas de prioridade em hardware por porta;

3.3.116. Implementar os algoritmos de gerenciamento de filas WRR (Weighted Round Robin), WDRR (Weighted Deficit Round Robin) e SP (Strict Priority);

3.3.117. Deve implementar, ao menos dois dos algoritimos acima, simultaneamente em uma mesma porta;

3.3.118. Implementar as seguintes RFCs:

3.3.118.1. RFC 2474 DiffServ Precedence;

3.3.118.2. RFC 2598 DiffServ Expedited Forwarding (EF);

3.3.118.3. RFC 2597 DiffServ Assured Forwarding (AF);

3.3.118.4. RFC 2475 DiffServ Core and Edge Router Functions;

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

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

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

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

3.3.122. Implementar Gratuitous ARP Protection;

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

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

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

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

3.3.127. A implementação do IEEE 802.1x deve incluir suporte a Guest VLAN, encaminhando o usuário

para esta VLAN caso este não possua suplicante 802.1x ativo, em caso de falha de autenticação e no caso de indisponibilidade do servidor AAA;

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

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

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

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

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

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

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

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

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

3.3.137. Implementar Policy Based Switching, ou seja, possibilitar que o tráfego classificado por uma ACL seja redirecionado para uma porta física específica;

3.3.138. Implementar funcionalidade que permita o mapeamento de usuários identificados via Kerberos (com a credencial de usuário no domínio), IEEE 802.1x e LLDP, provendo informações como endereço MAC, VLAN e porta física. Estas informações devem estar disponíveis na linha de comando (CLI) do equipamento;

3.3.139. O equipamento ofertado deve permitir que o mesmo faça parte de uma malha ethernet (Fabric Ethernet) descrito nos switches tipo distribuição com as seguintes funcionalidades:

3.3.140. O equipamento ofertado deve permitir a configuração como elemento anexo à malha ethernet;

3.3.141. O equipamento ofertado deve permitir a criação de VLANS mapeadas a serviços virtuais de rede, de que forma os serviços sejam criados automaticamente no elemento de borda da malha e propagados de maneira automática nos demais equipamentos que compõem a malha ethernet;

3.3.142. Deve permitir o gerenciamento do equipamento através de software de gerência do Fabric;

3.3.143. Deve possuir garantia do fabricante ou da revenda, desde que essa seja autorizada por carta pelo fabricante dos equipamentos a prestar o suporte e garantia, pelo período de 60 meses. A garantia deverá ser do tipo NBD com troca de equipamentos em caso de falha;

3.3.144. Marca/Modelo/Séries de Referencia: Extreme Networks 5320, Alcatel Lucent 6560, Ruckus 7450, Juniper EX3400, Cisco 9300 e Aruba 6200.

3.4. Switch de Acesso Tipo IV

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

3.4.2. A solução deve ser composta de um único equipamento, montável em rack 19” devendo este vir

acompanhado dos devidos acessórios para tal e possuir altura máxima de 1RU;

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

3.4.4. Possuir LEDS indicativos de funcionamento da fonte de alimentação e status das portas;

3.4.5. Deve possuir homologação ANATEL, de acordo com a resolução vigente;

3.4.6. Deve possuir pelo menos 24 portas 10/100/1000BASE-T;

3.4.7. Deve possuir pelo menos 04 portas 10GBASE-X baseadas em SFP+;

3.4.8. Deve possuir uma porta USB ou micro-USB para transferência de arquivos;

3.4.9. Possuir uma porta console com conector RJ-45 ou DB9 macho;

3.4.10. Todas as interfaces Gigabit Ethernet solicitadas neste termo de referência devem funcionar simultaneamente;

3.4.11. Todas as interfaces ofertadas devem ser non-blocking;

3.4.12. Deve possuir detecção automática MDI/MDIX em todas as portas 10/100/1000BASE-T;

3.4.13. Deve possuir capacidade de processamento de pelo menos 208Gbps;

3.4.14. Deve possuir capacidade de encaminhamento de pelo menos 154Mpps;

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

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

3.4.17. O equipamento deve suportar o agrupamento lógico (gerência por um único IP) de unidades remotamente instaladas;

3.4.18. O empilhamento deve possuir velocidade de pelo menos 20Gbps cada (ou 10Gbps Full Duplex), totalizando 40 Gbps (ou 20 Gbps full-duplex). Este empilhamento poderá ser feito através de portas SFP+, X2, XENPAK ou XFP, sendo essas portas adicionais às solicitadas anteriormente;

3.4.19. O empilhamento deve possuir arquitetura de anel para prover resiliência;

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

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

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

3.4.23. Deve armazenar, no mínimo, 32.000 (trinta e dois mil) endereços MAC;

3.4.24. Implementar, no mínimo, 4.000 (quatro mil) regras de ACL de entrada (ingress ACLs);

3.4.25. Implementar, no mínimo, 500 (quinhentas mil) regras de ACL de saída (egress ACLs);

3.4.26. Implementar 4000 VLANs por porta, ativas simultaneamente, através do protocolo 802.1Q;

3.4.27. Implementar agregação de links conforme padrão IEEE 802.3ad com suporte a LACP;

3.4.28. Em conjunto com outro equipamento de mesmo modelo, deverá permitir que um switch conectado aos dois, tenha a possibilidade de agregação de links (IEEE 802.3ad) com suporte a LACP com os mesmos, de forma a simular a existência de apenas um único link lógico entre este equipamento e os dois switches do modelo aqui especificado (Multi-Chassis Trunking, por exemplo). O único link lógico entre as camadas deve eliminar convergência do Spanning Tree, possibilitando o tráfego simultâneo por mais de uma conexão;

3.4.29. Implementar Proxy-ARP (RFC 1027);

3.4.30. Implementar IGMP v1, v2 e v3 Snooping;

3.4.31. Implementar IGMPv1 (RFC 1112), IGMP v2 (RFC 2236) e IGMPv3 (RFC 3376);

3.4.32. Implementar MVR (Multicast VLAN Registration);

3.4.33. Implementar DHCP/Bootp relay configurável por VLAN para IPv4 e IPv6;

3.4.34. Implementar servidor DHCP interno que permita a configuração de um intervalo de endereços IP a serem atribuídos os clientes DHCP e possibilite ainda a atribuição de, no mínimo, default-gateway, servidor DNS e servidor WINS;

3.4.35. Implementar DHCP Option 82, de acordo com a RFC 3046, com identificação de porta e VLAN, configurável por VLAN;

3.4.36. Implementar DHCP Client para IPv4 e IPv6;

3.4.37. Implementar RFC 3021 - Using 31-Bit Prefixes on IPv4 Point-to-Point Links;

3.4.38. Implementar Spanning-Tree (IEEE 802.1d), Rapid Spanning Tree (IEEE 802.1w), Multiple Instance STP (802.1s) e PVST+;

3.4.39. Implementar a configuração de Multiple Spanning Tree Protocol, com suporte a, pelo menos, 32 domínios;

3.4.40. Implementar funcionalidade vinculada ao Spanning-tree onde é possível designar portas de acesso (por exemplo onde estações estão conectadas) que não sofram o processo de Listening-Learning, passando direto para o estado de Forwarding. No entanto, as portas configuradas com esta funcionalidade devem detectar loops na rede normalmente;

3.4.41. Implementar funcionalidade vinculada ao Spanning-tree que evite a eleição de outros switches da rede como Root;

3.4.42. Implementar funcionalidade vinculada ao Spanning-tree que permita desabilitar uma porta de acesso assim que a mesma receba uma BPDU;

3.4.43. Deverá permitir a criação, remoção, gerenciamento e distribuição de VLANs de forma dinâmica através de portas configuradas como tronco IEEE 802.1Q utilizando o protocolo MVRP segundo o padrão IEEE802.1ak;

3.4.44. Possibilitar a coleta de estatísticas de tráfego baseada em VLANs IEEE 802.1Q e double-tagged VLANs IEEE 802.1ad;

3.4.45. Implementar MAC Based VLAN;

3.4.46. Implementar VLAN Translation;

3.4.47. Implementar Private VLANs;

3.4.48. Implementar Port Isolation ou funcionalidade que permita isolamento de portas específicas do switch. As portas isoladas não devem se comunicar entre si, porém podem se comunicar com qualquer outra porta no equipamento que não esteja isolada;

3.4.49. Implementar Private VLANs;

3.4.50. Implementar Port Isolation ou funcionalidade que permita isolamento de portas específicas do switch. As portas isoladas não devem se comunicar entre si, porém podem se comunicar com qualquer outra porta no equipamento que não esteja isolada;

3.4.51. Implementar IEEE 802.1ad com a possibilidade de associar CVIDs específicos para diferentes SVIDs (selective Q-in-Q ou 802.1ad CEP). A implementação deverá permitir a tradução do CVID;

3.4.52. Implementar IEEE 802.1ag (Connectivity Fault Management);

3.4.53. Implementar IEEE 802.3ah Ethernet OAM – Unidirectional Link Fault Management;

3.4.54. Implementar funcionalidade baseada na recomendação do ITU-T Y.1731 com medição de, no mínimo, Frame Delay;

3.4.55. Implementar o protocolo ITU-T G.8032 ERPS;

3.4.56. Implementar protocolo de resiliência em camada 2, específico para topologias em anel, que permita tempo de convergência inferior a 200 ms;

3.4.57. Implementar IEEE 802.1ab Link Layer Discovery Protocol (LLDP);

3.4.58. Implementar LLDP-MED (Media Endpoint Discovery);

3.4.59. Implementar os protocolos de roteamento IP: RFC 1058 – RIP v1 e RFC 2453 – RIP v2;

3.4.60. Suportar o protocolo de roteamento OSPFv2, incluindo autenticação MD5;

3.4.61. Suportar o protocolo de roteamento OSPFv2 (RFC 2328), incluindo autenticação MD5;

3.4.62. A implementação de OSPF deve estar de acordo com as seguintes RFCs:

3.4.62.1. RFC 1587 The OSPF NSSA Option;

3.4.62.2. RFC 1765 OSPF Database Overflow;

3.4.62.3. RFC 2370 The OSPF Opaque LSA Option;

3.4.62.4. RFC 3623 Graceful OSPF Restart;

3.4.63. Implementar PIM Snooping;

3.4.64. Suportar protocolo de multicast PIM-SM para IPv4 e IPv6;

3.4.65. Suportar PIM-DM para IPv4 e IPv6;

3.4.66. Suportar PIM-SSM segundo a RFC 3569;

3.4.67. Suportar MSDP (Multicast Source Discovery Protocol), de acordo com a RFC 3618;

3.4.68. Suportar VRRPv3 (RFC 5798);

3.4.69. Deve suportar BGPv4 de acordo com as seguintes RFCs:

3.4.69.1. RFC 4271, Border Gateway Protocol 4;

3.4.69.2. RFC 5065, Autonomous System Confederations for BGP;

3.4.69.3. RFC 4456, BGP Route Reflection;

3.4.69.4. RFC 1997, BGP Communities Attribute;

3.4.69.5. RFC 1745, BGP4/IDRP for IP-OSPF Interaction;

3.4.69.6. RFC 2439, BGP Route Flap Damping;

3.4.69.7. RFC 5492, Capabilities Advertisement with BGP-4;

3.4.69.8. RFC 2918, Route Refresh Capability for BGP-4;

3.4.69.9. RFC 4360, BGP Extended Communities Attribute;

3.4.69.10. RFC 4760, Multiprotocol Extensions for BGP4;

3.4.69.11. RFC 4724, Graceful Restart Mechanism for BGP;

3.4.69.12. RFC 6793, BGP Support for four-octet AS number space;

3.4.70. Deve implementar Dual Stack, ou seja, IPv6 e IPv4, com suporte as seguintes funcionalidades/RFCs:

3.4.70.1. RFC 1981, Path MTU Discovery for IPv6, August 1996 - Host Requirements;

3.4.70.2. RFC 5095, Internet Protocol, Version 6 (IPv6) Specification;

3.4.70.3. RFC 4861, Neighbor Discovery for IP Version 6, (IPv6);

3.4.70.4. RFC 2462, IPv6 Stateless Address Auto configuration - Host Requirements;

3.4.70.5. RFC 2463, Internet Control Message Protocol (ICMPv6) for the IPv6 Specification;

3.4.70.6. RFC 2464, Transmission of IPv6 Packets over Ethernet Networks;

3.4.70.7. RFC 2465, IPv6 MIB, General Group and Textual Conventions;

3.4.70.8. RFC 2466, MIB for ICMPv6;

3.4.70.9. RFC 3513, Internet Protocol Version 6 (IPv6) Addressing Architecture;

3.4.70.10. RFC 3587, Global Unicast Address Format;

3.4.71. Implementar os seguintes protocolos em IPv6: Ping, Traceroute, Telnet, SSHv2, SNMP, Syslog, SNTP e DNS;

3.4.72. Deve implementar IPv6 de acordo com as seguintes RFCs:

3.4.72.1. RFC 1981, Path MTU Discovery for IPv6, August 1996 - Router Requirements;

3.4.72.2. RFC 2462, IPv6 Stateless Address Auto configuration - Router Requirements;

3.4.72.3. RFC 2080, RIPng;

3.4.72.4. RFC 2462, IPv6 Stateless Address Auto configuration - Router Requirements;

3.4.72.5. RFC 2710, IPv6 Multicast Listener Discovery v1 (MLDv1) Protocol;

3.4.72.6. RFC 3810, IPv6 Multicast Listener Discovery v2 (MLDv2) Protocol;

3.4.72.7. RFC 6106, IPv6 Router Advertisement Options for DNS Configuration;

3.4.73. Suportar OSPFv3 conforme a RFC 5340;

3.4.74. Suportar OSPFv3 Graceful Restart conforme RFC 5187;

3.4.75. Suportar IS-IS, de acordo com as seguintes RFCs:

3.4.75.1. RFC 1195, Use of OSI IS-IS for Routing in TCP/IP and Dual Environments (TCP/IP transport only);

3.4.75.2. RFC 2763, Dynamic Hostname Exchange Mechanism for IS-IS;

3.4.75.3. RFC 2966, Domain-wide Prefix Distribution with Two-Level IS-IS;

3.4.75.4. RFC 2973, IS-IS Mesh Groups;

3.4.75.5. Draft-ietf-isis-restart-02, Restart Signaling for IS-IS;

3.4.75.6. Draft-ietf-isis-ipv6-06, Routing IPv6 with IS-IS;

3.4.75.7. Draft-ietf-isis-wg-multi-topology-11, Multi Topology (MT) Routing in IS-IS;

3.4.76. Implementar upload e download de configuração em formato ASCII ou XML, permitindo a edição do arquivo de configuração e, posteriormente, o download do arquivo editado para o equipamento;

3.4.77. Implementar TACACS+ segundo a RFC 1492;

3.4.78. Implementar autenticação RADIUS com suporte a:

3.4.79. RFC 2865 RADIUS Authentication;

3.4.80. RFC 2866 RADIUS Accounting;

3.4.81. RFC 3579 RADIUS EAP support for 802.1X;

3.4.82. A implementação de RADIUS deve suportar alteração dinâmica de parâmetros de autorização de uma sessão que já esteja ativa;

3.4.83. A implementação de RADIUS e TACACS+ deve estar disponível para autenticação de usuários via Telnet e Console serial;

3.4.84. Implementar per-command authorization para RADIUS e TACACS+;

3.4.85. Possuir DNS Client para IPv4 segundo a RFC 1591 e DNS Client para IPv6;

3.4.86. Possuir Telnet client and server segundo a RFC 854;

3.4.87. Implementar os seguintes grupos de RMON através da RFC 1757: History, Statistics, Alarms e Events;

3.4.88. Deve implementar RMON2-probe configuration segundo a RFC 2021, podendo ser implementada internamente no switch ou externamente, por meio de probe em hardware utilizando uma porta 1000BaseTX;

3.4.89. Implementar sFlow ou Netflow, em hardware;

3.4.90. Implementar a atualização de imagens de software e configuração através de um servidor TFTP;

3.4.91. Suportar múltiplos servidores Syslog;

3.4.92. Implementar ajuste de clock do equipamento utilizando NTP com autenticação MD5 e SNTP;

3.4.93. Implementar Port Mirroring, permitindo espelhar até 128 portas físicas ou 16 VLANs para até 16 portas de destino (portas de análise). Deve ser possível configurar mais de uma sessão de espelhamento simultânea;

3.4.94. Implementar RSPAN (Remote Mirroring), permitindo espelhar o tráfego de uma porta ou VLAN de um switch remoto para uma porta de um switch local (porta de análise);

3.4.95. Implementar gerenciamento através de SNMPv1 (RFC 1157), v2c (RFCs 1901 a 1908), v3 (RFCs 3410 a 3415) e SNMP para IPv6;

3.4.96. Implementar SMON de acordo com a RFC 2613;

3.4.97. Implementar cliente e servidor SSHv2;

3.4.98. Implementar cliente e servidor SCP e servidor SFTP;

3.4.99. Implementar gerenciamento via web com suporte a HTTP e HTTPS/SSL, permitindo visualização gráfica da utilização (em percentual, bytes e pacotes) das portas;

3.4.100. A interface gráfica deve permitir visualização de informações do sistema (VLAN, Portas, Fonte e Fans), monitoramento de Log, utilização de portas, QoS e configuração de portas, VLANs e ACLs;

3.4.101. O equipamento ofertado deve possuir um sistema operacional modular;

3.4.102. O sistema operacional deve possuir função grep/pipe para filtrar a saída de determinado comando;

3.4.103. O sistema operacional deve possuir comandos para visualização e monitoração de cada processo, sendo possível verificar por processo qual o consumo de cpu, process-id e qual o consumo de memória por processo;

3.4.104. O sistema operacional deve possuir comandos para que processos sejam terminados ou reiniciados sem que seja necessário a reinicialização do equipamento. Esta funcionalidade deve estar disponível pelo menos para Telnet, TFTP, HTTP e LLDP na versão atual;

3.4.105. O sistema operacional deve possuir comandos para que processos sejam terminados ou reiniciados sem que seja necessário a reinicialização do equipamento. Esta funcionalidade deve estar disponível pelo menos para Telnet, TFTP, HTTP, LLDP, OSPF e BGP na versão atual;

3.4.106. Implementar linguagem de scripting baseada em Python, permitindo a automatização de tarefas. A linguagem deve implementar estruturas de controle como loops e execução condicional e permitir a definição de variáveis;

3.4.107. Implementar protocolo de monitoramento de status de comunicação entre dois switches, que possibilite que uma porta seja desabilitada caso seja detectada uma falha de comunicação entre os dois peers;

3.4.108. Implementar funcionalidade que permita sua auto-configuração através dos protocolos DHCP e TFTP, permitindo o provisionamento em massa com o mínimo de intervenção humana;

3.4.109. Deve disponibilizar API (Aplication Programming Interface) aberta para integração com aplicações;

3.4.110. Implementar Rate limiting de entrada em todas as portas. A granularidade deve ser configurável

em intervalos de 64Kbps para portas de até 1Gbps. Caso o equipamento ofertado possua suporte a portas 10Gbps, a granularidade para este tipo de interface deve ser configurável em intervalos de 1Mbps. A implementação de Rate Limiting deve permitir a classificação do tráfego utilizando-se ACLs e parâmetros, MAC origem e destino (simultaneamente) IP origem e destino (simultaneamente), portas TCP, portas UDP e campo 802.1p;

3.4.111. Implementar Rate Shaping de saída em todas as portas. A granularidade deve ser configurável em intervalos de 64Kbps para portas de até 1Gbps. Caso o equipamento ofertado possua suporte a portas 10Gbps, a granularidade para este tipo de interface deve ser configurável em intervalos de 1Mbps;

3.4.112. A funcionalidade de Rate Shaping deve permitir a configuração de CIR (Commited Rate), banda máxima, banda mínima e peak rate;

3.4.113. Implementar a leitura, classificação e remarcação de QoS (802.1p e DSCP);

3.4.114. Implementar remarcação de prioridade de pacotes Layer 3, remarcando o campo DiffServ para grupos de tráfego classificados segundo portas TCP e UDP, endereço/subrede IP, VLAN e MAC origem e destino;

3.4.115. Implementar 8 filas de prioridade em hardware por porta;

3.4.116. Implementar os algoritmos de gerenciamento de filas WRR (Weighted Round Robin), WDRR (Weighted Deficit Round Robin) e SP (Strict Priority);

3.4.117. Deve implementar, ao menos dois dos algoritimos acima, simultaneamente em uma mesma porta;

3.4.118. Implementar as seguintes RFCs:

3.4.118.1. RFC 2474 DiffServ Precedence;

3.4.118.2. RFC 2598 DiffServ Expedited Forwarding (EF);

3.4.118.3. RFC 2597 DiffServ Assured Forwarding (AF);

3.4.118.4. RFC 2475 DiffServ Core and Edge Router Functions;

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

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

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

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

3.4.122. Implementar Gratuitous ARP Protection;

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

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

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

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

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

3.4.128. Implementar múltiplos suplicantes por porta, onde cada dispositivo deve ser autenticado de forma

independente, podendo ser encaminhados a VLANs distintas. As múltiplas autenticações devem ser realizadas através de IEEE 802.1x;

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

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

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

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

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

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

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

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

3.4.137. Implementar Policy Based Switching, ou seja, possibilitar que o tráfego classificado por uma ACL seja redirecionado para uma porta física específica;

3.4.138. Implementar funcionalidade que permita o mapeamento de usuários identificados via Kerberos (com a credencial de usuário no domínio), IEEE 802.1x e LLDP, provendo informações como endereço MAC, VLAN e porta física. Estas informações devem estar disponíveis na linha de comando (CLI) do equipamento;

3.4.139. O equipamento ofertado deve permitir que o mesmo faça parte de uma malha ethernet (Fabric Ethernet) descrito nos switches tipo distribuição com as seguintes funcionalidades:

3.4.140. O equipamento ofertado deve permitir a configuração como elemento anexo à malha ethernet;

3.4.141. O equipamento ofertado deve permitir a criação de VLANS mapeadas a serviços virtuais de rede, de que forma os serviços sejam criados automaticamente no elemento de borda da malha e propagados de maneira automática nos demais equipamentos que compõem a malha ethernet;

3.4.142. Deve permitir o gerenciamento do equipamento através de software de gerência do Fabric;

3.4.143. Deve possuir garantia do fabricante ou da revenda, desde que essa seja autorizada por carta pelo fabricante dos equipamentos a prestar o suporte e garantia, pelo período de 60 meses;

3.4.144. Marca/Modelo/Séries de Referencia: Extreme Networks 5320, Alcatel Lucent 6860E, Ruckus 7450, Juniper EX3400, Cisco 9300 e Aruba 6200.

3.5. Switch de Acesso Tipo V

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

3.5.2. A solução deve ser composta de um único equipamento, montável em rack 19” devendo este vir acompanhado dos devidos acessórios para tal e possuir altura máxima de 1RU;

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

3.5.4. Possuir LEDS indicativos de funcionamento da fonte de alimentação e status das portas;

3.5.5. Deve possuir homologação ANATEL, de acordo com a resolução vigente;

3.5.6. Deve possuir pelo menos 48 portas 10/100/1000BASE-T;

3.5.7. Deve possuir pelo menos 04 portas 10GBASE-X baseadas em SFP+;

3.5.8. Deve possuir uma porta USB ou micro-USB para transferência de arquivos;

3.5.9. Possuir uma porta console com conector RJ-45 ou DB9 macho;

3.5.10. Todas as interfaces Gigabit Ethernet solicitadas neste termo de referência devem funcionar simultaneamente;

3.5.11. Todas as interfaces ofertadas devem ser non-blocking;

3.5.12. Deve possuir detecção automática MDI/MDIX em todas as portas 10/100/1000BASE-T;

3.5.13. Deve possuir capacidade de processamento de pelo menos 256Gbps;

3.5.14. Deve possuir capacidade de encaminhamento de pelo menos 190Mpps;

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

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

3.5.17. O equipamento deve suportar o agrupamento lógico (gerência por um único IP) de unidades remotamente instaladas;

3.5.18. O empilhamento deve possuir velocidade de pelo menos 20Gbps cada (ou 10Gbps Full Duplex), totalizando 40 Gbps (ou 20 Gbps full-duplex). Este empilhamento poderá ser feito através de portas SFP+, X2, XENPAK ou XFP, sendo essas portas adicionais às solicitadas anteriormente;

3.5.19. O empilhamento deve possuir arquitetura de anel para prover resiliência.;

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

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

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

3.5.23. Deve armazenar, no mínimo, 32.000 (trinta e dois mil) endereços MAC;

3.5.24. Implementar, no mínimo, 4.000 (quatro mil) regras de ACL de entrada (ingress ACLs);

3.5.25. Implementar, no mínimo, 500 (quinhentas mil) regras de ACL de saída (egress ACLs);

3.5.26. Implementar 4000 VLANs por porta, ativas simultaneamente, através do protocolo 802.1Q;

3.5.27. Implementar agregação de links conforme padrão IEEE 802.3ad com suporte a LACP;

3.5.28. Em conjunto com outro equipamento de mesmo modelo, deverá permitir que um switch conectado aos dois, tenha a possibilidade de agregação de links (IEEE 802.3ad) com suporte a LACP com os mesmos, de forma a simular a existência de apenas um único link lógico entre este equipamento e os dois switches do modelo aqui especificado (Multi-Chassis Trunking, por exemplo). O único link lógico entre as camadas deve eliminar convergência do Spanning Tree, possibilitando o tráfego simultâneo por mais de uma conexão;

3.5.29. Implementar Proxy-ARP (RFC 1027);

3.5.30. Implementar IGMP v1, v2 e v3 Snooping;

3.5.31. Implementar IGMPv1 (RFC 1112), IGMP v2 (RFC 2236) e IGMPv3 (RFC 3376);

3.5.32. Implementar MVR (Multicast VLAN Registration);

3.5.33. Implementar DHCP/Bootp relay configurável por VLAN para IPv4 e IPv6;

3.5.34. Implementar servidor DHCP interno que permita a configuração de um intervalo de endereços IP a serem atribuídos os clientes DHCP e possibilite ainda a atribuição de, no mínimo, default-gateway, servidor DNS e servidor WINS;

3.5.35. Implementar DHCP Option 82, de acordo com a RFC 3046, com identificação de porta e VLAN, configurável por VLAN;

3.5.36. Implementar DHCP Client para IPv4 e IPv6;

3.5.37. Implementar RFC 3021 - Using 31-Bit Prefixes on IPv4 Point-to-Point Links;

3.5.38. Implementar Spanning-Tree (IEEE 802.1d), Rapid Spanning Tree (IEEE 802.1w), Multiple Instance STP (802.1s) e PVST+;

3.5.39. Implementar a configuração de Multiple Spanning Tree Protocol, com suporte a, pelo menos, 32 domínios;

3.5.40. Implementar funcionalidade vinculada ao Spanning-tree onde é possível designar portas de acesso (por exemplo onde estações estão conectadas) que não sofram o processo de Listening-Learning, passando direto para o estado de Forwarding. No entanto, as portas configuradas com esta funcionalidade devem detectar loops na rede normalmente;

3.5.41. Implementar funcionalidade vinculada ao Spanning-tree que evite a eleição de outros switches da rede como Root;

3.5.42. Implementar funcionalidade vinculada ao Spanning-tree que permita desabilitar uma porta de acesso assim que a mesma receba uma BPDU;

3.5.43. Deverá permitir a criação, remoção, gerenciamento e distribuição de VLANs de forma dinâmica através de portas configuradas como tronco IEEE 802.1Q utilizando o protocolo MVRP segundo o padrão IEEE802.1ak;

3.5.44. Possibilitar a coleta de estatísticas de tráfego baseada em VLANs IEEE 802.1Q e double-tagged VLANs IEEE 802.1ad;

3.5.45. Implementar MAC Based VLAN;

3.5.46. Implementar VLAN Translation;

3.5.47. Implementar Private VLANs;

3.5.48. Implementar Port Isolation ou funcionalidade que permita isolamento de portas específicas do switch. As portas isoladas não devem se comunicar entre si, porém podem se comunicar com qualquer outra porta no equipamento que não esteja isolada;

3.5.49. Implementar Private VLANs;

3.5.50. Implementar Port Isolation ou funcionalidade que permita isolamento de portas específicas do switch. As portas isoladas não devem se comunicar entre si, porém podem se comunicar com qualquer outra porta no equipamento que não esteja isolada;

3.5.51. Implementar IEEE 802.1ad com a possibilidade de associar CVIDs específicos para diferentes SVIDs (selective Q-in-Q ou 802.1ad CEP). A implementação deverá permitir a tradução do CVID;

3.5.52. Implementar IEEE 802.1ag (Connectivity Fault Management);

3.5.53. Implementar IEEE 802.3ah Ethernet OAM – Unidirectional Link Fault Management;

3.5.54. Implementar funcionalidade baseada na recomendação do ITU-T Y.1731 com medição de, no mínimo, Frame Delay;

3.5.55. Implementar o protocolo ITU-T G.8032 ERPS;

3.5.56. Implementar protocolo de resiliência em camada 2, específico para topologias em anel, que permita tempo de convergência inferior a 200 ms;

3.5.57. Implementar IEEE 802.1ab Link Layer Discovery Protocol (LLDP);

3.5.58. Implementar LLDP-MED (Media Endpoint Discovery);

3.5.59. Implementar os protocolos de roteamento IP: RFC 1058 – RIP v1 e RFC 2453 – RIP v2;

3.5.60. Suportar o protocolo de roteamento OSPFv2, incluindo autenticação MD5;

3.5.61. Suportar o protocolo de roteamento OSPFv2 (RFC 2328), incluindo autenticação MD5;

3.5.62. A implementação de OSPF deve estar de acordo com as seguintes RFCs:

3.5.62.1. RFC 1587 The OSPF NSSA Option;

3.5.62.2. RFC 1765 OSPF Database Overflow;

3.5.62.3. RFC 2370 The OSPF Opaque LSA Option;

3.5.62.4. RFC 3623 Graceful OSPF Restart;

3.5.63. Implementar PIM Snooping;

3.5.64. Suportar protocolo de multicast PIM-SM para IPv4 e IPv6;

3.5.65. Suportar PIM-DM para IPv4 e IPv6;

3.5.66. Suportar PIM-SSM segundo a RFC 3569;

3.5.67. Suportar MSDP (Multicast Source Discovery Protocol), de acordo com a RFC 3618;

3.5.68. Suportar VRRPv3 (RFC 5798);

3.5.69. Deve suportar BGPv4 de acordo com as seguintes RFCs:

3.5.69.1. RFC 4271, Border Gateway Protocol 4;

3.5.69.2. RFC 5065, Autonomous System Confederations for BGP;

3.5.69.3. RFC 4456, BGP Route Reflection;

3.5.69.4. RFC 1997, BGP Communities Attribute;

3.5.69.5. RFC 1745, BGP4/IDRP for IP-OSPF Interaction;

3.5.69.6. RFC 2439, BGP Route Flap Damping;

3.5.69.7. RFC 5492, Capabilities Advertisement with BGP-4;

3.5.69.8. RFC 2918, Route Refresh Capability for BGP-4;

3.5.69.9. RFC 4360, BGP Extended Communities Attribute;

3.5.69.10. RFC 4760, Multiprotocol Extensions for BGP4;

3.5.69.11. RFC 4724, Graceful Restart Mechanism for BGP;

3.5.69.12. RFC 6793, BGP Support for four-octet AS number space;

3.5.70. Deve implementar Dual Stack, ou seja, IPv6 e IPv4, com suporte as seguintes funcionalidades/RFCs:

3.5.70.1. RFC 1981, Path MTU Discovery for IPv6, August 1996 - Host Requirements;

3.5.70.2. RFC 5095, Internet Protocol, Version 6 (IPv6) Specification;

3.5.70.3. RFC 4861, Neighbor Discovery for IP Version 6, (IPv6);

3.5.70.4. RFC 2462, IPv6 Stateless Address Auto configuration - Host Requirements;

3.5.70.5. RFC 2463, Internet Control Message Protocol (ICMPv6) for the IPv6 Specification;

3.5.70.6. RFC 2464, Transmission of IPv6 Packets over Ethernet Networks;

3.5.70.7. RFC 2465, IPv6 MIB, General Group and Textual Conventions;

3.5.70.8. RFC 2466, MIB for ICMPv6;

3.5.70.9. RFC 3513, Internet Protocol Version 6 (IPv6) Addressing Architecture;

3.5.70.10. RFC 3587, Global Unicast Address Format;

3.5.71. Implementar os seguintes protocolos em IPv6: Ping, Traceroute, Telnet, SSHv2, SNMP, Syslog, SNTP e DNS;

3.5.72. Deve implementar IPv6 de acordo com as seguintes RFCs:

3.5.72.1. RFC 1981, Path MTU Discovery for IPv6, August 1996 - Router Requirements;

3.5.72.2. RFC 2462, IPv6 Stateless Address Auto configuration - Router Requirements;

3.5.72.3. RFC 2080, RIPng;

3.5.72.4. RFC 2462, IPv6 Stateless Address Auto configuration - Router Requirements;

3.5.72.5. RFC 2710, IPv6 Multicast Listener Discovery v1 (MLDv1) Protocol;

3.5.72.6. RFC 3810, IPv6 Multicast Listener Discovery v2 (MLDv2) Protocol;

3.5.72.7. RFC 6106, IPv6 Router Advertisement Options for DNS Configuration;

3.5.73. Suportar OSPFv3 conforme a RFC 5340;

3.5.74. Suportar OSPFv3 Graceful Restart conforme RFC 5187;

3.5.75. Suportar IS-IS, de acordo com as seguintes RFCs:

3.5.75.1. RFC 1195, Use of OSI IS-IS for Routing in TCP/IP and Dual Environments (TCP/IP transport only);

3.5.75.2. RFC 2763, Dynamic Hostname Exchange Mechanism for IS-IS;

3.5.75.3. RFC 2966, Domain-wide Prefix Distribution with Two-Level IS-IS;

3.5.75.4. RFC 2973, IS-IS Mesh Groups;

3.5.75.5. Draft-ietf-isis-restart-02, Restart Signaling for IS-IS;

3.5.75.6. Draft-ietf-isis-ipv6-06, Routing IPv6 with IS-IS;

3.5.75.7. Draft-ietf-isis-wg-multi-topology-11, Multi Topology (MT) Routing in IS-IS;

3.5.76. Implementar upload e download de configuração em formato ASCII ou XML, permitindo a edição do arquivo de configuração e, posteriormente, o download do arquivo editado para o equipamento;

3.5.77. Implementar TACACS+ segundo a RFC 1492;

3.5.78. Implementar autenticação RADIUS com suporte a:

3.5.79. RFC 2865 RADIUS Authentication;

3.5.80. RFC 2866 RADIUS Accounting;

3.5.81. RFC 3579 RADIUS EAP support for 802.1X;

3.5.82. A implementação de RADIUS deve suportar alteração dinâmica de parâmetros de autorização de uma sessão que já esteja ativa;

3.5.83. A implementação de RADIUS e TACACS+ deve estar disponível para autenticação de usuários via Telnet e Console serial;

3.5.84. Implementar per-command authorization para RADIUS e TACACS+;

3.5.85. Possuir DNS Client para IPv4 segundo a RFC 1591 e DNS Client para IPv6;

3.5.86. Possuir Telnet client and server segundo a RFC 854;

3.5.87. Implementar os seguintes grupos de RMON através da RFC 1757: History, Statistics, Alarms e Events;

3.5.88. Deve implementar RMON2-probe configuration segundo a RFC 2021, podendo ser implementada internamente no switch ou externamente, por meio de probe em hardware utilizando uma porta 1000BaseTX;

3.5.89. Implementar sFlow ou Netflow, em hardware;

3.5.90. Implementar a atualização de imagens de software e configuração através de um servidor TFTP;

3.5.91. Suportar múltiplos servidores Syslog;

3.5.92. Implementar ajuste de clock do equipamento utilizando NTP com autenticação MD5 e SNTP;

3.5.93. Implementar Port Mirroring, permitindo espelhar até 128 portas físicas ou 16 VLANs para até 16 portas de destino (portas de análise). Deve ser possível configurar mais de uma sessão de espelhamento simultânea;

3.5.94. Implementar RSPAN (Remote Mirroring), permitindo espelhar o tráfego de uma porta ou VLAN de um switch remoto para uma porta de um switch local (porta de análise);

3.5.95. Implementar gerenciamento através de SNMPv1 (RFC 1157), v2c (RFCs 1901 a 1908), v3 (RFCs 3410 a 3415) e SNMP para IPv6;

3.5.96. Implementar SMON de acordo com a RFC 2613;

3.5.97. Implementar cliente e servidor SSHv2;

3.5.98. Implementar cliente e servidor SCP e servidor SFTP;

3.5.99. Implementar gerenciamento via web com suporte a HTTP e HTTPS/SSL, permitindo visualização gráfica da utilização (em percentual, bytes e pacotes) das portas;

3.5.100. A interface gráfica deve permitir visualização de informações do sistema (VLAN, Portas, Fonte e Fans), monitoramento de Log, utilização de portas, QoS e configuração de portas, VLANs e ACLs;

3.5.101. O equipamento ofertado deve possuir um sistema operacional modular;

3.5.102. O sistema operacional deve possuir função grep/pipe para filtrar a saída de determinado comando;

3.5.103. O sistema operacional deve possuir comandos para visualização e monitoração de cada processo, sendo possível verificar por processo qual o consumo de cpu, process-id e qual o consumo de memória por processo;

3.5.104. O sistema operacional deve possuir comandos para que processos sejam terminados ou reiniciados sem que seja necessário a reinicialização do equipamento. Esta funcionalidade deve estar disponível pelo menos para Telnet, TFTP, HTTP e LLDP na versão atual;

3.5.105. O sistema operacional deve possuir comandos para que processos sejam terminados ou reiniciados sem que seja necessário a reinicialização do equipamento. Esta funcionalidade deve estar disponível pelo menos para Telnet, TFTP, HTTP, LLDP, OSPF e BGP na versão atual;

3.5.106. Implementar linguagem de scripting baseada em Python, permitindo a automatização de tarefas. A linguagem deve implementar estruturas de controle como loops e execução condicional e permitir a definição de variáveis;

3.5.107. Implementar protocolo de monitoramento de status de comunicação entre dois switches, que possibilite que uma porta seja desabilitada caso seja detectada uma falha de comunicação entre os dois peers;

3.5.108. Implementar funcionalidade que permita sua auto-configuração através dos protocolos DHCP e TFTP, permitindo o provisionamento em massa com o mínimo de intervenção humana;

3.5.109. Deve disponibilizar API (Aplication Programming Interface) aberta para integração com aplicações;

3.5.110. Implementar Rate limiting de entrada em todas as portas. A granularidade deve ser configurável em intervalos de 64Kbps para portas de até 1Gbps. Caso o equipamento ofertado possua suporte a portas 10Gbps, a granularidade para este tipo de interface deve ser configurável em intervalos de 1Mbps. A implementação de Rate Limiting deve permitir a classificação do tráfego utilizando-se ACLs e parâmetros, MAC origem e destino (simultaneamente) IP origem e destino (simultaneamente), portas TCP, portas UDP e campo 802.1p;

3.5.111. Implementar Rate Shaping de saída em todas as portas. A granularidade deve ser configurável em intervalos de 64Kbps para portas de até 1Gbps. Caso o equipamento ofertado possua suporte a portas 10Gbps, a granularidade para este tipo de interface deve ser configurável em intervalos de 1Mbps;

3.5.112. A funcionalidade de Rate Shaping deve permitir a configuração de CIR (Commited Rate), banda máxima, banda mínima e peak rate;

3.5.113. Implementar a leitura, classificação e remarcação de QoS (802.1p e DSCP);

3.5.114. Implementar remarcação de prioridade de pacotes Layer 3, remarcando o campo DiffServ para grupos de tráfego classificados segundo portas TCP e UDP, endereço/subrede IP, VLAN e MAC origem e destino;

3.5.115. Implementar 8 filas de prioridade em hardware por porta;

3.5.116. Implementar os algoritmos de gerenciamento de filas WRR (Weighted Round Robin), WDRR (Weighted Deficit Round Robin) e SP (Strict Priority);

3.5.117. Deve implementar, ao menos dois dos algoritimos acima, simultaneamente em uma mesma porta;

3.5.118. Implementar as seguintes RFCs:

3.5.118.1. RFC 2474 DiffServ Precedence;

3.5.118.2. RFC 2598 DiffServ Expedited Forwarding (EF);

3.5.118.3. RFC 2597 DiffServ Assured Forwarding (AF);

3.5.118.4. RFC 2475 DiffServ Core and Edge Router Functions;

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

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

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

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

3.5.122. Implementar Gratuitous ARP Protection;

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

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

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

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

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

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

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

3.5.130. Implementar autenticação baseada em endereço MAC, através de RADIUS ou através da base

local do switch;

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

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

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

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

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

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

3.5.137. Implementar Policy Based Switching, ou seja, possibilitar que o tráfego classificado por uma ACL seja redirecionado para uma porta física específica;

3.5.138. Implementar funcionalidade que permita o mapeamento de usuários identificados via Kerberos (com a credencial de usuário no domínio), IEEE 802.1x e LLDP, provendo informações como endereço MAC, VLAN e porta física. Estas informações devem estar disponíveis na linha de comando (CLI) do equipamento;

3.5.139. O equipamento ofertado deve permitir que o mesmo faça parte de uma malha ethernet (Fabric Ethernet) descrito nos switches tipo distribuição com as seguintes funcionalidades:

3.5.140. O equipamento ofertado deve permitir a configuração como elemento anexo à malha ethernet;

3.5.141. O equipamento ofertado deve permitir a criação de VLANS mapeadas a serviços virtuais de rede, de que forma os serviços sejam criados automaticamente no elemento de borda da malha e propagados de maneira automática nos demais equipamentos que compõem a malha ethernet;

3.5.142. Deve permitir o gerenciamento do equipamento através de software de gerência do Fabric;

3.5.143. Deve possuir garantia do fabricante ou da revenda, desde que essa seja autorizada por carta pelo fabricante dos equipamentos a prestar o suporte e garantia, pelo período de 60 meses;

3.5.144. Marca/Modelo/Séries de Referencia: Extreme Networks 5320, Alcatel Lucent 6860E, Ruckus 7450, Juniper EX3400, Cisco 9300 e Aruba 6200.

3.6. Switch de Distribuição

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

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

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

3.6.4. Possuir fonte de alimentação AC redundante interna, hot-swappable;

3.6.5. Possuir, no mínimo, 1Tb de Switch Fabric;

3.6.6. Possuir capacidade de encaminhamentos de pacotes, de no mínimo 800 Mpps utilizando pacotes de 64 bytes;

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

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

3.6.9. Possuir 24 portas 1/10GBASE-X ativas simultaneamente, baseadas em SFP+, devendo um mesmo slot suportar interfaces 10 Gigabit Ethernet 10GBASE-SR, 10GBASE-LR, 10GBASE-ER e 10GBASE-ZR e interfaces 1 Gigabit Ethernet 1000BASE-SX, 1000BASE-LX E 1000BASE-ZX;

3.6.10. Não é permitida a utilização de conversores externos;

3.6.11. Possuir, no mínimo, 01 slot de expansão futura de portas;

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

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

3.6.14. O equipamento deve suportar o agrupamento lógico (gerência por um único IP) de unidades remotamente instaladas;

3.6.15. O empilhamento deve possuir 02 portas dedicadas com velocidade de pelo menos 40Gbps Full Duplex cada;

3.6.16. O empilhamento deve possuir arquitetura de anel para prover resiliência;

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

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

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

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

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

3.6.22. Devem ser fornecidos todos os cabo e interfaces para o devido empilhamento de pelo menos 01 (um) metro;

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

3.6.24. Todas as interfaces ofertadas devem ser non-blocking;

3.6.25. Possuir altura máxima de 1U;

3.6.26. Deve armazenar, no mínimo, 114.000 (cento e quatorze mil) endereços MAC;

3.6.27. Implementar agregação de links conforme padrão IEEE 802.3ad com, no mínimo, 128 grupos, sendo 8 links agregados por grupo;

3.6.28. Implementar, no mínimo, 8.000 (oito mil) regras de ACL de entrada (ingress ACLs);

3.6.29. Implementar, no mínimo, 1000 (mil) regras de ACL de saída (egress ACLs);

3.6.30. Possuir homologação da ANATEL, de acordo com a Resolução número 242;

3.6.31. Implementar agregação de links conforme padrão IEEE 802.3ad com suporte a LACP;

3.6.32. Em conjunto com outro equipamento de mesmo modelo, deverá permitir que um switch conectado aos dois, tenha a possibilidade de agregação de links (IEEE 802.3ad) com suporte a LACP com eles, de forma a simular a existência de apenas um único link lógico entre este equipamento e os dois switches do modelo aqui especificado (Multi-Chassis Trunking, por exemplo). O único link lógico entre as camadas deve eliminar convergência do Spanning Tree, possibilitando o tráfego simultâneo por mais de uma conexão;

3.6.33. Implementar jumbo frames em todas as portas ofertadas, com suporte a pacotes de até 9216 Bytes;

3.6.34. Implementar Proxy-ARP (RFC 1027);

3.6.35. Implementar IGMP v1, v2 e v3 Snooping;

3.6.36. Implementar IGMPv1 (RFC 1112), IGMP v2 (RFC 2236) e IGMPv3 (RFC 3376);

3.6.37. Implementar MVR (Multicast VLAN Registration);

3.6.38. Implementar DHCP/Bootp relay configurável por VLAN para IPv4 e IPv6;

3.6.39. Implementar servidor DHCP interno que permita a configuração de um intervalo de endereços IP a serem atribuídos os clientes DHCP e possibilite ainda a atribuição de, no mínimo, defaultgateway, servidor DNS e servidor WINS;

3.6.40. Implementar DHCP Option 82, de acordo com a RFC 3046, com identificação de porta e VLAN, configurável por VLAN;

3.6.41. Implementar DHCP Client para IPv4 e IPv6;

3.6.42. Implementar RFC 3021 - Using 31-Bit Prefixes on IPv4 Point-to-Point Links;

3.6.43. Implementar Spanning-Tree (IEEE 802.1d), Rapid Spanning Tree (IEEE 802.1w), Multiple Instance STP (802.1s) e PVST+;

3.6.44. Implementar a configuração de Multiple Spanning Tree Protocol, com suporte a, pelo menos, 32 domínios;

3.6.45. Implementar funcionalidade vinculada ao Spanning-tree onde é possível designar portas de acesso (por exemplo onde estações estão conectadas) que não sofram o processo de Listening Learning, passando direto para o estado de Forwarding. No entanto, as portas configuradas com esta funcionalidade devem detectar loops na rede normalmente;

3.6.46. Implementar funcionalidade vinculada ao Spanning-tree que evite a eleição de outros switches da rede como Root;

3.6.47. Implementar funcionalidade vinculada ao Spanning-tree que permita desabilitar uma porta de acesso assim que ela receba uma BPDU;

3.6.48. Implementar 4000 VLANs por porta, ativas simultaneamente, através do protocolo 802.1Q;

3.6.49. Deverá permitir a criação, remoção, gerenciamento e distribuição de VLANs de forma dinâmica através de portas configuradas como tronco IEEE 802.1Q utilizando o protocolo MVRP segundo o padrão IEEE802.1ak;

3.6.50. Possibilitar a coleta de estatísticas de tráfego baseada em VLANs IEEE 802.1Q e double-tagged VLANs IEEE 802.1ad;

3.6.51. Implementar MAC Based VLAN;

3.6.52. Implementar VLAN Translation;

3.6.53. Suportar VLAN Aggregation ou funcionalidade que permita o compartilhamento de uma mesma subnet e de um mesmo endereço IPv4 utilizado como default-gateway por hosts de diferentes VLANs;

3.6.54. Implementar Private VLANs;

3.6.55. Implementar Port Isolation ou funcionalidade que permita isolamento de portas específicas do switch. As portas isoladas não devem se comunicar entre si, porém podem se comunicar com qualquer outra porta no equipamento que não esteja isolada;

3.6.56. Implementar IEEE 802.1ad com a possibilidade de associar CVIDs específicos para diferentes SVIDs (selective Q-in-Q ou 802.1ad CEP);

3.6.57. Implementar IEEE 802.1ag (Connectivity Fault Management);

3.6.58. Implementar funcionalidade baseada na recomendação do ITU-T Y.1731 com medição de, no mínimo, Frame Delay;

3.6.59. Implementar o protocolo ITU-T G.8032 ERPS;

3.6.60. Implementar protocolo de resiliência em camada 2, específico para topologias em anel, que permita tempo de convergência inferior a 200 m;

3.6.61. Implementar IEEE 802.1ab Link Layer Discovery Protocol (LLDP);

3.6.62. Implementar LLDP-MED (Media Endpoint Discovery);

3.6.63. Implementar, no mínimo, 2000 interfaces IP (IPv4 ou IPv6);

3.6.64. Implementar os protocolos de roteamento IP: RFC 1058 – RIP v1 e RFC 2453 – RIP v2;

3.6.65. Suportar o protocolo de roteamento OSPFv2 (RFC 2328), incluindo autenticação MD5;

3.6.66. Implementar PIM Snooping;

3.6.67. Suportar protocolo de multicast PIM-SM para IPv4 e IPv6;

3.6.68. Suportar PIM-SSM segundo a RFC 3569;

3.6.69. Suportar VRRPv3 (RFC 5798);

3.6.70. Deve implementar Dual Stack, ou seja, IPv6 e IPv4, com suporte as seguintes funcionalidades/RFCs:

3.6.71. RFC 1981, Path MTU Discovery for IPv6, August 1996 - Host Requirements;

3.6.72. RFC 5095, Internet Protocol, Version 6 (IPv6) Specification;

3.6.73. RFC 4861, Neighbor Discovery for IP Version 6, (IPv6);

3.6.74. RFC 2462, IPv6 Stateless Address Auto configuration - Host Requirements;

3.6.75. RFC 2463, Internet Control Message Protocol (ICMPv6) for the IPv6 Specification;

3.6.76. RFC 2464, Transmission of IPv6 Packets over Ethernet Networks;

3.6.77. RFC 2465, IPv6 MIB, General Group and Textual Conventions;

3.6.78. RFC 2466, MIB for ICMPv6;

3.6.79. RFC 3513, Internet Protocol Version 6 (IPv6) Addressing Architecture;

3.6.80. RFC 3587, Global Unicast Address Format;

3.6.81. Implementar os seguintes protocolos em IPv6: Ping, Traceroute, Telnet, SSHv2, SNMP, Syslog, SNTP e DNS;

3.6.82. Deve implementar IPv6 de acordo com as seguintes RFCs:

3.6.83. RFC 1981, Path MTU Discovery for IPv6, August 1996 - Router Requirements;

3.6.84. RFC 2462, IPv6 Stateless Address Auto configuration - Router Requirements;

3.6.85. RFC 2080, RIPng;

3.6.86. RFC 2462, IPv6 Stateless Address Auto configuration - Router Requirements;

3.6.87. RFC 2710, IPv6 Multicast Listener Discovery v1 (MLDv1) Protocol;

3.6.88. RFC 3810, IPv6 Multicast Listener Discovery v2 (MLDv2) Protocol;

3.6.89. RFC 6106, IPv6 Router Advertisement Options for DNS Configuration;

3.6.90. Suportar OSPFv3 conforme a RFC 5340;

3.6.91. Suportar OSPFv3 Graceful Restart conforme RFC 5187;

3.6.92. Implementar BFD (Bidirectional Forwarding Detection);

3.6.93. Implementar Policy Based Routing;

3.6.94. Implementar upload e download de configuração em formato ASCII ou XML, permitindo a edição do arquivo de configuração e, posteriormente, o download do arquivo editado para o equipamento;

3.6.95. Implementar TACACS+ segundo a RFC 1492;

3.6.96. Implementar autenticação RADIUS com suporte a:

3.6.97. RFC 2865 RADIUS Authentication;

3.6.98. RFC 2866 RADIUS Accounting;

3.6.99. RFC 3579 RADIUS EAP support for 802.1X;

3.6.100. A implementação de RADIUS deve suportar alteração dinâmica de parâmetros de autorização de uma sessão que já esteja ativa;

3.6.101. A implementação de RADIUS e TACACS+ deve estar disponível para autenticação de usuários via Telnet e Console serial;

3.6.102. Implementar per-command authorization para RADIUS e TACACS+;

3.6.103. Possuir DNS Client para IPv4 segundo a RFC 1591 e DNS Client para IPv6;

3.6.104. Possuir Telnet client and server segundo a RFC 854;

3.6.105. Implementar os seguintes grupos de RMON através da RFC 1757: History, Statistics, Alarms e Events;

3.6.106. Deve implementar RMON2-probe configuration segundo a RFC 2021, podendo ser implementada internamente no switch ou externamente, por meio de probe em hardware utilizando uma porta 1000BaseTX;

3.6.107. Implementar sFlow ou Netflow, em hardware;

3.6.108. Implementar a atualização de imagens de software e configuração através de um servidor TFTP;

3.6.109. Suportar múltiplos servidores Syslog;

3.6.110. Implementar ajuste de clock do equipamento utilizando NTP com autenticação MD5 e SNTP;

3.6.111. Implementar Port Mirroring, permitindo espelhar até 128 portas físicas ou 16 VLANs para até 16 portas de destino (portas de análise). Deve ser possível configurar mais de uma sessão de espelhamento simultânea;

3.6.112. Implementar RSPAN (Remote Mirroring), permitindo espelhar o tráfego de uma porta ou VLAN de um switch remoto para uma porta de um switch local (porta de análise);

3.6.113. Implementar gerenciamento através de SNMPv1 (RFC 1157), v2c (RFCs 1901 a 1908), v3 (RFCs 3410 a 3415) e SNMP para IPv6;

3.6.114. Implementar SMON de acordo com a RFC 2613;

3.6.115. Implementar cliente e servidor SSHv2;

3.6.116. Implementar cliente e servidor SCP e servidor SFTP;

3.6.117. Implementar gerenciamento via web com suporte a HTTP e HTTPS/SSL, permitindo visualização gráfica da utilização (em percentual, bytes e pacotes) das portas;

3.6.118. A interface gráfica deve permitir visualização de informações do sistema (VLAN, Portas, Fonte e Fans), monitoramento de Log, utilização de portas, QoS e configuração de portas, VLANs e ACLs;

3.6.119. O equipamento ofertado deve possuir um sistema operacional modular;

3.6.120. O sistema operacional deve possuir função grep/pipe para filtrar a saída de determinado comando;

3.6.121. O sistema operacional deve possuir comandos para visualização e monitoração de cada processo, sendo possível verificar por processo qual o consumo de cpu, process-id e qual o consumo de memória por processo;

3.6.122. O sistema operacional deve possuir comandos para que processos sejam terminados ou reiniciados sem que seja necessário a reinicialização do equipamento. Esta funcionalidade deve estar disponível pelo menos para Telnet, TFTP, HTTP e LLDP na versão atual;

3.6.123. Implementar linguagem de scripting baseada em Python, permitindo a automatização de tarefas.

A linguagem deve implementar estruturas de controle como loops e execução condicional e permitir a definição de variáveis;

3.6.124. Implementar protocolo de monitoramento de status de comunicação entre dois switches, que possibilite que uma porta seja desabilitada caso seja detectada uma falha de comunicação entre os dois peers;

3.6.125. Implementar funcionalidade que permita sua autoconfiguração através dos protocolos DHCP e TFTP, permitindo o provisionamento em massa com o mínimo de intervenção humana;

3.6.126. Deve disponibilizar API (Aplication Programming Interface) aberta para integração com aplicações;

3.6.127. Implementar Rate limiting de entrada em todas as portas. A granularidade deve ser configurável em intervalos de 64Kbps para portas de até 1Gbps. Caso o equipamento ofertado possua suporte a portas 10Gbps, a granularidade para este tipo de interface deve ser configurável em intervalos de 1Mbps. A implementação de Rate Limiting deve permitir a classificação do tráfego utilizando-se ACLs e parâmetros, MAC origem e destino (simultaneamente) IP origem e destino (simultaneamente), portas TCP, portas UDP e campo 802.1p;

3.6.128. Implementar Rate Shaping de saída em todas as portas. A granularidade deve ser configurávelem intervalos de 64Kbps para portas de até 1Gbps. Caso o equipamento ofertado possua suporte a portas 10Gbps, a granularidade para este tipo de interface deve ser configurável em intervalos de 1Mbps;

3.6.129. A funcionalidade de Rate Shaping deve permitir a configuração de CIR (Commited Rate), banda máxima, banda mínima e peak rate;

3.6.130. Implementar a leitura, classificação e remarcação de QoS (802.1p e DSCP);

3.6.131. Implementar remarcação de prioridade de pacotes Layer 3, remarcando o campo DiffServ para grupos de tráfego classificados segundo portas TCP e UDP, endereço/subrede IP, VLAN e MAC origem e destino;

3.6.132. Implementar 8 filas de prioridade em hardware por porta;

3.6.133. Implementar os algoritmos de gerenciamento de filas WRR (Weighted Round Robin), WDRR (Weighted Deficit Round Robin) e SP (Strict Priority);

3.6.134. Deve implementar, ao menos dois dos algoritmos acima, simultaneamente em uma mesma porta;

3.6.135. Implementar as seguintes RFCs:

3.6.136. RFC 2474 DiffServ Precedence;

3.6.137. RFC 2598 DiffServ Expedited Forwarding (EF);

3.6.138. RFC 2597 DiffServ Assured Forwarding (AF);

3.6.139. RFC 2475 DiffServ Core and Edge Router Functions;

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

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

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

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

3.6.144. Implementar Gratuitous ARP Protection;

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

3.6.146. Implementar limitação de número de endereços MAC aprendidos por uma porta, para uma

determinada VLAN;

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

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

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

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

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

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

3.6.153. Implementar ACLs de entrada (ingress ACLs) em hardware, baseadas em critérios da camada 2 (MAC origem e destino e campo 802.1p), camada 3 (IP origem e destino) e camada 4 (portas TCP e UDP), em todas as interfaces e VLANs, com suporte a endereços IPv6. As ACLs devem ser configuradas para permitir, negar, aplicar QoS, espelhar o tráfego para uma porta de análise, criar entrada de log e incrementar contador;

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

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

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

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

3.6.158. Implementar Policy Based Switching, ou seja, possibilitar que o tráfego classificado por uma ACL seja redirecionado para uma porta física específica;

3.6.159. Implementar funcionalidade que permita o mapeamento de usuários identificados via Kerberos (com a credencial de usuário no domínio), IEEE 802.1x e LLDP, provendo informações como endereço MAC, VLAN e porta física. Estas informações devem estar disponíveis na linha de comando (CLI) do equipamento;

3.6.160. Suportar protocolo OpenFlow versão 1.0;

3.6.161. Deve permitir automação e escalabilidade de rede utilizando protocolo de malha ethernet (fabric ethernet) baseado em TRILL, SPB ou similar;

3.6.162. A malha ethernet deve implementar, nativamente no equipamento ou via software de gerência externo, mecanismo para estabelecimento de serviços virtualizados de redes lógicas em camada 2 e suportar em camada 3 através de aplicação de licenciamento adicional, de qualquer ponto da malha ethernet para qualquer outro ponto da malha ethernet, sem necessidade de configuração manual dos equipamentos intermediários entre os pontos que terão os serviços configurados;

3.6.163. A malha ethernet deve suportar criação de serviços virtualizados em camada 3, segmentados por VRF, em que um serviço virtualizado não deverá se comunicar com outro. Deve possuir, ainda, mecanismo para permitir que uma VRF se comunique com outra na malha ethernet para os casos em que a

comunicação entre essas seja necessária;

3.6.164. A malha ethernet deve implementar mecanismo para tratamento de tráfego Multicast de forma inteligente, permitindo controle de multicast mesmo dentro de serviços virtualizados da malha ethernet, evitando assim flooding desnecessário para portas que não fazem parte de um mesmo grupo multicast;

3.6.165. Deve suportar o estabelecimento de caminhos de serviços virtualizados em camada 2 e camada 3;

3.6.166. A malha ethernet deve ser agnóstica à topologia física;

3.6.167. A malha ethernet deve permitir escalabilidade de, no mínimo, 100 (cem) equipamentos;

3.6.168. A malha ethernet deve permitir a adição de equipamentos do tipo FFF (Fixed Form Factor) e equipamentos do tipo chassi;

3.6.169. A malha ethernet deverá permitir alta disponibilidade em caso de falhas de links e deverá permitir a utilização de todos os links da topologia sem gerar loops;

3.6.170. Deve possuir garantia do fabricante ou da revenda, desde que essa seja autorizada por carta pelo fabricante dos equipamentos a prestar o suporte e garantia, pelo período de 60 meses;

3.6.171. Marca/Modelo/Séries de Referencia: Extreme Networks 5520, Alcatel Lucent 6860N, Ruckus 7550, Juniper EX4600, Cisco 9500 Aruba 6300M.

3.7. Transceiver 1000BASE-X

3.7.1. Todos os módulos descritos neste item devem ser do mesmo fabricante dos switches;

3.7.2. Transceiver padrão SFP 1000BASE-SX que opere em fibra multimodo (MMF) de 850nm;

3.7.3. Deverá suportar distâncias de transmissão nominais de no mínimo 220m;

3.7.4. Deve ter a capacidade de ser inserido e removido no módulo de forma online;

3.7.5. Deve possuir garantia do fabricante ou da revenda, desde que essa seja autorizada por carta pelo fabricante dos equipamentos a prestar o suporte e garantia, pelo período de 60 meses;

3.8. Transceiver 10GBASE-X

3.8.1. Todos os módulos descritos neste item devem ser do mesmo fabricante dos switches;

3.8.2. Transceiver padrão SFP+ 10GBASE que opere em fibra multimodo (MMF) de 850nm;

3.8.3. Deverá suportar distâncias de transmissão nominais de no mínimo 300m;

3.8.4. Deve ter a capacidade de ser inserido e removido no módulo de forma online;

3.8.5. Deve possuir garantia do fabricante ou da revenda, desde que essa seja autorizada por carta pelo fabricante dos equipamentos a prestar o suporte e garantia, pelo período de 60 meses;

3.9. Licenças Software de Gerência Centralizada - LAN

3.9.1. Características Gerais

3.9.1.1. A Solução de Gerência Centralizada (SGC) deve ser fornecida em formato local (on premises) ou em nuvem pública ou de forma híbrida com ambos trabalhando em conjunto. Em quaisquer das opções ofertadas, a solução deverá ser do mesmo fabricante dos pontos de acesso e switches e deverá seguir os seguintes requisitos:

3.9.1.2. Deve ser possível gerenciar todos os dispositivos com todas as funcionalidades descritas pelo período mínimo de 60 meses;

3.9.1.3. Em caso de componente de nuvem pública:

3.9.1.3.1. Deve ser fornecido na modalidade SaaS (Software as a Service) do próprio fabricante. Não será

permitida a utilização de softwares instalados em nuvem pública com intuito de atendimento desse termo de referência;

3.9.1.3.2. Deve apresentar disponibilidade mínima de 99,9%;

3.9.1.3.3. Deve permitir retenção de dados estatísticos de, no mínimo, 90 dias;

3.9.1.4. Em caso de componente de solução local (on premises), deverá ser fornecido em, pelo menos, um dos formatos abaixo:

3.9.1.4.1. Appliance físico (Hardware)

3.9.1.4.1.1. Deverá possuir hardware dedicado com software de gerenciamento e administração já embarcados;

3.9.1.4.1.2. Deverá possuir porta de console para gerenciamento e configuração via linha de comando CLI com conector RJ-45 ou Conector padrão RS-232 ou USB;

3.9.1.4.1.3. Deverá possuir, no mínimo 02 (duas) interfaces Ethernet 10Gbps SFP+;

3.9.1.4.1.4. Possuir fontes de alimentação redundantes com seleção automática de tensão (100-240V AC);

3.9.1.4.1.5. Permitir ser montado em rack padrão de 19 (dezenove) polegadas, incluindo todos os acessórios necessários e não consumir mais que 2 RU form factor;

3.9.1.4.1.6. Deve suportar temperatura de operação entre 0°C a 40°C;

3.9.1.4.1.7. Deve ser acompanhado de todos os acessórios necessários para operacionalização da solução, tais como: softwares, licenças, cabos de energia elétrica, documentações técnicas e manuais que contenham informações suficientes, que possibilite a instalação, configuração e operacionalização do equipamento;

3.9.1.4.1.8. Implementar redundância N+1 com sincronismo automático das configurações entre os appliances, onde a falha de um appliance não impacte nenhuma função descrita nesse termo de referência;

3.9.1.4.2. Appliance virtual

3.9.1.4.2.1. Para instalação deverá ser compatível com uma das seguintes plataformas:

3.9.1.4.2.1.1. Bare Metal ou Hypervisors:

3.9.1.4.2.1.2. Xen 4 ou superior;

3.9.1.4.2.1.3. Hyper-V 2012 R2 ou superior;

3.9.1.4.2.1.4. VMware vSphere ESXi 6 ou superior;

3.9.1.4.2.2. Deve ser acompanhado de todos os acessórios necessários para operacionalização da solução, tais como: softwares, licenças, documentações técnicas e manuais que contenham informações suficientes, que possibilite a instalação, configuração e operacionalização do equipamento;

3.9.1.4.3. Para atendimento desse termo de referência, será permitida a composição de softwares, desde que sejam do mesmo fabricante para atendimento de toda a especificação;

3.9.1.4.4. Deve suportar a centralização da configuração e monitoramento dos pontos de acesso e switches gerenciados;

3.9.1.4.5. Capacidade para gerenciar no mínimo 1.500 (mil e quinhentos) Pontos de Acesso e/ou Switches;

3.9.1.4.6. Deve ser fornecido licenciado nos termos desse edital para atender a quantidade total de Pontos de Acesso e Switches solicitada nesse termo de forma simultânea;

3.9.1.4.7. Deve permitir o acréscimo unitário de licenças para expansão da capacidade dos Pontos de Acesso e Switches ou cada Ponto de Acesso e Switch deve vir acompanhado de sua licença;

3.9.1.4.8. Deve permitir a portabilidade de licenças em caso de troca de equipamentos, permitindo utilizar a mesma licença de um ponto de acesso ou switch qualquer para outro ponto de acesso ou switch qualquer. Não deve haver vínculo de uma licença com um modelo de equipamento específico;

3.9.1.4.9. Deve possuir garantia, suporte, atualizações e troca de hardware com envio na modalidade NBD

por um período de 60 meses, independente da arquitetura adotada (hardware dedicado, computação virtual ou nuvem pública do fabricante dos pontos de acesso) para todos os itens que sejam fornecidos para compor a solução;

3.9.1.4.10. A SGC poderá estar diretamente e/ou remotamente conectado aos Pontos de Acesso e Switches por ele gerenciados, inclusive via roteamento nível 3 da camada OSI;

3.9.1.4.11. Implementar, no mínimo, dois níveis de acesso administrativo à SGC (apenas leitura e leitura/escrita) protegidos por senhas independentes;

3.9.1.4.12. Permitir a customização do acesso administrativo através de atribuição de grupo de função do usuário administrador;

3.9.1.4.13. Permitir a configuração e gerenciamento através de browser padrão (HTTPS) ou porta console;

3.9.1.4.14. Permitir que o processo de atualização de versão nos dispositivos gerenciados seja realizado através de browser padrão (HTTPS) ou SSH;

3.9.1.4.15. Possibilitar cópia “backup” da configuração, bem como a funcionalidade de restauração da configuração através de browser padrão (HTTPS) ou FTP ou TFTP;

3.9.2. Gerenciamento de Switches

3.9.2.1. Deve permitir fazer o aprovisionamento de switches a partir da sua configuração de fábrica, sem a necessidade de configuração inicial via CLI;

3.9.2.2. Deve permitir a criação de políticas ou modelos (templates) de configuração para aplicação a um grupo de switches;

3.9.2.3. Deve permitir que as configurações sejam aplicadas em vários switches simultaneamente;

3.9.2.4. Deve permitir que as configurações sejam aplicadas em apenas um switch pontualmente, sobrescrevendo a configuração da política ou modelo (template) de configuração;

3.9.2.5. Deve permitir que as configurações aplicadas em apenas um switch pontualmente possam ser revertidas para a configuração da política ou modelo (template) de configuração;

3.9.2.6. Deve permitir a criação e remoção de VLANs nos dispositivos e associação de portas às mesmas;

3.9.2.7. Deve permitir a configuração nos switches gerenciados de, no mínimo:

3.9.2.7.1.1. PoE;

3.9.2.7.1.2. LLDP;

3.9.2.7.1.3. SNMP;

3.9.2.7.1.4. NTP ou SNTP;

3.9.2.7.1.5. Syslog;

3.9.2.7.1.6. MTU ou Jumbo Frame;

3.9.2.7.1.7. IGMP Snooping;

3.9.2.7.1.8. STP, RSTP e MSTP;

3.9.2.8. Limitação de taxa de encaminhamento de broadcast e multicast, por porta do switch;

3.9.2.9. Deve permitir a criação de um script ou objeto com comandos de CLI customizados para os dispositivos gerenciados. Deve permitir a aplicação desse script ou objeto para um grupo de dispositivos gerenciados simultaneamente;

3.9.2.10. Deve permitir acessar os switches utilizando SSH, a partir de conexão com a nuvem;

3.9.2.11. Deve permitir desabilitar e habilitar as portas dos switches;

3.9.2.12. Deve permitir monitorar de forma história, com, no mínimo, 90 dias de retenção de dados, os seguintes parâmetros dos switches:

3.9.2.12.1. Utilização de CPU e memória RAM;

3.9.2.12.2. Consumo de dados enviados e recebidos, por porta;

3.9.2.13. Deve permitir visualizar e exportar inventário dos switches, contendo, no mínimo:

3.9.2.13.1. Modelo;

3.9.2.13.2. Número Serial;

3.9.2.13.3. Versão de Software;

3.9.2.13.4. Endereço MAC;

3.9.2.13.5. Endereço IP;

3.9.2.14. Deve permitir visualizar informações, por porta, contendo, no mínimo:

3.9.2.14.1. Status da porta;

3.9.2.14.2. VLANs configuradas;

3.9.2.14.3. Vizinho conectado via LLDP, CDP ou similar;

3.9.2.14.4. Tráfego enviado e recebido;

3.9.2.14.5. Potência PoE fornecida, caso o switch suporte PoE;

3.9.2.14.6. Velocidade da porta;

3.9.2.15. Deve possuir mapa de topologia que permita visualizar as conexões entre os pontos de acesso e switches gerenciados;

3.9.2.16. O mapa de topologia deve criar automaticamente os links entre os dispositivos de rede, através de protocolos de descobrimento como LLDP, CDP ou similar;

3.9.3. Gerenciamento sem Fio

3.9.3.1. Suportar, no mínimo, 20.000 (vinte mil) dispositivos conectados simultaneamente;

3.9.3.2. Deve permitir que as configurações sejam aplicadas em vários pontos de acesso selecionados simultaneamente, isto é, não será permitido soluções que necessitem configurar os pontos de acesso individualmente;

3.9.3.3. Permitir a configuração total dos pontos de acesso, assim como os aspectos de segurança da rede wireless (WLAN) e Rádio Frequência (RF);

3.9.3.4. Possibilitar a configuração de envio dos eventos dos Pontos de Acesso ou da SGC para um servidor de Syslog remoto;

3.9.3.5. Implementar, pelo menos, os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps SNMP;

3.9.3.6. Permitir a visualização de alertas da rede sem fio em tempo real;

3.9.3.7. Gerenciar de forma centralizada a autenticação de usuários na integração com servidores AAA (Radius);

3.9.3.8. Permitir o envio de alertas ou alarmes através do protocolo SMTP, sendo que a comunicação com o servidor deverá ser autenticada e cifrada (SMTP/TLS);

3.9.3.9. Deverá possuir a capacidade de importação de certificados digitais emitidos por uma autoridade certificadora externa;

3.9.3.10. Deverá implementar disponibilidade de SSID baseado em dia da semana/hora, permitindo ao administrador do sistema, habilitar ou não um determinado SSID somente em hora/dia da semana determinados;

3.9.3.11. Possuir ferramentas de debug e log de eventos para depuração e gerenciamento em primeiro nível (ping, trace e logs);

3.9.3.12. Possuir ferramenta que permita o monitoramento em tempo real de informações de utilização de CPU, memória e estatísticas de rede da SGC ou dos Pontos de Acesso;

3.9.3.13. Possuir a capacidade de armazenar múltiplos arquivos de configuração pertencente à rede wireless;

3.9.3.14. Monitorar o desempenho da rede wireless, permitindo a visualização de informações de cada ponto de acesso;

3.9.3.15. A falha de comunicação entre SGC e os Pontos de Acesso não devem interferir na operação dos Pontos de Acesso;

3.9.3.16. Deverá possuir a capacidade de geração de informações ou relatórios de no mínimo os seguintes tipos: Listagem de clientes Wireless, Listagem de Pontos de Acesso, utilização da rede;

3.9.3.17. Deverá suportar protocolo LLDP;

3.9.3.18. Deverá suportar a identificação de aplicações dos clientes conectados ao ponto de acesso;

3.9.3.19. Permitir visualizar a localização dos pontos de acesso e através desta obter o status de funcionamento dos mesmos;

3.9.3.20. Na ocorrência de inoperância de um Ponto de Acesso, a solução deverá ajustar automaticamente a potência dos Pontos de Acesso adjacentes, de modo a prover a cobertura da área não assistida;

3.9.3.21. Ajustar automaticamente a utilização de canais de modo a otimizar a cobertura de rede de acordo com as condições de RF;

3.9.3.22. Detectar interferência e ajustar parâmetros de RF, evitando problemas de cobertura de RF de forma automática;

3.9.3.23. O SGC deve possuir funcionalidade de analisador gráfico de espectro para detecção de interferências nas faixas de frequência de 2.4 e 5 GHz, sejam elas IEEE 802.11 ou não. Deve disponibilizar interface gráfica com, pelo menos, gráficos de Fast Fourier Transform (FFT) e espectrograma, caso a funcionalidade não possa ser apresentada pelo SGC, deve ser fornecido um equipamento ou software, do mesmo fabricante, que a faça;

3.9.3.24. Deve detectar interferências Wi-Fi (provenientes de dispositivos padrão IEEE802.11) e detectar e classificar no mínimo 3 (três) padrões de assinaturas de interferências não-Wi-Fi, com por exemplo, telefones sem fio, microondas, etc.;

3.9.3.25. Deve possuir ferramenta de localização e analíticos sobre localização que implemente:

3.9.3.25.1. Criação de zonas ou regiões de interesse dentro de plantas de uma determinada localidade;

3.9.3.25.2. Mapeamento de zonas ou regiões de interesse em categorias de engajamento;

3.9.3.25.3. Coleta de dados de presença e proximidade, reportando para uma determinada localidade, no mínimo, a quantidade de:

3.9.3.25.3.1. Visitantes internos engajados;

3.9.3.25.3.2. Passantes externos;

3.9.3.25.3.3. Novos visitantes;

3.9.3.25.3.4. Visitantes já vistos anteriormente;

3.9.3.25.4. Informações sobre fluxo ou trajeto entre categorias de engajamento diferentes;

3.9.3.25.5. Informações sobre aglomerações em determinadas categorias de engajamento;

3.9.3.25.6. Rastreamento de ativos baseados em beacons Bluetooth Low Energy e Wi-Fi;

3.9.3.25.7. Associação de ativos baseados em beacons Bluetooth Low Energy ou Wi-Fi a determinadas categorias de engajamento permitidas;

3.9.3.25.8. Alarmes caso um ativo baseado em beacons Bluetooth Low Energy ou Wi-Fi viole o confinamento de uma categoria de engajamento;

3.9.3.26. Exportação de dados para coletores externos, suportando integração com soluções de terceiros;

3.9.3.27. Deve possuir ferramenta integrada ao SGC de projeto da rede sem fio, que permita:

3.9.3.27.1. Importação de plantas baixas em pelo menos um dos formatos gráficos: dwg, dxf, dxb, dwf, jpg, gif, bmp e png dos locais de instalação;

3.9.3.27.2. Simulação da cobertura da rede sem fio, apresentando, no mínimo, RSSI, SNR e distribuição de canais;

3.9.3.27.3. Posicionamento automático e manual dos Pontos de Acesso, e os ajustes das características dos rádios destes APs;

3.9.3.27.4. Geração de relatórios com os mapas de cobertura projetados e lista dos dispositivos utilizados na simulação;

3.9.3.28. Deve possuir ferramenta integrada ao SGC para permitir ao administrador visualizar e monitorar o mapa de cobertura detalhado (heatmap) da rede sem fio;

3.9.3.29. Implementar sistema automático de balanceamento de carga para associação de clientes entre Pontos de Acesso próximos, para otimizar a performance;

3.9.3.30. Implementar funcionalidade de balanceamento de carga entre os rádios de um mesmo Ponto de Acesso;

3.9.3.31. Permitir que o serviço wireless seja desabilitado de determinado ponto de acesso. Também deve ser possível selecionar o serviço de qual rádio (banda) de determinado ponto de acesso deve ser desabilitado;

3.9.4. Rede

3.9.4.1. Deverá implementar suporte aos protocolos IPv4 e IPv6;

3.9.4.2. Deverá implementar tagging de VLANs através do protocolo 802.1Q;

3.9.4.3. Suportar a configuração de no mínimo 4000 (quatro mil) VLANs;

3.9.4.4. Deverá oferecer os recursos de mobilidade para roaming de camada L2 e L3;

3.9.4.5. Deverá implementar DHCP Relay e DHCP Server nos Pontos de Acesso;

3.9.4.6. Implementar associação dinâmica de usuário a VLAN com base nos parâmetros da etapa de autenticação via IEEE 802.1X;

3.9.4.7. Deverá permitir que clientes sejam designados para diferentes VLANs dentro de um mesmo SSID;

3.9.4.8. Em caso de falha de comunicação entre os pontos de acesso e a SGC, os usuários associados à rede sem fios devem continuar conectados com acesso à rede. Também deve permitir que novos usuários se associam à rede sem fios utilizando autenticação do tipo 802.1X mesmo que os pontos de acesso estejam sem comunicação com a SGC;

3.9.4.9. Deve permitir o uso de voz e dados em cima de um mesmo SSID;

3.9.4.10. Deve suportar WMM, U-APSD e T-SPEC;

3.9.4.11. Implementar qualidade de serviço com a marcação de pacotes utilizando DSCP e suporte a 802.1p;

3.9.4.12. Deverá suportar Voice Enterprise;

3.9.4.13. Implementar CAC (Call Admission Control);

3.9.4.14. Deverá possuir funcionalidade de configuração do limite de banda disponível por usuário ou através de SSID/BSSID;

3.9.4.15. Deve permitir visibilidade e controle das aplicações, permitindo no mínimo o bloqueio e permissão de aplicações já na camada de acesso. Deve ter a capacidade de identificar, no mínimo, 1000 (um mil) aplicações diferentes;

3.9.4.16. Possuir relatório de compliance com regulamentação PCI DSS v3.0 ou superior;

3.9.5. Segurança

3.9.5.1. Os itens a seguir devem estar integrados a solução ofertada e não serão aceitos equipamentos

externos a solução. Caso sejam necessárias licenças ou softwares de controle os mesmos devem ser fornecidos de forma que a solução esteja operacional e sem nenhuma restrição no ato de sua implementação (hardware e softwares necessários para implementação);

3.9.5.2. Implementar, pelo menos, os seguintes padrões de segurança wireless:

3.9.5.2.1. (WPA) Wi-Fi Protected Access;

3.9.5.2.2. (WPA2) Wi-Fi Protected Access 2;

3.9.5.2.3. (WPA3) Wi-Fi Protected Access 3;

3.9.5.2.4. (TKIP) Temporal Key Integrity Protocol;

3.9.5.2.5. (AES) Advanced Encryption Standard;

3.9.5.2.6. IEEE 802.1X;

3.9.5.2.7. IEEE 802.11i;

3.9.5.2.8. IEEE 802.11w;

3.9.5.3. Implementar, pelo menos, os seguintes controles/filtros:

3.9.5.3.1. L2 – Baseado em MAC Address e Client Isolation;

3.9.5.3.2. L3 – Baseado em Endereço IP;

3.9.5.3.3. L4 – Baseado em Portas TCP/UDP;

3.9.5.3.4. Autenticação e Gerenciamento de usuários;

3.9.5.4. Permitir a autenticação para acesso dos usuários conectados nas redes WLAN (Wireless) através:

3.9.5.4.1. MAC Address;

3.9.5.4.2. Autenticação Local;

3.9.5.4.3. Captive Portal;

3.9.5.4.4. Active Directory;

3.9.5.4.5. RADIUS;

3.9.5.4.6. IEEE 802.1X;

3.9.5.4.7. LDAP;

3.9.5.5. Deve implementar autenticação IEEE 802.1X utilizando base de usuários interna e também servidor RADIUS externo;

3.9.5.6. Deverá permitir a seleção/uso de servidor RADIUS específico com base no SSID;

3.9.5.7. Deverá suportar servidor de autenticação RADIUS redundante, isto é, na falha de comunicação com o servidor RADIUS principal, o sistema deverá buscar um servidor RADIUS secundário;

3.9.5.8. Deverá permitir o Accounting do servidor RADIUS, inclusive com suporte ao parâmetro Framed-IP-Address, permitindo a identificação de um usuário e seu respectivo endereço IP associado;

3.9.5.9. Deverá suportar RADIUS CoA (Dynamic Change of Authorization);

3.9.5.10. Deve permitir a associação de controles/filtros/políticas de segurança para cada usuário de um mesmo SSID, com base nos parâmetros de autenticação;

3.9.5.11. A solução deverá suportar a criação de uma zona ou rede de visitantes, que terão seu acesso controlado através de senha cadastrada internamente, sendo que este deverá possuir a configuração de tempo pré-determinado de acesso a rede wireless;

3.9.5.12. A SGC deverá permitir a criação de múltiplos usuários visitantes (guests) de uma única vez (em lote);

3.9.5.13. Deve permitir que após o processo de autenticação de usuários visitantes (guests) os mesmos sejam redirecionados para uma página de navegação específica e configurável;

3.9.5.14. Deve permitir que o portal interno para usuários visitantes (guest) seja customizável;

3.9.5.15. Deverá permitir enviar a senha de usuários visitantes (guests), por e-mail ou por SMS;

3.9.5.16. Deverá permitir o encaminhamento do tráfego de saída de usuários visitantes (guests) diretamente para a internet, de forma totalmente separada do tráfego da rede corporativa;

3.9.5.17. Deverá permitir o isolamento da comunicação entre usuários visitantes (guests) em uma mesma VLAN/Subnet;

3.9.5.18. Possuir portal de autosserviço que permita que os próprios usuários visitantes da rede sem fio façam a solicitação de acesso por meio de preenchimento de formulários (self-registration), com possibilidade de aprovação manual realizada por operadores credenciados no sistema (sponsor);

3.9.6. WIPS

3.9.6.1. Implementar varredura de radiofrequência nas faixas de frequência dos padrões IEEE 802.11a/g/n/ac/ax para identificação de Pontos de Acesso intrusos não autorizados (rogues);

3.9.6.2. Detectar e gerar relatório de Pontos de Acesso não autorizados (rogue);

3.9.6.3. Detectar redes ad hoc;

3.9.6.4. Permitir a configuração dos Pontos de Acesso para atuarem exclusivamente como sensores de radiofrequência para fazer a monitoração do ambiente sem fio;

3.9.6.5. Realizar o rastreamento e a localização física aproximada dos Pontos de Acesso não autorizados (rogues);

3.9.6.6. Permitir a classificação automática dos Pontos de Acesso válidos e não autorizados (rogues);

3.9.6.7. Possuir funcionalidades de proteção contra-ataques dos ou Flood, com no mínimo os seguintes tipos:

3.9.6.7.1. Flood de autenticação;

3.9.6.7.2. Flood de desautenticação;

3.9.6.7.3. Flood de associação;

3.9.6.7.4. Flood de dissociação;

3.9.6.7.5. Flood de requisição de probe;

3.9.6.7.6. Flood de resposta de probe.

3.9.7. Marca/Modelo/Séries de Referencia: Extreme Networks XIQ, Alcatel Lucent OmniVista, Ruckus SmartZone, Juniper Junos Space, Cisco DNA e Aruba Central.

3.10. Serviço de instalação especializada - LAN

3.10.1. Correrá por conta da CONTRATADA toda e qualquer despesa, independentemente da sua natureza, decorrente dos serviços de instalação e configuração aqui mencionados. Cada unidade de serviço deverá contemplar instalação e configuração de um equipamento, considerando a ativação dele junto a plataforma de gerência e sua configuração básica;

3.10.2. Será realizada uma conferência de planejamento antes do início das atividades com o ponto de contato da CONTRATANTE para apresentar os principais participantes, confirmar a disponibilidade do local e outros pré-requisitos, além de discutir a logística de entrega do serviço;

3.10.3. Após o recebimento da solução (hardware/software), a CONTRATANTE deverá definir juntamente com a CONTRATADA o cronograma de instalação e configuração da mesma, enviando à CONTRATADA, documento contendo informações de Data, Hora, Local, e equipamentos a serem instalados;

3.10.4. No cronograma de instalação poderão ser definidos períodos fora do horário comercial, assim como finais de semana e feriados;

3.10.5. Deverá ser agendada uma reunião de kick-off com os times envolvidos para confirmar o escopo do projeto, identificar responsabilidades, riscos e pré-requisitos;

3.10.6. Deverá ser realizado o levantamento do ambiente atual, validando as premissas adotadas na elaboração desta proposta de serviço;

3.10.7. Deverá ocorrer a confirmação do pleno funcionamento da infraestrutura a ser utilizada no projeto (Rede, Servidores, Storage, por exemplo);

3.10.8. Deverá ser validado todo o licenciamento adquirido pelo CONTRATANTE relacionado aos produtos que serão instalados e configurados;

3.10.9. O processo de instalação/configuração deverá ter início em no máximo 30 (trinta) dias após a entrega dos equipamentos. Prazo este que poderá ser prorrogado de acordo com interesse da CONTRATANTE;

3.10.10. A CONTRATADA deverá realizar a instalação física e lógica "assistida" de todos os componentes de hardware e software, contemplados pelo escopo deste serviço, sob a supervisão dos técnicos da CONTRATANTE;

3.10.11. A CONTRATANTE deve acompanhar toda a atividade a ser realizada na janela de implantação;

3.10.12. Todo pessoal e ferramentas necessárias para execução dos serviços de instalação e configuração incluindo equipamentos ou ferramentas, bem como eventuais materiais necessários para ligações temporárias, são de inteira responsabilidade da empresa CONTRATADA;

3.10.13. Escopo dos Serviços a Serem Realizados:

3.10.13.1. Realizar a instalação do OS dos Switches a serem instalados no ambiente da CONTRATANTE;

3.10.13.2. Realizar a instalação do Software de Gerência de Rede a ser instalados no ambiente da CONTRATANTE;

3.10.13.3. Executar os testes necessários para validação da atualização, atestando o funcionamento adequado;

3.10.13.4. Configuração de VLANs, ACL, Malha ethernet e entre outros serviços relacionados ao funcionamento dos novos equipamentos na rede da CONTRATANTE;

3.11. Serviço de treinamento especializado - LAN

3.11.1. O Treinamento deverá possuir carga horária mínima de 40 (quarenta) horas e deverá ser realizado em Palmas/TO de forma presencial, ou de forma remota a critério da DPE-TO, com emissão de certificados de participação, para no mínimo 04 (quatro) servidores da DPE-TO;

3.11.2. O Treinamento deverá possuir conteúdo organizado em módulos, incluir material didático digital e abranger funcionalidades dos switches e software de gerência de rede descritos nesse instrumento.

3.12. Cordão Óptico 2 metros

3.12.1. Duplex, multimodo, com conectores LC/LC;

3.12.2. Composto por um par de fibras ópticas multimodo com revestimento primário em acrilato e revestimento secundário em material polimérico e termoplástico;

3.12.3. Deve possuir tamanho mínimo de 02 (dois) metros;

3.12.4. Possuir capa externa em PVC, não propagante a chama;

3.12.5. Deve utilizar padrão "zip-cord" em conformidade com os procedimentos exigidos pela NBR 14433;

3.12.6. Deve possuir certificação ANATEL para os conectores ópticos LC/LC;

3.12.7. Deverá possuir certificação ANATEL;

3.12.8. Deve possuir garantia de 12 meses;

3.12.9. Marca/Modelo/Séries de Referencia: Furukawa, CommScope, Nexans e Panduit.

3.13. Cordão Óptico 20 metros

3.13.1. Duplex, multimodo, com conectores LC/LC;

3.13.2. Composto por um par de fibras ópticas multimodo com revestimento primário em acrilato e revestimento secundário em material polimérico e termoplástico;

3.13.3. Deve possuir tamanho mínimo de 20 (vinte) metros;

3.13.4. Possuir capa externa em PVC, não propagante a chama;

3.13.5. Deve utilizar padrão “zip-cord” em conformidade com os procedimentos exigidos pela NBR 14433;

3.13.6. Deve possuir certificação ANATEL para os conectores ópticos LC/LC;

3.13.7. Deverá possuir certificação ANATEL;

3.13.8. Deve possuir garantia de 12 meses;

3.13.9. Marca/Modelo/Séries de Referencia: Furukawa, CommScope, Nexans e Panduit.

3.14. Access Point Indoor

3.14.1. Geral

3.14.1.1. Deve ser um equipamento ponto de acesso específico para ambientes internos e deverá atender aos padrões IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac e IEEE 802.11ax com operação nas frequências 2.4 GHz e 5 GHz de forma simultânea;

3.14.1.2. Deverá ser do mesmo fabricante da solução de SGC e/ou Controlador de Rede Sem Fio;

3.14.1.3. Deverá ser apresentado o certificado dentro do prazo de validade referente à homologação da Agência Nacional de Telecomunicações (ANATEL) para o produto, com data anterior à publicação do edital, conforme a resolução 242. Não serão aceitos protocolos de entrada ou outros documentos diferentes do certificado, uma vez que os mesmos não garantem o fornecimento de equipamentos homologados e em conformidade com as leis brasileira;

3.14.1.4. Deverá ser apresentado certificado válido fornecido pela Wi-Fi Alliance na categoria de Enterprise Access Point;

3.14.1.5. Implementar IEEE 802.11k;

3.14.1.6. Implementar IEEE 802.11r;

3.14.1.7. Implementar IEEE 802.11v;

3.14.1.8. Deverá vir acompanhado de estrutura que permita a utilização do equipamento em locais internos, com fixação em teto e parede;

3.14.1.9. Deve ser fornecido com injetor PoE que consiga fornecer potência suficiente para alimentação deste equipamento, este deverá ser do mesmo equipamento ou compatível com o fabricante;

3.14.1.10. Deverá possuir antenas internas e integradas com padrão de irradiação omnidirecional compatíveis com as frequências de rádio dos padrões IEEE 802.11a/b/g/n/ac/ax e com ganho de no mínimo 2.5 dBi em 2.4GHz e de no mínimo 3.5 dBi em 5GHz;

3.14.1.11. Não serão aceitos equipamentos com antenas aparentes (externas ao ponto de acesso) que sejam rosqueáveis, permitindo a remoção das antenas;

3.14.1.12. Deve suportar potência máxima de transmissão de no mínimo 18 dBm na frequência 2.4 GHz e de no mínimo 18 dBm na frequência 5 GHz;

3.14.1.13. Deverá atender aos padrões IEEE 802.11d e IEEE 802.11h;

3.14.1.14. Deverá suportar canalização de 20 MHz, 40 MHz e 80 MHz;

3.14.1.15. Deverá possuir mecanismo de rádio com suporte a MIMO 2x2 com 2 Spatial Streams;

3.14.1.16. Deverá suportar funcionamento com dois rádios operando em 5GHz. Caso o equipamento ofertado não possua tal funcionalidade, deverá suportar MIMO 4x4 com 4 Spatial Streams no rádio de 5GHz;

3.14.1.17. Deverá possuir suporte a Multi User MIMO (MU-MIMO);

3.14.1.18. Deverá suportar, no mínimo, 768 clientes associados, por ponto de acesso;

3.14.1.19. Deve suportar mecanismo que identifique e associe clientes preferencialmente na banda de 5GHz, deixando a banda de 2,4 GHz livre para dispositivos que trabalhem somente nesta frequência;

3.14.1.20. Deve implementar mecanismo de localização e rastreamento de usuários (Location Based Service);

3.14.1.21. Deverá possuir, no mínimo, 01 (uma) interface IEEE 802.3 10/100/1000Base-T Ethernet, auto-sensing, com conector RJ-45, para conexão à rede local fixa;

3.14.1.22. Possuir porta de console para gerenciamento e configuração via linha de comando (CLI – command line interface) com conector RJ-45 ou USB/microUSB, diferente da porta de rede solicitada anteriormente;

3.14.1.23. Possuir indicador luminoso (LED) ou indicadores luminosos (LEDs) para indicar o estado de operação do equipamento;

3.14.1.24. Possibilitar alimentação elétrica via padrão Power over Ethernet 802.3af;

3.14.1.25. Deve suportar temperatura de operação entre 0°C a 40°C com PoE ativado;

3.14.1.26. Deverá possuir estrutura que permita a utilização do equipamento em locais internos, com fixação em teto ou parede ou fornecer acessórios para que possa ser feita a fixação;

3.14.1.27. Não deve haver licença restringindo a quantidade de usuários conectados;

3.14.1.28. Deverá ser fornecido com todas as licenças para funcionamento em MESH (WiFi Mesh);

3.14.1.29. Deve suportar a utilização de sistema antifurto do tipo Kensington lock ou similar que permita a instalação de um cabo de segurança com a finalidade de evitar furto do equipamento;

3.14.1.30. Deverá possuir ao menos uma porta USB;

3.14.1.31. Deve possuir rádio Bluetooth Low-Energy (BLE) nativo no equipamento, caso o equipamento não possua nativamente, deve ser ofertado separadamente respeitando a quantidade de “Pontos de Acesso Sem Fio”;

3.14.2. Gerenciamento

3.14.2.1. Permitir gerenciamento através de plataformas de software que sigam padrões SNMPv2c e SNMPv3;

3.14.2.2. Implementar funcionamento em modo gerenciado por Sistema de Gerência Centralizada (SGC) ou Controlador de Rede Sem Fio, permitindo a manutenção, configuração e otimização dos pontos de acesso, otimizando o desempenho e a cobertura da radiofrequência (RF);

3.14.2.3. Permitir que sua configuração seja automaticamente realizada quando este for conectado no ambiente de rede do Sistema de Gerência Centralizada (SGC) ou Controlador de Rede Sem Fio especificado neste documento;

3.14.2.4. O ponto de acesso poderá estar diretamente ou remotamente conectado ao controlador WLAN, inclusive via roteamento da camada 3 de rede OSI;

3.14.2.5. O ponto de acesso deverá conectar-se ao Sistema de Gerência Centralizada (SGC) ou Controlador de Rede Sem Fio através de túnel seguro padrão ou através de protocolo de comunicação seguro para controle do equipamento;

3.14.2.6. Permitir o ajuste dinâmico de nível de potência de modo a otimizar o tamanho da célula de RF;

3.14.2.7. Deve suportar a identificação e controle de aplicações dos clientes conectados ao ponto de acesso;

3.14.3. Rede

3.14.3.1. Implementar cliente DHCP, para configuração automática de seu endereço IP e implementar também suporte à endereçamento IP estático;

3.14.3.2. Deve suportar VLAN seguindo a norma IEEE 802.1Q;

3.14.3.3. Possuir suporte de pelo menos a 8 SSIDs por rádio;

3.14.3.4. Permitir habilitar e desabilitar a divulgação do SSID;

3.14.3.5. Possuir capacidade de selecionar automaticamente o canal de transmissão;

3.14.3.6. Deve suportar limitação de banda por grupo de usuários ou SSID;

3.14.3.7. Implementar as seguintes taxas de transmissão com fallback automático:

3.14.3.7.1. IEEE 802.11b: 11, 5.5, 2 e 1 Mbps;

3.14.3.7.2. IEEE 802.11a e IEEE 802.11g: 54, 48, 36, 24, 18, 12, 9 e 6 Mbps;

3.14.3.7.3. IEEE 802.11n: 6.5 a 300 Mbps (MCS0 a MCS15);

3.14.3.7.4. IEEE 802.11ac: 6.5 a 866.6 Mbps (VHT0 a VHT9);

3.14.3.7.5. IEEE 802.11ax 2.4 GHz: 8.6 Mbps a 573.5 Mbps (HE0 a HE11);

3.14.3.7.6. IEEE 802.11ax 5 GHz: 8.6 Mbps a 1200 Mbps (HE0 a HE11);

3.14.4. Segurança

3.14.4.1.1. Implementar, pelo menos, os seguintes padrões de segurança:

3.14.4.1.2. (WPA2) Wi-Fi Protected Access 2;

3.14.4.1.3. (WPA3) Wi-Fi Protected Access 3;

3.14.4.1.4. (AES) Advanced Encryption Standard;

3.14.4.1.5. 802.1X;

3.14.4.1.6. IEEE 802.11i;

3.14.5. Deve possuir garantia do fabricante ou da revenda, desde que essa seja autorizada por carta pelo fabricante dos equipamentos a prestar o suporte e garantia, pelo período de 60 meses;

3.14.6. Marca/Modelo/Séries de Referencia: AP305C, OmniAccess AP1321, Ruckus R750, Juniper Mist AP12, Cisco 9105AX e Aruba AP-535.

3.15. Access Point Outdoor

3.15.1. Geral

3.15.1.1. Deve ser um equipamento ponto de acesso específico para ambientes externos e deverá atender aos padrões IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n, IEEE 802.11ac e IEEE 802.11ax com operação nas frequências 2.4 GHz e 5 GHz de forma simultânea;

3.15.1.2. Deverá ser do mesmo fabricante da solução de SGC e/ou Controlador de Rede Sem Fio;

3.15.1.3. Deverá ser apresentado o certificado dentro do prazo de validade referente à homologação da Agência Nacional de Telecomunicações (ANATEL) para o produto, com data anterior à publicação do edital, conforme a resolução 242. Não serão aceitos protocolos de entrada ou outros documentos diferentes do certificado, uma vez que os mesmos não garantem o fornecimento de equipamentos homologados e em conformidade com as leis brasileira;

3.15.1.4. Deverá ser apresentado certificado válido fornecido pela Wi-Fi Alliance na categoria de

Enterprise Access Point;

3.15.1.5. Implementar IEEE 802.11k;

3.15.1.6. Implementar IEEE 802.11r;

3.15.1.7. Implementar IEEE 802.11v;

3.15.1.8. Deverá possuir estrutura que permita a utilização do equipamento em locais externos, com fixação em poste e fornecer acessórios para que possa ser feita a fixação;

3.15.1.9. Deve ser fornecido com injetor PoE+ 802.3at que consiga fornecer potência suficiente para alimentação deste equipamento, este deverá ser do mesmo equipamento ou compatível com o fabricante, ainda deverá ser um injetor próprio para áreas externas;

3.15.1.10. Deverá possuir antenas internas e integradas com padrão de irradiação omnidirecional compatíveis com as frequências de rádio dos padrões IEEE 802.11a/b/g/n/ac/ax e com ganho de no mínimo 3 dBi em 2.4GHz e de no mínimo 4 dBi em 5GHz;

3.15.1.11. Não serão aceitos equipamentos com antenas aparentes (externas ao ponto de acesso) que sejam rosqueáveis, permitindo a remoção das antenas;

3.15.1.12. Deve suportar potência máxima de transmissão de no mínimo 18 dBm na frequência 2.4 GHz e de no mínimo 18 dBm na frequência 5 GHz;

3.15.1.13. Deverá atender aos padrões IEEE 802.11d e IEEE 802.11h;

3.15.1.14. Deverá suportar canalização de 20 MHz, 40 MHz, 80 MHz e 160 MHz;

3.15.1.15. Deverá possuir mecanismo de rádio com suporte a MIMO 4x4 com 4 Spatial Streams;

3.15.1.16. Deverá possuir suporte a Multi User MIMO (MU-MIMO);

3.15.1.17. Deverá suportar, no mínimo, 768 clientes associados, por ponto de acesso;

3.15.1.18. Deve suportar mecanismo que identifique e associe clientes preferencialmente na banda de 5GHz, deixando a banda de 2,4 GHz livre para dispositivos que trabalhem somente nesta frequência;

3.15.1.19. Deve implementar mecanismo de localização e rastreamento de usuários (Location Based Service);

3.15.1.20. Deverá possuir, no mínimo, 01 (uma) interface IEEE 802.3 10/100/1000Base-T Ethernet, auto-sensing, com conector RJ-45, para conexão à rede local fixa;

3.15.1.21. Deverá possuir, no mínimo, 01 (uma) interface IEEE 802.3 100/1000/2500Base-T Ethernet, auto-sensing, com conector RJ-45, para conexão à rede local fixa;

3.15.1.22. Possuir porta de console para gerenciamento e configuração via linha de comando (CLI – command line interface) com conector RJ-45 ou USB/microUSB, diferente da porta de rede solicitada anteriormente;

3.15.1.23. Possuir indicador luminoso (LED) ou indicadores luminosos (LEDs) para indicar o estado de operação do equipamento;

3.15.1.24. Possibilitar alimentação elétrica via padrão Power over Ethernet 802.3at através de uma única interface de rede, permitindo a ativação de todas as funcionalidades e rádios do ponto de acesso;

3.15.1.25. Deve suportar temperatura de operação entre -40°C a 60°C com PoE ativado;

3.15.1.26. Deve suportar, no mínimo, proteção IP-67;

3.15.1.27. Deverá possuir estrutura que permita a utilização do equipamento em locais externos, com fixação em poste e fornecer acessórios para que possa ser feita a fixação;

3.15.1.28. Não deve haver licença restringindo a quantidade de usuários conectados;

3.15.1.29. Deverá ser fornecido com todas as licenças para funcionamento em MESH (WiFi Mesh);

3.15.1.30. Deverá possuir ao menos uma porta USB;

3.15.1.31. Deve possuir rádio Bluetooth Low-Energy (BLE) nativo no equipamento, caso o equipamento não possua nativamente, deve ser ofertado separadamente respeitando a quantidade de “Pontos de Acesso Sem Fio”;

3.15.2. Gerenciamento

3.15.2.1. Permitir gerenciamento através de plataformas de software que sigam padrões SNMPv2c e SNMPv3;

3.15.2.2. Implementar funcionamento em modo gerenciado por Sistema de Gerência Centralizada (SGC) ou Controlador de Rede Sem Fio, permitindo a manutenção, configuração e otimização dos pontos de acesso, otimizando o desempenho e a cobertura da radiofrequência (RF);

3.15.2.3. Permitir que sua configuração seja automaticamente realizada quando este for conectado no ambiente de rede do Sistema de Gerência Centralizada (SGC) ou Controlador de Rede Sem Fio especificado neste documento;

3.15.2.4. O ponto de acesso poderá estar diretamente ou remotamente conectado ao controlador WLAN, inclusive via roteamento da camada 3 de rede OSI;

3.15.2.5. O ponto de acesso deverá conectar-se ao Sistema de Gerência Centralizada (SGC) ou Controlador de Rede Sem Fio através de túnel seguro padrão ou através de protocolo de comunicação seguro para controle do equipamento;

3.15.2.6. Permitir o ajuste dinâmico de nível de potência de modo a otimizar o tamanho da célula de RF;

3.15.2.7. Deve suportar a identificação e controle de aplicações dos clientes conectados ao ponto de acesso;

3.15.3. Rede

3.15.3.1. Implementar cliente DHCP, para configuração automática de seu endereço IP e implementar também suporte à endereçamento IP estático;

3.15.3.2. Deve suportar VLAN seguindo a norma IEEE 802.1Q;

3.15.3.3. Possuir suporte de pelo menos a 8 SSIDs por rádio;

3.15.3.4. Permitir habilitar e desabilitar a divulgação do SSID;

3.15.3.5. Possuir capacidade de selecionar automaticamente o canal de transmissão;

3.15.3.6. Deve suportar limitação de banda por grupo de usuários ou SSID;

3.15.3.7. Implementar as seguintes taxas de transmissão com fallback automático:

3.15.3.7.1. IEEE 802.11b: 11, 5.5, 2 e 1 Mbps;

3.15.3.7.2. IEEE 802.11a e IEEE 802.11g: 54, 48, 36, 24, 18, 12, 9 e 6 Mbps;

3.15.3.7.3. IEEE 802.11n: 6.5 a 600 Mbps (MCS0 a MCS31);

3.15.3.7.4. IEEE 802.11ac: 6.5 a 3466.6 Mbps (VHT0 a VHT9);

3.15.3.7.5. IEEE 802.11ax 2.4 GHz: 8.6 Mbps a 573.5 Mbps (HE0 a HE11);

3.15.3.7.6. IEEE 802.11ax 5 GHz: 8.6 Mbps a 4800 Mbps (HE0 a HE11);

3.15.4. Segurança

3.15.4.1. Implementar, pelo menos, os seguintes padrões de segurança:

3.15.4.1.1. (WPA2) Wi-Fi Protected Access 2;

3.15.4.1.2. (WPA3) Wi-Fi Protected Access 3;

3.15.4.1.3. (AES) Advanced Encryption Standard;

3.15.4.1.4. 802.1X;

3.15.4.1.5. IEEE 802.11i;

3.15.5. Deve possuir garantia do fabricante ou da revenda, desde que essa seja autorizada por carta pelo fabricante dos equipamentos a prestar o suporte e garantia, pelo período de 60 meses;

3.15.6. Marca/Modelo/Séries de Referencia: AP460C, OmniAccess AP1361, Ruckus T750, Juniper Mist AP63, Cisco 9124AX e Aruba AP-575.

3.16. Licenças Software de Gerência Centralizada - WLAN

3.16.1. Características Gerais

3.16.1.1. A Solução de Gerência Centralizada (SGC) deve ser fornecida em formato local (on premises) ou em nuvem pública do mesmo fabricante dos pontos de acesso;

3.16.1.1.1. Em caso de nuvem pública, deve apresentar disponibilidade mínima de 99,9%;

3.16.1.2. Deve ser possível gerenciar todos os dispositivos com todas as funcionalidades descritas pelo período mínimo de 60 meses;

3.16.1.3. Deve possibilitar a centralização da configuração, otimização, monitoramento e manutenção dos pontos de acesso gerenciados;

3.16.1.4. Será permitido que as funções de controle da rede sem fio sejam executadas por uma das seguintes arquiteturas:

3.16.1.5. Centralizada na própria Solução de Gerência Centralizada (SGC)

3.16.1.5.1. Pode-se utilizar nuvem pública que apresente disponibilidade mínima de 99,9%;

3.16.1.5.2. Ser do mesmo fabricante dos pontos de acesso;

3.16.1.6. Controlador de Rede Sem Fio Centralizado em appliance físico (Hardware)

3.16.1.6.1. Deverá possuir hardware dedicado com software de gerenciamento e administração já embarcado;

3.16.1.6.2. Deverá possuir porta de console para gerenciamento e configuração via linha de comando CLI com conector RJ-45 ou Conector padrão RS-232 ou USB;

3.16.1.6.3. Deverá possuir, no mínimo 02 (duas) interfaces Ethernet 10Gbps SFP+;

3.16.1.6.4. Possuir fontes de alimentação redundantes com seleção automática de tensão (100-240V AC);

3.16.1.6.5. Permitir ser montado em rack padrão de 19 (dezenove) polegadas, incluindo todos os acessórios necessários e não consumir mais que 2 RU form factor;

3.16.1.6.6. Deve suportar temperatura de operação entre 0°C a 40°C;

3.16.1.6.7. Deve ser acompanhado de todos os acessórios necessários para operacionalização da solução, tais como: softwares, licenças, cabos de energia elétrica, documentações técnicas e manuais que contenham informações suficientes, que possibilite a instalação, configuração e operacionalização do equipamento;

3.16.1.6.8. Implementar redundância N+1 ou Cluster de Controladores, com sincronismo automático das configurações entre os equipamentos, garantindo assim que se um controlador de rede sem fio falhar, os Pontos de Acesso relacionados serão associados automaticamente a um controlador de rede sem fio alternativo, não permitindo que a rede sem fio se torne inoperante;

3.16.1.7. Controlador de Rede Sem Fio Centralizado em appliance virtual

3.16.1.7.1. Para instalação deverá ser compatível com uma das seguintes plataformas:

3.16.1.7.1.1. Bare Metal ou Hypervisors:

3.16.1.7.1.2. Xen 4 ou superior;

3.16.1.7.1.3. Hyper-V 2012 R2 ou superior;

3.16.1.7.1.4. VMware vSphere ESXi 6 ou superior;

3.16.1.7.2. Deve ser acompanhado de todos os acessórios necessários para operacionalização da solução, tais como: softwares, licenças, documentações técnicas e manuais que contenham informações suficientes, que possibilite a instalação, configuração e operacionalização do equipamento;

3.16.1.7.3. Implementar redundância N+1 ou Cluster de Controladores, com sincronismo automático das configurações entre os equipamentos, garantindo assim que se um controlador de rede sem fio falhar, os Pontos de Acesso relacionados serão associados automaticamente a um controlador de rede sem fio alternativo, não permitindo que a rede sem fio se torne inoperante;

3.16.1.7.4. Seguir as mesmas características de capacidade e licenciamento da Solução de Gerência Centralizada (SGC);

3.16.1.8. Não será permitido soluções onde um único Ponto de Acesso mesmo que redundante seja promovido para suportar as funções de controle da rede sem fio ou da Solução de Gerência Centralizada (SGC);

3.16.1.9. Qualquer que seja a solução escolhida, deverá suportar pontos de acesso internos e externos nos padrões 802.11a/b/g/n/ac/ax, compatíveis com os demais itens deste termo;

3.16.1.10. Deve possuir garantia, suporte, atualizações e troca de hardware com envio na modalidade NBD por um período de 60 (sessenta) meses, independente da arquitetura adotada (hardware dedicado, computação virtual ou nuvem pública do fabricante dos pontos de acesso) para todos os itens que sejam fornecidos para compor a solução;

3.16.2. Gerenciamento

3.16.2.1. Suportar, no mínimo, 20.000 (vinte mil) dispositivos conectados simultaneamente;

3.16.2.2. Deve permitir que as configurações sejam aplicadas em vários pontos de acesso selecionados simultaneamente, isto é, não será permitido soluções que necessitem configurar os pontos de acesso individualmente;

3.16.2.3. Permitir a configuração total dos pontos de acesso, assim como os aspectos de segurança da rede wireless (WLAN) e Rádio Frequência (RF);

3.16.2.4. A SGC poderá estar diretamente e/ou remotamente conectado aos Pontos de Acesso por ele gerenciados, inclusive via roteamento nível 3 da camada OSI;

3.16.2.5. Possibilitar a configuração de envio dos eventos dos Pontos de Acesso ou da SGC para um servidor de Syslog remoto;

3.16.2.6. Implementar, pelo menos, os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps SNMP;

3.16.2.7. Permitir a visualização de alertas da rede sem fio em tempo real;

3.16.2.8. Implementar no mínimo dois níveis de acesso administrativo à SGC (apenas leitura e leitura/escrita) protegidos por senhas independentes;

3.16.2.9. Permitir a customização do acesso administrativo através de atribuição de grupo de função do usuário administrador;

3.16.2.10. Permitir a configuração e gerenciamento através de browser padrão (HTTPS) ou porta console;

3.16.2.11. Gerenciar de forma centralizada a autenticação de usuários na integração com servidores AAA (Radius);

3.16.2.12. Permitir o envio de alertas ou alarmes através do protocolo SMTP, sendo que a comunicação com o servidor deverá ser autenticada e cifrada (SMTP/TLS);

3.16.2.13. Permitir que o processo de atualização de versão seja realizado através de browser padrão (HTTPS) ou SSH;

3.16.2.14. Deverá possuir a capacidade de importação de certificados digitais emitidos por uma autoridade certificadora externa;

3.16.2.15. Deverá implementar disponibilidade de SSID baseado em dia da semana/hora, permitindo ao

administrador do sistema, habilitar ou não um determinado SSID somente em hora/dia da semana determinados;

3.16.2.16. Possuir ferramentas de debug e log de eventos para depuração e gerenciamento em primeiro nível (ping, trace e logs);

3.16.2.17. Possuir ferramenta que permita o monitoramento em tempo real de informações de utilização de CPU, memória e estatísticas de rede da SGC ou dos Pontos de Acesso;

3.16.2.18. Possibilitar cópia "backup" da configuração, bem como a funcionalidade de restauração da configuração através de browser padrão (HTTPS) ou FTP ou TFTP;

3.16.2.19. Possuir a capacidade de armazenar múltiplos arquivos de configuração pertencente à rede wireless;

3.16.2.20. Monitorar o desempenho da rede wireless, permitindo a visualização de informações de cada ponto de acesso;

3.16.2.21. A falha de comunicação entre SGC e os Pontos de Acesso não devem interferir na operação dos Pontos de Acesso;

3.16.2.22. Deverá possuir a capacidade de geração de informações ou relatórios de no mínimo os seguintes tipos: Listagem de clientes Wireless, Listagem de Pontos de Acesso, utilização da rede;

3.16.2.23. Deverá suportar protocolo LLDP;

3.16.2.24. Deverá suportar a identificação de aplicações dos clientes conectados ao ponto de acesso;

3.16.2.25. Permitir visualizar a localização dos pontos de acesso e através desta obter o status de funcionamento dos mesmos;

3.16.2.26. Deverá permitir o acréscimo unitário de licenças para expansão da capacidade dos Pontos de Acesso ou cada Pontos de Acesso deve vir acompanhado de sua licença;

3.16.2.27. Na ocorrência de inoperância de um Ponto de Acesso, a solução deverá ajustar automaticamente a potência dos Pontos de Acesso adjacentes, de modo a prover a cobertura da área não assistida;

3.16.2.28. Ajustar automaticamente a utilização de canais de modo a otimizar a cobertura de rede de acordo com as condições de RF;

3.16.2.29. Detectar interferência e ajustar parâmetros de RF, evitando problemas de cobertura de RF de forma automática;

3.16.2.30. O SGC deve possuir funcionalidade de analisador gráfico de espectro para detecção de interferências nas faixas de frequência de 2.4 e 5 GHz, sejam elas IEEE 802.11 ou não. Deve disponibilizar interface gráfica com, pelo menos, gráficos de Fast Fourier Transform (FFT) e espectrograma; Caso a funcionalidade não possa ser apresentada pelo SGC, deve ser fornecido um equipamento ou software, do mesmo fabricante, que a faça;

3.16.2.31. Deve detectar interferências Wi-Fi (provenientes de dispositivos padrão IEEE802.11) e também detectar e classificar no mínimo 3 (três) padrões de assinaturas de interferências não-Wi-Fi, com por exemplo, telefones sem fio, microondas, etc.;

3.16.2.32. Deve possuir ferramenta de localização e analíticos sobre localização que implemente:

3.16.2.32.1. Criação de zonas ou regiões de interesse dentro de plantas de uma determinada localidade;

3.16.2.32.2. Mapeamento de zonas ou regiões de interesse em categorias de engajamento;

3.16.2.32.3. Coleta de dados de presença e proximidade, reportando para uma determinada localidade, no mínimo, a quantidade de:

3.16.2.32.3.1. Visitantes internos engajados;

3.16.2.32.3.2. Passantes externos;

3.16.2.32.3.3. Novos visitantes;

3.16.2.32.3.4. Visitantes já vistos anteriormente;

3.16.2.32.4. Informações sobre fluxo ou trajeto entre categorias de engajamento diferentes;

3.16.2.32.5. Informações sobre aglomerações em determinadas categorias de engajamento;

3.16.2.32.6. Rastreamento de ativos baseados em beacons Bluetooth Low Energy e Wi-Fi;

3.16.2.32.7. Associação de ativos baseados em beacons Bluetooth Low Energy ou Wi-Fi a determinadas categorias de engajamento permitidas;

3.16.2.32.8. Alarmes caso um ativo baseado em beacons Bluetooth Low Energy ou Wi-Fi viole o confinamento de uma categoria de engajamento;

3.16.2.32.9. Exportação de dados para coletores externos, suportando integração com soluções de terceiros;

3.16.2.33. Deve possuir ferramenta integrada ao SGC de projeto da rede sem fio, que permita:

3.16.2.33.1. Importação de plantas baixas em pelo menos um dos formatos gráficos: dwg, dxf, dxb, dwf, jpg, gif, bmp e png dos locais de instalação;

3.16.2.33.2. Simulação da cobertura da rede sem fio, apresentando, no mínimo, RSSI, SNR e distribuição de canais;

3.16.2.33.3. Posicionamento automático e manual dos Pontos de Acesso, e os ajustes das características dos rádios destes APs;

3.16.2.33.4. Geração de relatórios com os mapas de cobertura projetados e lista dos dispositivos utilizados na simulação;

3.16.2.34. Deve possuir ferramenta integrada ao SGC para permitir ao administrador visualizar e monitorar o mapa de cobertura detalhado (heatmap) da rede sem fio;

3.16.2.35. Implementar sistema automático de balanceamento de carga para associação de clientes entre Pontos de Acesso próximos, para otimizar a performance;

3.16.2.36. Implementar funcionalidade de balanceamento de carga entre os rádios de um mesmo Ponto de Acesso;

3.16.2.37. Permitir que o serviço wireless seja desabilitado de determinado ponto de acesso. Também deve ser possível selecionar o serviço de qual rádio (banda) de determinado ponto de acesso deve ser desabilitado;

3.16.3. Rede

3.16.3.1. Deverá implementar suporte aos protocolos IPv4 e IPv6;

3.16.3.2. Deverá implementar tagging de VLANs através do protocolo 802.1Q;

3.16.3.3. Suportar a configuração de no mínimo 4000 (quatro mil) VLANs;

3.16.3.4. Deverá oferecer os recursos de mobilidade para roaming de camada L2 e L3;

3.16.3.5. Deverá implementar DHCP Relay e DHCP Server nos Pontos de Acesso;

3.16.3.6. Implementar associação dinâmica de usuário a VLAN com base nos parâmetros da etapa de autenticação via IEEE 802.1X;

3.16.3.7. Deverá permitir que clientes sejam designados para diferentes VLANs dentro de um mesmo SSID;

3.16.3.8. Em caso de falha de comunicação entre os pontos de acesso e a SGC, os usuários associados à rede sem fios devem continuar conectados com acesso à rede. Também deve permitir que novos usuários se associam à rede sem fios utilizando autenticação do tipo 802.1X mesmo que os pontos de acesso estejam sem comunicação com a SGC;

3.16.3.9. Deve permitir o uso de voz e dados em cima de um mesmo SSID;

3.16.3.10. Deve suportar WMM, U-APSD e T-SPEC;

3.16.3.11. Implementar qualidade de serviço com a marcação de pacotes utilizando DSCP e suporte a

802.1p;

3.16.3.12. Deverá suportar Voice Enterprise;

3.16.3.13. Implementar CAC (Call Admission Control);

3.16.3.14. Deverá possuir funcionalidade de configuração do limite de banda disponível por usuário ou através de SSID/BSSID;

3.16.3.16. Deve permitir visibilidade e controle das aplicações, permitindo no mínimo o bloqueio e permissão de aplicações já na camada de acesso. Deve ter a capacidade de identificar, no mínimo, 1000 (um mil) aplicações diferentes;

3.16.3.16. Possuir relatório de compliance com regulamentação PCI DSS v3.0 ou superior;

3.16.4. Segurança

3.16.4.1. Os itens a seguir devem estar integrados a solução ofertada e não serão aceitos equipamentos externos a solução. Caso sejam necessárias licenças ou softwares de controle os mesmos devem ser fornecidos de forma que a solução esteja operacional e sem nenhuma restrição no ato de sua implementação (hardware e softwares necessários para implementação);

3.16.4.2. Implementar, pelo menos, os seguintes padrões de segurança wireless:

3.16.4.2.1. (WPA) Wi-Fi Protected Access;

3.16.4.2.2. (WPA2) Wi-Fi Protected Access 2;

3.16.4.2.3. (WPA3) Wi-Fi Protected Access 3;

3.16.4.2.4. (TKIP) Temporal Key Integrity Protocol;

3.16.4.2.5. (AES) Advanced Encryption Standard;

3.16.4.2.6. IEEE 802.1X;

3.16.4.2.7. IEEE 802.11i;

3.16.4.2.8. IEEE 802.11w;

3.16.4.3. Implementar, pelo menos, os seguintes controles/filtros:

3.16.4.3.1. L2 – Baseado em MAC Address e Client Isolation;

3.16.4.3.2. L3 – Baseado em Endereço IP;

3.16.4.3.3. L4 – Baseado em Portas TCP/UDP;

3.16.4.3.4. Autenticação e Gerenciamento de usuários;

3.16.4.4. Permitir a autenticação para acesso dos usuários conectados nas redes WLAN (Wireless) através:

3.16.4.4.1. MAC Address;

3.16.4.4.2. Autenticação Local;

3.16.4.4.3. Captive Portal;

3.16.4.4.4. Active Directory;

3.16.4.4.5. RADIUS;

3.16.4.4.6. IEEE 802.1X;

3.16.4.4.7. LDAP;

3.16.4.5. Deve implementar autenticação IEEE 802.1X utilizando base de usuários interna e também servidor RADIUS externo;

3.16.4.6. Deverá permitir a seleção/uso de servidor RADIUS específico com base no SSID;

3.16.4.7. Deverá suportar servidor de autenticação RADIUS redundante, isto é, na falha de comunicação com o servidor RADIUS principal, o sistema deverá buscar um servidor RADIUS secundário;

3.16.4.8. Deverá permitir o Accounting do servidor RADIUS, inclusive com suporte ao parâmetro Framed-IP-Address, permitindo a identificação de um usuário e seu respectivo endereço IP associado;

3.16.4.9. Deverá suportar RADIUS CoA (Dynamic Change of Authorization);

3.16.4.10. Deve permitir a associação de controles/filtros/políticas de segurança para cada usuário de um mesmo SSID, com base nos parâmetros de autenticação;

3.16.4.11. A solução deverá suportar a criação de uma zona ou rede de visitantes, que terão seu acesso controlado através de senha cadastrada internamente, sendo que este deverá possuir a configuração de tempo pré-determinado de acesso a rede wireless;

3.16.4.12. A SGC deverá permitir a criação de múltiplos usuários visitantes (guests) de uma única vez (em lote);

3.16.4.13. Deve permitir que após o processo de autenticação de usuários visitantes (guests) os mesmos sejam redirecionados para uma página de navegação específica e configurável;

3.16.4.14. Deve permitir que o portal interno para usuários visitantes (guest) seja customizável;

3.16.4.15. Deverá permitir enviar a senha de usuários visitantes (guests), por e-mail ou por SMS;

3.16.4.16. Deverá permitir o encaminhamento do tráfego de saída de usuários visitantes (guests) diretamente para a internet, de forma totalmente separada do tráfego da rede corporativa;

3.16.4.17. Deverá permitir o isolamento da comunicação entre usuários visitantes (guests) em uma mesma VLAN/Subnet;

3.16.4.18. Possuir portal de autosserviço que permita que os próprios usuários visitantes da rede sem fio façam a solicitação de acesso por meio de preenchimento de formulários (self-registration), com possibilidade de aprovação manual realizada por operadores credenciados no sistema (sponsor);

3.16.5. WIPS

3.16.5.1. Implementar varredura de radiofrequência nas faixas de frequência dos padrões IEEE 802.11a/g/n/ac/ax para identificação de Pontos de Acesso intrusos não autorizados (rogues);

3.16.5.2. Detectar e gerar relatório de Pontos de Acesso não autorizados (rogue);

3.16.5.3. Detectar redes ad hoc;

3.16.5.4. Permitir a configuração dos Pontos de Acesso para atuarem exclusivamente como sensores de radiofrequência para fazer a monitoração do ambiente sem fio;

3.16.5.5. Realizar o rastreamento e a localização física aproximada dos Pontos de Acesso não autorizados (rogues);

3.16.5.6. Permitir a classificação automática dos Pontos de Acesso válidos e não autorizados (rogues);

3.16.5.7. Possuir funcionalidades de proteção contra ataques DoS ou Flood, com no mínimo os seguintes tipos:

3.16.5.7.1. Flood de autenticação;

3.16.5.7.2. Flood de desautenticação;

3.16.5.7.3. Flood de associação;

3.16.5.7.4. Flood de dissociação;

3.16.5.7.5. Flood de requisição de probe;

3.16.5.7.6. Flood de resposta de probe;

1.16.6. Marca/Modelo/Séries de Referencia: Extreme Networks XIQ, Alcatel Lucent OmniVista, Ruckus SmartZone, Juniper Mist AI, Cisco DNA e Aruba Mobility Controller.

3.17. Serviço de instalação especializada - WLAN

3.17.1. Correrá por conta da CONTRATADA toda e qualquer despesa, independentemente da sua natureza, decorrente dos serviços de instalação e configuração aqui mencionados. Cada unidade de serviço deverá contemplar instalação e configuração de um equipamento, considerando a ativação dele junto a plataforma de gerência e sua configuração básica;

3.17.2. Será realizada uma conferência de planejamento antes do início das atividades com o ponto de contato da CONTRATANTE para apresentar os principais participantes, confirmar a disponibilidade do local e outros pré-requisitos, além de discutir a logística de entrega do serviço;

3.17.3. Após o recebimento da solução (hardware/software), a CONTRATANTE deverá definir juntamente com a CONTRATADA o cronograma de instalação e configuração da mesma, enviando à CONTRATADA, documento contendo informações de Data, Hora, Local, e equipamentos a serem instalados;

3.17.4. No cronograma de instalação poderão ser definidos períodos fora do horário comercial, assim como finais de semana e feriados

3.17.5. Deverá ser agendada uma reunião de kick-off com os times envolvidos para confirmar o escopo do projeto, identificar responsabilidades, riscos e pré-requisitos;

3.17.6. Deverá ser realizado o levantamento do ambiente atual, validando as premissas adotadas na elaboração desta proposta de serviço;

3.17.7. Deverá ocorrer a confirmação do pleno funcionamento da infraestrutura a ser utilizada no projeto (Rede, Servidores, Storage, Access Points, por exemplo);

3.17.8. Deverá ser validado todo o licenciamento adquirido pelo CONTRATANTE relacionado aos produtos que serão instalados e configurados;

3.17.9. O processo de instalação/configuração deverá ter início em no máximo 30 (trinta) dias após a entrega dos equipamentos. Prazo este que poderá ser prorrogado de acordo com interesse da CONTRATANTE;

3.17.10. A CONTRATADA deverá realizar a instalação física e lógica “assistida” de todos os componentes de hardware e software, contemplados pelo escopo deste serviço, sob a supervisão dos técnicos da CONTRATANTE;

3.17.11. A CONTRATANTE deve acompanhar toda a atividade a ser realizada na janela de implantação;

3.17.12. Todo pessoal e ferramentas necessárias para execução dos serviços de instalação e configuração incluindo equipamentos ou ferramentas, bem como eventuais materiais necessários para ligações temporárias, são de inteira responsabilidade da empresa CONTRATADA;

3.17.13. Escopo dos Serviços a Serem Realizados:

3.17.14. Realizar a instalação do OS dos Access Points a serem instalados no ambiente da CONTRATANTE;

3.17.15. Realizar a instalação do Software de Gerência WLAN a ser instalados no ambiente da CONTRATANTE;

3.17.16. Executar os testes necessários para validação da atualização, atestando o funcionamento adequado;

3.17.17. Configuração de serviços relacionados ao funcionamento dos equipamentos Wi-Fi na rede da CONTRATANTE;

3.18. Serviço de treinamento especializada - WLAN

3.18.1. O Treinamento deverá possuir carga horária mínima de 24 (vinte e quatro) horas e deverá ser realizado em Palmas/TO de forma presencial, ou de forma remota a critério da DPE-TO, com emissão de certificados de participação, para no mínimo 04 (quatro) servidores da DPE-TO;

3.18.2. O Treinamento deverá possuir conteúdo organizado em módulos, incluir material didático digital e

abranger funcionalidades dos pontos de acesso e software de gerência wlan desse termo de referência;

4. DO CUSTO ESTIMADO

4.1. O valor estimado da aquisição é de **R$ 5.882.032,81 (cinco milhões, oitocentos e oitenta e dois mil trinta e dois reais e oitenta e um centavos)**;

4.2. A formalização da despesa se dará por meio de contrato a ser devidamente assinado.

5 – DAS CONDIÇÕES DE PAGAMENTO

5.1. O pagamento ocorrerá no prazo de até 30 dias corridos contados após o recebimento da Nota Fiscal/Fatura, por meio de crédito em conta bancária, após efetiva emissão das notas fiscais e comprovação quanto à manutenção da regularidade fiscal e trabalhista, condicionado ao atesto do titular ou substituto responsável pela fiscalização do contrato.

5.2. O CNPJ constante da Nota Fiscal/Fatura deverá ser o mesmo indicado na nota de empenho, vinculado a conta corrente da CONTRATADA;

5.3. A DPE-TO reserva-se ao direito de não atestar a Nota Fiscal/Fatura para o pagamento, caso os dados constantes desta estiverem em desacordo com os dados da CONTRATANTE ou ainda, se os equipametnos ou serviços entregues não estiverem em conformidade com as especificações apresentadas neste Instrumento, ficando o pagamento suspenso até a regularização;

5.4. No caso de atraso de pagamento, desde que o contratado não tenha concorrido de alguma forma para tanto, serão devidos pela DPE encargos moratórios à taxa nominal de 6% a.a. (seis por cento ao ano), capitalizados diariamente em regime de juros simples.

6 - DO PRAZO E LOCAL DA ENTREGA

6.1. Os equipamentos/licenças deverão ser entregues na Coordenação de Almoxarifado da DPE-TO, localizada na Quadra 903 Sul, Alameda 11, QI 05, Lote 09 Plano Diretor Sul – Palmas – TO, ou em outro local a ser informado previamente pela DPE-TO, nos seguintes horários: 08:00 às 11:30 e 14:00 às 16:30;

6.2. O prazo de entrega do objeto será de, no máximo 60 (sessenta) dias corridos, contados a partir da assinatura do contrato, podendo ser prorrogado caso haja pedido formal devidamente justificado pela CONTRATADA e acatado pela Defensoria Pública do Estado do Tocantins.

7. DA VIGÊNCIA DO REGISTRO DE PREÇOS

7.1. A Ata de Registro de Preços terá vigência de 12 (doze) meses, a contar da publicação do seu extrato em Diário Oficial da Defensoria Púbica do Estado do Tocantins.

8. DA VIGÊNCIA DO CONTRATO

8.1. O Contrato terá vigência de 12 (doze) meses contados a partir da assinatura do contrato;

9. DAS OBRIGAÇÕES DO ÓRGÃO GERENCIADOR

9.1. A Diretoria de Tecnologia da Informação da Defensoria Pública do Estado do Tocantins gerenciará a Ata de Registro de Preços.

9.2. São obrigações do órgão gerenciador:

a) Efetuar o registro do licitante fornecedor e firmar a correspondente Ata de Registro de Preços;

b) Designar servidor responsável pelo acompanhamento das despesas decorrentes do presente termo e para atestar o recebimento dos materiais/equipamentos, ou rejeitá-los no todo ou em parte;

c) Assegurar-se do fiel cumprimento das condições estabelecidas na ata, no instrumento convocatório e seus anexos, em relação às suas próprias contratações;

d) Aplicar as penalidades por descumprimento do pactuado na Ata de Registro de Preços, em relação às suas próprias contratações;

e) Responsabilizar-se pela observância quanto às leis, decretos, regulamentos, portarias e demais normas legais, direta e indiretamente aplicáveis à execução do objeto, em relação às suas próprias contratações.

10. DAS OBRIGAÇÕES DO FORNECEDOR REGISTRADO

10.1. São obrigações do licitante fornecedor:

a) Assinar a Ata de Registro de Preços em até 05 (cinco) dias úteis, contados da sua

notificação, conforme previsto no edital;

b) Assinar o contrato em até 05 (cinco) dias úteis, contados da sua notificação;

c) Não subcontratar o objeto do presente termo;

d) Manter, durante a vigência da ata de registro de preço, as condições de habilitação exigidas no Edital;

10.2 A contratação ora pretendida ocorrerá através da assinatura do instrumento contratual, momento em que a Contratada, obrigar-se-á:

a) Observar as Leis, Decretos, Regulamentos, Portarias e normas Federais, Estaduais e Municipais direta e indiretamente aplicáveis ao objeto licitado;

b) Indenizar quaisquer danos ou prejuízos causados a Defensoria Pública do Estado do Tocantins, ou a terceiros, por ação ou omissão no fornecimento do objeto;

c) Prestar as informações e os esclarecimentos solicitados pela Contratante, no prazo máximo de 48 (quarenta e oito) horas, contados da data do protocolo de recebimento da demanda;

d) Responsabilizar-se por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas na legislação específica, cuja inadimplência não transfere responsabilidade a esta Instituição;

e) Reparar o equipamento caso este venha a ser danificado, sem que haja quaisquer ônus para esta Instituição, em até 24 (vinte e quatro) horas contadas a partir do recebimento da solicitação. Em casos de necessidade de substituição de peças/equipamento terá até 15 (quinze) dias corridos contados a partir do recebimento da solicitação. O prazo poderá ser prorrogado por igual período, a critério da administração pública, quando requerida pela contratada, mediante justificativa apresentada dentro do prazo inicial;

f) Providenciar todos os recursos e insumos necessários à perfeita execução do objeto, devendo estar incluídas no preço proposto todas as despesas com materiais, insumos, mão-de-obra, fretes, embalagens, seguros, impostos, taxas, tarifas, encargos sociais e trabalhistas e demais despesas necessárias à perfeita entrega dos produtos;

g) Entregar os equipamentos, acondicionado adequadamente, em invólucro lacrado, de forma a permitir completa segurança durante o transporte, acompanhado de nota fiscal, discriminando o quantitativo do produto, de acordo com as especificações técnicas;

h) Comunicar à Defensoria Pública do Estado do Tocantins, em até 24 (vinte e quatro) horas antecedentes ao prazo de vencimento da entrega, os motivos que impossibilite o seu cumprimento, caso haja;

i) Entregar as quantidades estipuladas no Nota de Empenho/Contrato no prazo de 60 (sessenta) dias corridos, conforme item 6, acompanhados da Nota Fiscal com as especificações estabelecidas neste Termo de Referência.

11. DAS SANÇÕES

11.1. A licitante ficará impedida de licitar e contratar com a União, Estados, Distrito Federal ou Município pelo prazo de até 05 (cinco) anos, sem prejuízo da multa de 20% do valor estimado/contratado e das

demais cominações legais, garantidos o contraditório e a ampla defesa, que deverá ser apresentada no prazo de 05 (cinco) dias úteis a contar da sua notificação, nos seguintes casos:

a) Não apresentar documentação exigida para o certame;

b) Apresentar documentação falsa;

c) Não assinar a ata de registro de Preços ou o Contrato dentro do prazo de validade da sua proposta;

d) Ensejar o retardamento da execução de seu objeto;

e) Não manter as condições ofertadas na proposta;

f) Falhar ou fraudar na execução do ajustado;

g) Comportar-se de modo inidôneo, nos termos da Lei;

h) Cometer fraude fiscal.

11.2. Pela inexecução total ou parcial das condições estabelecidas no instrumento convocatório, a Defensoria Pública do Estado do Tocantins poderá aplicar, sem prejuízo das responsabilidades penal e cível, as seguintes sanções:

a) Advertência, por escrito, quando o FORNECEDOR REGISTRADO/CONTRATADA deixar de atender quaisquer indicações aqui constantes;

b) Multa compensatória / indenizatória no percentual de até 20% (vinte por cento) calculado sobre o valor contratado;

c) Suspensão temporária de participação de licitação e impedimento de contratar com a Defensoria Pública do Estado do Tocantins, pelo prazo de até 02 (dois) anos;

d) Declaração de inidoneidade para licitar e contratar com Administração Pública enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação, na forma da Lei, perante a própria autoridade que aplicou a penalidade.

11.3. Na hipótese de atraso no cumprimento de quaisquer obrigações assumidas pelo FORNECEDOR REGISTRADO/CONTRATADA será aplicada multa moratória de 0,5% (zero vírgula cinco por cento) sobre o valor do contrato ou instrumento equivalente, por dia de atraso, limitada a 10 % (dez por cento) do valor inadimplido;

11.4. O valor da multa aplicada, tanto compensatória quanto moratória, deverá ser recolhida em conta da Defensoria Pública do Estado do Tocantins a ser indicada, dentro do prazo de 05 (cinco) dias úteis após a respectiva notificação;

11.5. Caso não seja paga na forma do subitem anterior, a multa será descontada por ocasião do pagamento posterior a ser efetuado ao FORNECEDOR REGISTRADO/CONTRATADA ou cobrada judicialmente;

11.6. Além das penalidades citadas, o FORNECEDOR REGISTRADO/CONTRATADA ficará sujeito, ainda, no que couber, às demais penalidades referidas no Capítulo IV da Lei n° 8.666/93;

11.7. Na aplicação de quaisquer sanções previstas, será garantido o contraditório e a ampla defesa.

Documento assinado eletronicamente por **Luiz Philipe Azevedo Dias**, **Diretor(a) de Tecnologia da Informação**, em 06/10/2022, às 15:05, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Joao Paulo Resende Fialho**, **Coordenador(a) de Redes**, em 06/10/2022, às 15:11, conforme art. 1º, III, "b", da Lei 11.419/2006.

ANEXO II-ATA DE REGISTRO DE PREÇO Nº ___/20__.

OBJETO: REGISTRO DE PREÇOS para eventual contratação de empresa fornecedora de *switches* gerenciáveis, cordões ópticos, *access points*, *sofware* de gerencia, serviços de instalação e treinamento especializados, para atender as necessidades da Defensoria Pública do Estado do Tocantins, conforme processo licitatório **22.0.000001581-8**, Pregão Eletrônico Nº __/20--.

Aos ___ dias do mês de _____ do ano de 20__, A **DEFENSORIA PÚBLICA DO ESTADO DO TOCANTINS**, com sede à Quadra 502 Sul, Av. Teotônio Segurado, s/nº, Plano Diretor Sul, CEP: 77.021-654, em Palmas-TO, inscrita no CNPJ/MF sob o nº. 07.248.660/0001-35, neste ato representada Subdefensor Público-Geral **Pedro Alexandre Conceição A. Gonçalves**, nomeado pelo **Ato nº 32 de 25 de janeiro de 2021**, publicado no **DOE 5.774, de 26/01/2021**, e no exercício das atribuições legais que lhe são conferidas por meio do **Ato nº 34/2021, publicado no Diário Oficial nº 5.777, de 29 de janeiro de 2021**, com alterações, doravante denominada simplesmente **ÓRGÃO GERENCIADOR** e a empresa _____, inscrita no CNPJ sob o nº _____, com sede _____, neste ato, representada pelo Sr. _____, (nacionalidade), (estado civil), (profissão), portador da Cédula de identidade RG _____- SSP/___, inscrito no CPF/MF sob o nº _____-__, residente e domiciliado na _____, e, daqui por diante, denominada simplesmente **FORNECEDOR REGISTRADO**, resolvem na forma da Lei 10.520, de 17 de julho de 2002, Decreto Federal 7.892/2013, Decreto Federal 10.024/2019, Decreto Federal 8.538/2015, Lei Complementar nº 123/2006 e subsidiariamente pela Lei nº 8.666, de 21 de junho de 1993 e suas alterações, firmar a presente **ATA DE REGISTRO DE PREÇOS**, cuja minuta foi examinada pela Assessoria Jurídica da Defensoria Pública, que emitiu seu parecer, conforme o parágrafo único do artigo 38 da Lei nº 8.666, de 1993, mediante as seguintes condições:

1. DO OBJETO

1.1. A presente Ata tem por objeto REGISTRO DE PREÇOS para eventual contratação de empresa fornecedora de *switches* gerenciáveis, cordões ópticos, *access points*, *sofware* de gerencia, serviços de instalação e treinamento especializados, para atender as necessidades da Defensoria Pública do Estado do Tocantins, nos quantitativos e especificações constantes no ANEXO I do Edital do **Pregão Eletrônico nº __/20--**.

2. DA VINCULAÇÃO AO EDITAL

2.1. Este instrumento guarda inteira conformidade com os termos do **Pregão Eletrônico nº ___/20-- para Registro de Preços,** e seus Anexos, Processo Licitatório nº **22.0.000001581-8**, do qual é parte integrante e complementar, vinculando-se, ainda, à proposta do Fornecedor Registrado.

3. DA VIGÊNCIA DA ATA

3.1. A presente Ata de Registro de Preços terá vigência de **12 (doze) meses**, a contar da data de publicação de seu extrato no Diário Oficial da Defensoria Pública do Estado do Tocantins

4. DO PREÇO

4.1. Os preços registrados e a indicação dos respectivos fornecedores detentores da Ata serão publicados

na imprensa oficial e divulgados em meio eletrônico.

4.2. A qualquer tempo, o preço registrado poderá ser revisto em decorrência de eventual redução daqueles existentes no mercado, cabendo ao Órgão Gerenciador convocar os Fornecedores registrados para negociar o novo valor.

4.2.1 Caso o Fornecedor registrado se recuse a baixar os seus preços, o Órgão Gerenciador poderá liberar o fornecedor do compromisso assumido, uma vez frustrada a negociação e convocar os demais fornecedores visando a igual oportunidade de negociação.

4.3. Durante o período de validade da Ata de Registro de Preços, os preços não serão reajustados, ressalvada a superveniência de normas federais aplicáveis à espécie.

5. DO CONTROLE DOS PREÇOS REGISTRADOS

5.1. O Órgão Gerenciador adotará a prática de todos os atos necessários ao controle e administração da presente Ata.

5.2 DO(S) PREÇO(S) REGISTRADO(S)

FORNECEDOR: (---) – CNPJ Nº (---)

GRUPO	ITEM	QTD	UND	DESCRIÇÃO	Valor	
					Unitário	Total
1	1	100	Und.	Switch de Acesso Tipo I		
	2	60	Und.	Switch de Acesso Tipo II		
	3	30	Und.	Switch de Acesso Tipo III		
	4	20	Und.	Switch de Acesso Tipo IV		
	5	20	Und.	Switch de Acesso Tipo V		
	6	2	Und.	Switch de Distribuição		
	7	80	Und.	Transceiver 1000BASE-X		
	8	60	Und.	Transceiver 10GBASE-X		
	9	232	Und.	Licenças Software de Gerência LAN		
	10	232	SERV	Serviço de instalação especializada LAN		
	11	1	SERV	Serviço de treinamento especializado LAN		

GRUPO	ITEM	QTD	UND	DESCRIÇÃO	VALOR	
					UNITÁRIO	TOTAL
2	12	80	UND	Access Point Indoor		
	13	6	UND	Access Point Outdoor		
	14	86	UND	Licenças Software de Gerência WLAN		
	15	86	SERV	Serviço de instalação especializada WLAN		
	16	1	SERV	Serviço de treinamento especializado WLAN		
TOTAL GRUPO 2						

ITEM	QTD	UND	DESCRIÇÃO	VALOR	
				UNITÁRIO	TOTAL
17	100	UND	Cordão Óptico 2 metros		

ITEM	QTD	UND	DESCRIÇÃO	VALOR	
				UNITÁRIO	TOTAL
18	20	UND	Cordão Óptico 20 metros		

6. DO CANCELAMENTO DO REGISTRO DE PREÇOS

6.1. O fornecedor registrado poderá ter o seu registro de preços cancelado mediante processo administrativo específico, assegurado o contraditório e a ampla defesa.

6.2. O cancelamento do seu registro poderá ser:

6.2.1. A pedido do próprio Fornecedor Registrado, quando comprovar estar impossibilitado de cumprir as exigências da Ata, por ocorrência de casos fortuitos ou de força maior;

6.2.2. Por iniciativa do Órgão Gerenciador, quando:

a) O fornecedor registrado não aceitar reduzir o preço registrado, na hipótese deste se tornar superior àqueles praticados no mercado:

b) O fornecedor registrado perder qualquer condição de habilitação ou qualificação técnica exigida no processo licitatório;

c) Por razões de interesse público, devidamente motivadas e justificadas;

d) O fornecedor registrado não cumprir as obrigações decorrentes da Ata de Registro de Preços;

e) O fornecedor registrado não comparecer ou se recusar a retirar, no prazo estabelecido, as solicitações decorrentes da Ata de Registro de Preços;

f) Caracterizada qualquer hipótese de inexecução total ou parcial das condições estabelecidas na Ata de Registro de Preços ou nas solicitações dela decorrentes.

6.3. Em qualquer das hipóteses acima, concluído o processo, o Órgão Gerenciador fará o devido apostilamento na Ata de Registro de Preços e informará aos proponentes a nova ordem de registro.

7. DA DIVULGAÇÃO DA ATA DE REGISTRO DE PREÇOS

7.1. A presente Ata será divulgada no portal da internet www.defensoria.to.def.br e terá seu extrato publicado no Diário Oficial da Defensoria Pública do Estado do Tocantins

8. DAS OBRIGAÇÕES DO FORNECEDOR REGISTRADO

8.1. São obrigações do licitante fornecedor:

a) Assinar a Ata de Registro de Preços em até 05 (cinco) dias úteis, contados da sua

notificação, conforme previsto no edital;

b) Assinar o contrato em até 05 (cinco) dias úteis, contados da sua notificação;

c) Não subcontratar o objeto da presente ata;

d) Manter, durante a vigência da ata de registro de preço, as condições de habilitação exigidas no Edital;

8.2 A contratação ora pretendida ocorrerá através da assinatura do instrumento contratual, momento em que a Contratada, obrigar-se-á:

a) Observar as Leis, Decretos, Regulamentos, Portarias e normas Federais, Estaduais e Municipais direta e indiretamente aplicáveis ao objeto licitado;

b) Indenizar quaisquer danos ou prejuízos causados a Defensoria Pública do Estado do Tocantins, ou a terceiros, por ação ou omissão no fornecimento do objeto;

c) Prestar as informações e os esclarecimentos solicitados pela Contratante, no prazo máximo de 48 (quarenta e oito) horas, contados da data do protocolo de recebimento da demanda;

d) Responsabilizar-se por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas na legislação específica, cuja inadimplência não transfere responsabilidade a esta Instituição;

e) Reparar o equipamento caso este venha a ser danificado, sem que haja quaisquer ônus para esta Instituição, em até 24 (vinte e quatro) horas contadas a partir do recebimento da solicitação. Em casos de necessidade de substituição de peças/equipamento terá até 15 (quinze) dias corridos contados a partir do recebimento da solicitação. O prazo poderá ser prorrogado por igual período, a critério da administração pública, quando requerida pela contratada, mediante justificativa apresentada dentro do prazo inicial;

f) Providenciar todos os recursos e insumos necessários à perfeita execução do objeto, devendo estar incluídas no preço proposto todas as despesas com materiais, insumos, mão-de-obra, fretes, embalagens, seguros, impostos, taxas, tarifas, encargos sociais e trabalhistas e demais despesas necessárias à perfeita entrega dos produtos;

g) Entregar os equipamentos, acondicionado adequadamente, em invólucro lacrado, de forma a permitir completa segurança durante o transporte, acompanhado de nota fiscal, discriminando o quantitativo do produto, de acordo com as especificações técnicas;

h) Comunicar à Defensoria Pública do Estado do Tocantins, em até 24 (vinte e quatro) horas antecedentes ao prazo de vencimento da entrega, os motivos que impossibilite o seu cumprimento, caso haja;

i) Entregar as quantidades estipuladas no Nota de Empenho/Contrato no prazo de 60 (sessenta) dias corridos, conforme item 6, acompanhados da Nota Fiscal com as especificações estabelecidas neste Termo de Referência.

9. DAS OBRIGAÇÕES DO ÓRGÃO GERENCIADOR

9.1. A Diretoria de Tecnologia da Informação da Defensoria Pública do Estado do Tocantins gerenciará a Ata de Registro de Preços.

9.2. São obrigações do órgão gerenciador:

a) Efetuar o registro do licitante fornecedor e firmar a correspondente Ata de Registro de Preços;

b) Designar servidor responsável pelo acompanhamento das despesas decorrentes do presente termo e para atestar o recebimento dos materiais/equipamentos, ou rejeitá-los no todo ou em parte;

c) Assegurar-se do fiel cumprimento das condições estabelecidas na ata, no instrumento convocatório e seus anexos, em relação às suas próprias contratações;

d) Aplicar as penalidades por descumprimento do pactuado na Ata de Registro de Preços, em relação às suas próprias contratações;

e) Responsabilizar-se pela observância quanto às leis, decretos, regulamentos, portarias e demais normas legais, direta e indiretamente aplicáveis à execução do objeto, em relação às suas próprias contratações.

10. DO PAGAMENTO

10.1. O pagamento ocorrerá no prazo de até 30 dias corridos contados após o recebimento da Nota Fiscal/Fatura, por meio de crédito em conta bancária, após efetiva emissão das notas fiscais e comprovação quanto à manutenção da regularidade fiscal e trabalhista, condicionado ao atesto do titular ou substituto responsável pela fiscalização do contrato.

10.2. O CNPJ constante da Nota Fiscal/Fatura deverá ser o mesmo indicado na nota de empenho, vinculado a conta corrente da CONTRATADA;

10.3. A DPE-TO reserva-se ao direito de não atestar a Nota Fiscal/Fatura para o pagamento, caso os dados constantes desta estiverem em desacordo com os dados da CONTRATANTE ou ainda, se os equipametnos ou serviços entregues não estiverem em conformidade com as especificações apresentadas neste Instrumento, ficando o pagamento suspenso até a regularização;

10.4. No caso de atraso de pagamento, desde que o contratado não tenha concorrido de alguma forma para tanto, serão devidos pela DPE encargos moratórios à taxa nominal de 6% a.a. (seis por cento ao ano), capitalizados diariamente em regime de juros simples.

11. DO PRAZO E LOCAL DA ENTREGA

11.1. Os equipamentos/licenças deverão ser entregues na Coordenação de Almoxarifado da DPE-TO, localizada na Quadra 903 Sul, Alameda 11, QI 05, Lote 09 Plano Diretor Sul – Palmas – TO, ou em outro local a ser informado previamente pela DPE-TO, nos seguintes horários: 08:00 às 11:30 e 14:00 às 16:30;

11.2. O prazo de entrega do objeto será de, no máximo 60 (sessenta) dias corridos, contados a partir da assinatura do contrato, podendo ser prorrogado caso haja pedido formal devidamente justificado pela CONTRATADA e acatado pela Defensoria Pública do Estado do Tocantins.

13. DAS SANÇÕES

13.1. A licitante ficará impedida de licitar e contratar com a União, Estados, Distrito Federal ou Município pelo prazo de até 05 (cinco) anos, sem prejuízo da multa de 20% do valor estimado/contratado e das demais cominações legais, garantidos o contraditório e a ampla defesa, que deverá ser apresentada no prazo de 05 (cinco) dias úteis a contar da sua notificação, nos seguintes casos:

a) Não apresentar documentação exigida para o certame;

b) Apresentar documentação falsa;

c) Não assinar a ata de registro de Preços ou o Contrato dentro do prazo de validade da sua proposta;

d) Ensejar o retardamento da execução de seu objeto;

e) Não manter as condições ofertadas na proposta;

f) Falhar ou fraudar na execução do ajustado;

g) Comportar-se de modo inidôneo, nos termos da Lei;

h) Cometer fraude fiscal.

13.2. Pela inexecução total ou parcial das condições estabelecidas no instrumento convocatório, a Defensoria Pública do Estado do Tocantins poderá aplicar, sem prejuízo das responsabilidades penal e cível, as seguintes sanções:

a) Advertência, por escrito, quando o FORNECEDOR REGISTRADO/CONTRATADA deixar de atender quaisquer indicações aqui constantes;

b) Multa compensatória / indenizatória no percentual de até 20% (vinte por cento) calculado sobre o valor contratado;

c) Suspensão temporária de participação de licitação e impedimento de contratar com a Defensoria Pública do Estado do Tocantins, pelo prazo de até 02 (dois) anos;

d) Declaração de inidoneidade para licitar e contratar com Administração Pública enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação, na forma da Lei, perante a própria autoridade que aplicou a penalidade.

13.3. Na hipótese de atraso no cumprimento de quaisquer obrigações assumidas pelo FORNECEDOR REGISTRADO/CONTRATADA será aplicada multa moratória de 0,5% (zero vírgula cinco por cento) sobre o valor do contrato ou instrumento equivalente, por dia de atraso, limitada a 10 % (dez por cento) do valor inadimplido;

13.4. O valor da multa aplicada, tanto compensatória quanto moratória, deverá ser recolhida em conta da Defensoria Pública do Estado do Tocantins a ser indicada, dentro do prazo de 05 (cinco) dias úteis após a respectiva notificação;

13.5. Caso não seja paga na forma do subitem anterior, a multa será descontada por ocasião do pagamento posterior a ser efetuado ao FORNECEDOR REGISTRADO/CONTRATADA ou cobrada judicialmente;

13.6. Além das penalidades citadas, o FORNECEDOR REGISTRADO/CONTRATADA ficará sujeito, ainda, no que couber, às demais penalidades referidas no Capítulo IV da Lei n° 8.666/93;

13.7. Na aplicação de quaisquer sanções previstas, será garantido o contraditório e a ampla defesa.

14. DA ADESÃO À ATA DE REGISTRO DE PREÇOS

14.1. Caberá ao órgão aderente à Ata de Registro de Preços verificar junto ao Fornecedor Registrado a capacidade de fornecimento dos objetos registrados, bem como consultar o Órgão Gerenciador sobre a sua anuência.

14.2. Caberá ao Fornecedor Registrado beneficiário da Ata de Registro de Preços, observadas as condições estabelecidas, optar pela aceitação ou não do fornecimento dos objetos decorrente de adesão, desde que não prejudique as obrigações presentes e futuras decorrentes da Ata, assumidas com o Órgão Gerenciador.

14.3. Os fornecimentos adicionais não poderão exceder, na totalidade, **ao dobro do quantitativo de cada item registrado** para o Órgão Gerenciador.

14.4. Para fins de autorização, só serão aceitos pedidos de adesões que não excedam, por órgão ou entidade solicitante, **a cinquenta por cento dos quantitativos dos itens registrados**.

14.5. Após a autorização do Órgão Gerenciador, o órgão não participante deverá efetivar a contratação solicitada em até noventa dias, observado o prazo de vigência da Ata.

14.6. Compete ao órgão, não participante, os atos relativos à cobrança do cumprimento pelo Fornecedor Registrado das obrigações contratualmente assumidas e a aplicação, observada a ampla defesa e o contraditório, de eventuais penalidades decorrentes do descumprimento de cláusulas contratuais, em relação às suas próprias contratações, informando as ocorrências ao Órgão Gerenciador.

15. DAS DISPOSIÇÕES GERAIS

15.1. Independente de sua transcrição, o edital e seus anexos, principalmente a proposta de preço e os documentos da proposta e da habilitação apresentados pelo Fornecedor Registrado no pregão farão parte

desta Ata de Registro de Preços.

15.2. Não será concedido reajuste ou correção monetária do valor da ata.

15.3. Fica assegurado o restabelecimento do equilíbrio econômico-financeiro inicial da ata, na ocorrência de fato superveniente que implique a inviabilidade de sua execução.

16. DO FORO

16.1. Para dirimir, na esfera judicial, às questões oriundas da presente Ata de Registro de Preços será competente o foro da Comarca de Palmas, Capital do Estado do Tocantins.

E para firmeza e como prova de assim haverem, entre si, ajustado, foi lavrada a presente ata de registro de preços que, lida e achada conforme, é assinada pelos signatários deste instrumento.

Palmas, ... de ..... de 20__.

DEFENSORIA PÚBLICA DO ESTADO DO TOCANTINS

PEDRO ALEXANDRE CONCEIÇÃO A. GONÇALVES

SUBDEFENSOR PÚBLICO-GERAL

FORNECEDOR REGISTRADO

ANEXO III - MINUTA DO CONTRATO

Processo Eletrônico SEI nº 22.0.000001581-8.

Contrato nº ___ / ____.

CONTRATO QUE ENTRE SI CELEBRAM A DEFENSORIA PUBLICA DO ESTADO DO TOCANTINS E A EMPRESA _____.

A DEFENSORIA PÚBLICA DO ESTADO DO TOCANTINS, Pessoa Jurídica de Direito Público Interno, com sede na Quadra 502 Sul, Avenida Teotônio Segurado, S/N, Plano Diretor Sul, Palmas - TO, inscrita no CNPJ sob o nº. 07.248.660/0001-35, doravante denominada **CONTRATANTE**, ou simplesmente **DPE-TO**, neste ato representada pelo Subdefensor Público-Geral no uso das atribuições legais que lhe são conferidas pelo Ato nº 034 de 25 de janeiro de 2021, publicado no DOE 5.777 de 29 de janeiro de 2021, **PEDRO ALEXANDRE CONCEIÇÃO AIRES GONÇALVES,** brasileiro, portador do RG. nº 4603598-2 DGPC- GO e do CPF/MF nº. 009.286.711-19, residente e domiciliado nesta capital, nomeado pelo Ato nº 032, de 25 de janeiro de 2021, publicado no DOE 5.774 de 26/01/2021 e a empresa _____**,** CNPJ sob o nº _____ /___, com endereço _____, Telefone: (DDD) _____, e-mail _____, doravante designada **CONTRATADA,** neste ato representada pelo(a) Sr.(a) _____, portador(a) da Cédula de Identidade nº _____, e inscrito(a) no CPF sob o nº _____, de acordo com a representação legal que lhe é outorgada por _____, tendo em vista o que consta no Processo Eletrônico - SEI nº 22.0.000001581-8, e em observância às disposições da Lei 10.520, de 17 de julho de 2002, Decreto Federal 7.892/2013, Decreto Federal 10.024/2019, Decreto Federal 8.538/2015, Lei Complementar nº 123/2006 e subsidiariamente pela Lei nº 8.666, de 21 de junho de 1993, e suas alterações, resolvem celebrar o presente

Termo de Contrato, decorrente do Pregão Eletrônico nº _____/20__ e Ata de Registro de Preços nº _____/20__, mediante as cláusulas e condições a seguir enunciadas.

CLÁUSULA PRIMEIRA – DO OBJETO

1.1. Contratação de empresa fornecedora de *switches* gerenciáveis, cordões ópticos, *access points*, *sofware* de gerencia, serviços de instalação e treinamento especializados, para atender as necessidades da Defensoria Pública do Estado do Tocantins.

CLÁUSULA SEGUNDA - DAS ESPECIFICAÇÕES, DAS QUANTIDADES E DOS VALORES ESTIMADOS

2.1. O Objeto deste Contrato será adquirido, conforme especificações e quantitativos descritos abaixo:

GRUPO	ITEM	QTD	UND	DESCRIÇÃO	Valor Unit. (R$)	Valor Total (R$)

2.2. Switch de Acesso Tipo I

2.2.1. As características e exigências técnicas do produto são as constantes na Proposta da Contratada e no Termo de Referência anexo ao edital do Pregão Eletrônico nº ___.

2.3. Switch de Acesso Tipo II

2.3.1. As características e exigências técnicas do produto são as constantes na Proposta da Contratada e no Termo de Referência anexo ao edital do Pregão Eletrônico nº ___.

2.4. Switch de Acesso Tipo III

2.4.1. As características e exigências técnicas do produto são as constantes na Proposta da Contratada e no Termo de Referência anexo ao edital do Pregão Eletrônico nº ___.

2.5. Switch de Acesso Tipo IV

2.5.1. As características e exigências técnicas do produto são as constantes na Proposta da Contratada e no Termo de Referência anexo ao edital do Pregão Eletrônico nº ___.

2.6. Switch de Acesso Tipo V

2.6.1. As características e exigências técnicas do produto são as constantes na Proposta da Contratada e no Termo de Referência anexo ao edital do Pregão Eletrônico nº ___.

2.7. Switch de Distribuição

2.7.1. As características e exigências técnicas do produto são as constantes na Proposta da Contratada e no Termo de Referência anexo ao edital do Pregão Eletrônico nº ___.

2.8. Da Garantia

2.8.1. Os itens _____ deverão ter garantia de ____ ( ) meses do fabricante ou da revenda, desde que essa seja autorizada por carta pelo fabricante dos equipamentos a prestar o suporte e garantia, pelo período de ____ ( ) meses. A garantia do item _____ deverá ser do tipo NBD com troca de equipamentos em caso de falha;

2.9. Transceiver 1000BASE-X

2.9.1. As características e exigências técnicas do produto são as constantes na Proposta da Contratada e no Termo de Referência anexo ao edital do Pregão Eletrônico nº ___.

2.10. Transceiver 10GBASE-X

2.10.1. As características e exigências técnicas do produto são as constantes na Proposta da Contratada e no Termo de Referência anexo ao edital do Pregão Eletrônico nº ___.

2.11. Serviço de instalação especializada - LAN

2.11.1. Ocorrerá por conta da CONTRATADA toda e qualquer despesa, independentemente da sua natureza, decorrente dos serviços de instalação e configuração aqui mencionados. Cada unidade de serviço deverá contemplar instalação e configuração de um equipamento, considerando a ativação dele junto a plataforma de gerência e sua configuração básica;

2.11.2. Será realizada uma conferência de planejamento antes do início das atividades com o ponto de

contato da CONTRATANTE para apresentar os principais participantes, confirmar a disponibilidade do local e outros pré-requisitos, além de discutir a logística de entrega do serviço;

2.11.3. Após o recebimento da solução (hardware/software), a CONTRATANTE deverá definir juntamente com a CONTRATADA o cronograma de instalação e configuração da mesma, enviando à CONTRATADA, documento contendo informações de Data, Hora, Local, e equipamentos a serem instalados;

2.11.4. No cronograma de instalação poderão ser definidos períodos fora do horário comercial, assim como finais de semana e feriados;

2.11.5. Será agendada uma reunião de kick-off com os times envolvidos para confirmar o escopo do projeto, identificar responsabilidades, riscos e pré-requisitos;

2.11.6. Será realizado o levantamento do ambiente atual, validando as premissas adotadas na elaboração desta proposta de serviço;

2.11.7. Ocorrerá a confirmação do pleno funcionamento da infraestrutura a ser utilizada no projeto (Rede, Servidores, Storage, por exemplo);

2.11.8. Será validado todo o licenciamento adquirido pelo CONTRATANTE relacionado aos produtos que serão instalados e configurados;

2.11.9. O processo de instalação/configuração deverá ter início em no máximo 30 (trinta) dias após a entrega dos equipamentos. Prazo este que poderá ser prorrogado de acordo com interesse da CONTRATANTE;

2.11.10. A CONTRATADA deverá realizar a instalação física e lógica “assistida” de todos os componentes de hardware e software, contemplados pelo escopo deste serviço, sob a supervisão dos técnicos da CONTRATANTE;

2.11.11. A CONTRATANTE deve acompanhar toda a atividade a ser realizada na janela de implantação;

2.11.12. Todo pessoal e ferramentas necessárias para execução dos serviços de instalação e configuração incluindo equipamentos ou ferramentas, bem como eventuais materiais necessários para ligações temporárias, são de inteira responsabilidade da empresa CONTRATADA;

2.11.13. Escopo dos Serviços a Serem Realizados:

2.11.13.1. Realizar a instalação do OS dos Switches a serem instalados no ambiente da CONTRATANTE;

2.11.13.2. Realizar a instalação do Software de Gerência de Rede a ser instalados no ambiente da CONTRATANTE;

2.11.13.3. Executar os testes necessários para validação da atualização, atestando o funcionamento adequado;

2.11.13.4. Configuração de VLANs, ACL, Malha ethernet e entre outros serviços relacionados ao funcionamento dos novos equipamentos na rede da CONTRATANTE;

2.12. Serviço de treinamento especializado - LAN

2.12.1. O Treinamento terá carga horária de ____ (____) horas e será realizado em Palmas/TO de forma presencial, ou de forma remota a critério da DPE-TO, com emissão de certificados de participação, para _____ (_____) servidores da DPE-TO;

2.12.2. Conteúdo do treinamento será organizado em módulos, incluirá material didático digital e abrangerá funcionalidades dos switches e softwares de gerência de rede descritos no termo de referência e proposta da

contratada.

2.13. Access Point Indoor

2.13.1. As características e exigências técnicas do produto serão conforme a Proposta da Contratada e o Termo de Referência.

2.14. Access Point Outdoor

2.14.1. As características e exigências técnicas do produto serão conforme a Proposta da Contratada e o Termo de Referência.

2.15. Serviço de instalação especializada - WLAN

2.15.1. Ocorrera por conta da CONTRATADA toda e qualquer despesa, independentemente da sua natureza, decorrente dos serviços de instalação e configuração aqui mencionados. Cada unidade de serviço deverá contemplar instalação e configuração de um equipamento, considerando a ativação dele junto a plataforma de gerência e sua configuração básica;

2.15.2. Será realizada uma conferência de planejamento antes do início das atividades com o ponto de contato da CONTRATANTE para apresentar os principais participantes, confirmar a disponibilidade do local e outros pré-requisitos, além de discutir a logística de entrega do serviço;

2.15.3. Após o recebimento da solução (hardware/software), a CONTRATANTE deverá definir juntamente com a CONTRATADA o cronograma de instalação e configuração da mesma, enviando à CONTRATADA, documento contendo informações de Data, Hora, Local, e equipamentos a serem instalados;

2.15.4. No cronograma de instalação poderão ser definidos períodos fora do horário comercial, assim como finais de semana e feriados

2.15.5. Será agendada uma reunião de kick-off com os times envolvidos para confirmar o escopo do projeto, identificar responsabilidades, riscos e pré-requisitos;

2.15.6. Será realizado o levantamento do ambiente atual, validando as premissas adotadas na elaboração desta proposta de serviço;

2.15.7. Ocorrera a confirmação do pleno funcionamento da infraestrutura a ser utilizada no projeto (Rede, Servidores, Storage, Access Points, por exemplo);

3.15.8. Será validado todo o licenciamento adquirido pelo CONTRATANTE relacionado aos produtos que serão instalados e configurados;

2.15.9. O processo de instalação/configuração deverá ter início em no máximo 30 (trinta) dias após a entrega dos equipamentos. Prazo este que poderá ser prorrogado de acordo com interesse da CONTRATANTE;

2.15.10. A CONTRATADA deverá realizar a instalação física e lógica “assistida” de todos os componentes de hardware e software, contemplados pelo escopo deste serviço, sob a supervisão dos técnicos da CONTRATANTE;

2.15.11. A CONTRATANTE deve acompanhar toda a atividade a ser realizada na janela de implantação;

2.15.12. Todo pessoal e ferramentas necessárias para execução dos serviços de instalação e configuração

incluindo equipamentos ou ferramentas, bem como eventuais materiais necessários para ligações temporárias, são de inteira responsabilidade da empresa CONTRATADA;

2.15.13. Escopo dos Serviços a Serem Realizados:

2.15.14. Realizar a instalação do OS dos Access Points a serem instalados no ambiente da CONTRATANTE;

2.15.15. Realizar a instalação do Software de Gerência WLAN a ser instalados no ambiente da CONTRATANTE;

2.15.16. Executar os testes necessários para validação da atualização, atestando o funcionamento adequado;

2.15.17. Configuração de serviços relacionados ao funcionamento dos equipamentos Wi-Fi na rede da CONTRATANTE;

2.16. Serviço de treinamento especializado - WLAN

2.16.1. O Treinamento terá carga horária de ____ (____) horas e será realizado em Palmas/TO de forma presencial, ou de forma remota a critério da DPE-TO, com emissão de certificados de participação, para _____ (_____) servidores da DPE-TO;

2.16.2. Conteúdo do treinamento será organizado em módulos, incluirá material didático digital e abrangerá funcionalidades dos switches e softwares de gerência de rede descritos no termo de referência e proposta da contratada.

CLÁUSULA TERCEIRA – DO VALOR

3.1. O valor do presente contrato é de R$ **_____** (_____), em conformidade com a Ata de Registro de Preços nº _____.

CLÁUSULA QUARTA – DO PAGAMENTO

4.1. O pagamento ocorrerá no prazo de até 30 (trinta) dias corridos contados após o recebimento da Nota Fiscal/Fatura, por meio de crédito em conta bancária, após efetiva emissão das notas fiscais e comprovação quanto à manutenção da regularidade fiscal e trabalhista, condicionado ao atesto do titular ou substituto responsável pela fiscalização do contrato;

4.2. O CNPJ constante da nota fiscal/fatura deverá ser o mesmo indicado na nota de empenho, vinculado à conta corrente da CONTRATADA;

4.3. A Defensoria Pública do Estado do Tocantins reserva-se ao direito de não atestar a nota fiscal/fatura para o pagamento, caso os dados constantes desta estiverem em desacordo com os dados da CONTRATANTE, ou ainda, se os equipamentos ou serviços entregues não estiverem em conformidade com as especificações apresentadas neste Instrumento, ficando o pagamento suspenso até a regularização;

4.4. No caso de atraso de pagamento, desde que o contratado não tenha concorrido de alguma forma para tanto, serão devidos pela DPE encargos moratórios à taxa nominal de 6% a.a. (seis por cento ao ano), capitalizados diariamente em regime de juros simples.

CLÁUSULA QUINTA – DA DOTAÇÃO ORÇAMENTÁRIA

5.1. A despesa com a presente contratação correrá à conta da Dotação Orçamentária _____, Elemento de despesa _____, Subitem _____, Fonte _____, conforme juntado aos autos sob Código verificador nº _____.

CLÁUSULA SEXTA – DO PRAZOS E LOCAL DE ENTREGA

6.1. Os equipamentos/licenças deverão ser entregues na Coordenação de Almoxarifado da DPE-TO, localizada na Quadra 903 Sul, Alameda 11, QI 05, Lote 09 Plano Diretor Sul – Palmas – TO, ou em outro local a ser informado previamente pela DPE-TO, nos seguintes horários: 08:00 às 11:30 e 14:00 às 16:30;

6.2. O prazo de entrega do objeto será de, no máximo 60 (sessenta) dias corridos, contados a partir da assinatura do contrato, podendo ser prorrogado caso haja pedido formal devidamente justificado pela CONTRATADA e acatado pela Defensoria Pública do Estado do Tocantins.

CLÁUSULA SÉTIMA – DAS OBRIGAÇÕES DA CONTRATADA

7.1. Não subcontratar o objeto do presente Contrato;

7.2. Manter, durante a vigência do Contrato, as condições de habilitação exigidas no Edital;

7.3. Observar as Leis, Decretos, Regulamentos, Portarias e normas Federais, Estaduais e Municipais direta e indiretamente aplicáveis ao objeto contratado;

7.4. Indenizar quaisquer danos ou prejuízos causados a Defensoria Pública do Estado do Tocantins, ou a terceiros, por ação ou omissão na prestação dos serviços;

7.5. Responsabilizar-se por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas na legislação específica, cuja inadimplência não transfere responsabilidade a Defensoria Pública do Estado do Tocantins;

7.6. Prestar as informações e os esclarecimentos solicitados pela Contratante, no prazo máximo de 48 (quarenta e oito) horas, contados da data do protocolo de recebimento da demanda;

7.7. Providenciar todos os recursos e insumos necessários à prestação dos serviços, estando incluídas no preço estabelecidos todas as despesas com materiais, insumos, mão de obra, fretes, embalagens, seguros, impostos, taxas, tarifas, encargos sociais e trabalhistas e demais despesas necessárias à perfeita execução do objeto;

7.8. Reparar o equipamento caso este venha a ser danificado, sem que haja quaisquer ônus para esta Instituição, em até 24 (vinte e quatro) horas contadas a partir do recebimento da solicitação. Em casos de necessidade de substituição de peças/equipamento terá até 15 (quinze) dias corridos contados a partir do recebimento da solicitação. O prazo poderá ser prorrogado por igual período, a critério da administração pública, quando requerida pela contratada, mediante justificativa apresentada dentro do prazo inicial;

7.9. Entregar os equipamentos, acondicionado adequadamente, em invólucro lacrado, de forma a permitir completa segurança durante o transporte, acompanhado de nota fiscal, discriminando o quantitativo do produto, de acordo com as especificações técnicas;

7.10. Comunicar à Defensoria Pública do Estado do Tocantins, em até 24 (vinte e quatro) horas antecedentes ao prazo de vencimento da entrega, os motivos que impossibilite o seu cumprimento, caso haja;

7.11. Entregar as quantidades estipuladas no Nota de Empenho/Contrato no prazo de 60 (sessenta) dias corridos, conforme item 6, acompanhados da Nota Fiscal com as especificações estabelecidas neste Contrato.

CLÁUSULA OITAVA - DAS OBRIGAÇÕES DA CONTRATANTE

8.1. Designar servidor responsável pelo acompanhamento das despesas decorrentes do presente termo e para atestar os serviços prestados, ou rejeitá-los no todo ou em parte;

8.2. Assegurar-se do fiel cumprimento das condições estabelecidas neste Contrato, no instrumento convocatório e seus anexos;

8.3. Aplicar penalidades por descumprimento do pactuado neste Contrato;

8.4. Responsabilizar-se pela observância quanto às leis, decretos, regulamentos, portarias e demais normas legais, direta e indiretamente aplicáveis a execução do objeto;

CLÁUSULA NONA - CASOS DE RESCISÃO

9.1. A inexecução total ou parcial deste contrato por parte da contratada assegurará à contratante o direito de rescisão nos termos do artigo 77 da Lei nº 8.666/93, de 21 de junho de 1993 e suas alterações, bem como nos casos citados no artigo 78 da mesma lei, garantida a prévia defesa sempre mediante notificação por escrito.

9.2. A rescisão também se submeterá ao regime previsto no artigo 79, seus incisos e parágrafos, da Lei nº 8.666/93 e suas alterações.

CLÁUSULA DÉCIMA - DAS SANÇÕES ADMINISTRATIVAS

10.1. A empresa ficará impedida de licitar e contratar com a União, Estados, Distrito Federal ou Município pelo prazo de até 05 (cinco) anos, sem prejuízo das multas previstas neste Contrato e das demais cominações legais, garantidos o contraditório e a ampla defesa, que deverá ser apresentada no prazo de 05 (cinco) dias úteis a contar da sua notificação, nos seguintes casos:

10.1.1. Apresentar documentação falsa;

10.1.2. Ensejar o retardamento da execução de seu objeto;

10.1.3. Não manter as condições ofertadas em sua proposta;

10.1.4. Falhar ou fraudar na execução do ajustado;

10.1.5. Comportar-se de modo inidôneo, nos termos da Lei;

10.1.6. Cometer fraude fiscal.

10.2. Pela inexecução total ou parcial das condições estabelecidas neste instrumento contratual, a Contratante poderá aplicar, sem prejuízo das responsabilidades penal e cível, as seguintes sanções:

10.2.1. Advertência, por escrito, quando a Contratada deixar de atender quaisquer indicações aqui constantes;

10.2.2. Multa compensatória / indenizatória no percentual de até 20% (vinte por cento) calculado sobre o valor Contratado;

10.2.3. Suspensão temporária de participação de licitação e impedimento de contratar com a Defensoria Pública do Estado do Tocantins, pelo prazo de até 02 (dois) anos;

10.2.4. Declaração de inidoneidade para licitar e contratar com Administração Pública enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação, na forma da Lei, perante a própria autoridade que aplicou a penalidade;

10.3. Na hipótese de atraso no cumprimento de quaisquer obrigações assumidas pela Contratada, será aplicada multa moratória de 0,5% (zero vírgula cinco por cento) sobre o valor contratado, por dia de atraso, limitada a 10 % (dez por cento) desse valor;

10.4. O valor da multa aplicada, tanto compensatória quanto moratória, deverá ser recolhido em conta da DPE-TO a ser indicada, dentro do prazo de 05 (cinco) dias úteis após a respectiva notificação;

10.4.1. Caso não seja paga na forma do subitem anterior, a multa será descontada por ocasião do pagamento posterior a ser efetuado pela Contratante ou cobrada judicialmente;

10.5. Além das penalidades citadas, a Contratada ficará sujeita, ainda, no que couber, as demais penalidades referidas no Capítulo IV da Lei n.° 8.666/93;

10.6. Na aplicação de quaisquer sanções previstas, será garantido o contraditório e a ampla defesa.

CLÁUSULA DÉCIMA PRIMEIRA – DA VINCULAÇÃO AO INSTRUMENTO CONVOCATÓRIO

11.1. O presente Contrato vincula-se ao Edital e anexos do Pregão Eletrônico nº ____/20___, constante sob código verificador nº _____, Processo Licitatório nº _____, como se aqui estivessem transcritos, vinculando-se, ainda, à proposta da Contratada.

CLÁUSULA DÉCIMA SEGUNDA - DA FUNDAMENTAÇÃO LEGAL

12.1. O presente instrumento de Contrato rege-se pela Lei 10.520, de 17 de julho de 2002, Decreto Federal 7.892/2013, Decreto Federal 10.024/2019, Decreto Federal 8.538/2015, Lei Complementar nº 123/2006 e subsidiariamente pela Lei nº 8.666, de 21 de junho de 1993 e suas alterações, além das demais normas pertinentes.

CLÁUSULA DÉCIMA TERCEIRA - DOS ACRÉSCIMOS E SUPRESSÕES

13.1. O valor inicial atualizado do Contrato poderá ser acrescido ou suprimido dentro dos limites previstos no §1º do art. 65 da Lei nº 8.666/93, podendo a supressão exceder tal limite, nos termos do §2º do inciso II do mesmo artigo, conforme redação introduzida pela Lei nº 9.648 de 27 de maio de 1998.

CLÁUSULA DÉCIMA QUARTA - DA VIGÊNCIA

14.1 A vigência do Contrato será de 12 (doze) meses, a contar de sua assinatura.

14.2. Considerando que as assinaturas do presente instrumento ocorrerão por meio eletrônico e poderão ser realizadas em datas distintas, o prazo a que se refere o caput desta cláusula, se iniciará a partir da data da assinatura da Contratante.

CLÁUSULA DÉCIMA QUINTA - DA PUBLICIDADE

15.1. O extrato do presente Contrato será publicado no Diário Oficial Eletrônico da Defensoria Pública do Estado do Tocantins, conforme Legislação aplicável.

CLÁUSULA DÉCIMA SEXTA – DA FISCALIZAÇÃO DO CONTRATO

16.1. Nos termos do art. 67, § 1°, da Lei n° 8.666, de 1993, a Contratante designará um representante para acompanhar e fiscalizar a execução do Contrato, anotando em registro próprio todas as ocorrências e determinando o que for necessário à regularização das falhas ou defeitos observados.

16.2. Ao Fiscal do Contrato compete, entre outras atribuições:

16.2.1. Fiscalizar a execução do objeto, objetivando garantir a qualidade desejada;

16.2.2. Solicitar e/ou sugerir à Comissão de Penalidade à aplicação de sanção por descumprimento de cláusula contratual, após tentativas frustradas de solucionar o problema;

16.2.3. Acompanhar e atestar a execução do objeto, indicando as eventuais ocorrências;

16.2.4. Atestar e encaminhar a Nota Fiscal ao Setor competente para autorização de pagamento;

16.3. A instituição e a atuação da fiscalização do objeto do contrato não excluem ou atenuam a responsabilidade da Contratada, nem a exime de manter fiscalização própria.

CLÁUSULA DÉCIMA SÉTIMA – DOS ANEXOS

17.1. Integram este Contrato, como anexo, a cópia da proposta apresentada pela Contratada (Código Verificador nº _____), Termo de Referência (Código Verificador _____), Autorização de Compras (Código Verificador nº _____), e a Ata de Registro de Preços nº ____/_____, (Código Verificador _____), das quais os signatários declaram ciência.

CLÁUSULA DÉCIMA OITAVA– DAS DISPOSIÇÕES GERAIS

18.1. O presente instrumento será firmado através de sistema de assinatura eletrônica, certificada pelo SEI - Sistema Eletrônico de Informações da Defensoria Pública do Estado do Tocantins, garantida a eficácia das Cláusulas cujo compromisso é assumido;

18.2. As comunicações, solicitações, notificações ou intimações da Administração decorrentes deste Contrato, serão feitas pessoalmente, publicadas no Diário Oficial Eletrônico da Defensoria Pública do Estado do Tocantins ou encaminhadas via correios ou e-mail para o endereço eletrônico indicado pela Contratada na documentação/proposta apresentada, considerando-se recebida pelo destinatário/interessado, para todos os efeitos legais, na data do recebimento, da publicação, ou do envio da mensagem eletrônica;

18.3. Fica expressamente vedada à vinculação deste Contrato em operação de qualquer natureza que a CONTRATADA tenha ou venha a assumir.

CLÁUSULA DÉCIMA NONA - DO FORO

19.1. Na forma do disposto do artigo 55, § 2º da Lei 8.666/93, fica eleito o foro da Comarca de Palmas, Capital do Estado do Tocantins, para dirimir quaisquer questões oriundas deste Contrato.

CLÁUSULA VIGÉSIMA - DA ASSINATURA

20.1. Por estarem de acordo, lavrou-se o presente termo, o qual, depois de lido, será assinado eletronicamente nos termos da Lei 11.419/2006, pelos representantes das partes, CONTRATANTE e CONTRATADA, através do Sistema Eletrônico de Informações - SEI.

Palmas/TO, __ de _____ de 20__.

CONTRATANTE **Defensoria Pública do Estado do Tocantins** Pedro Alexandre Conceição Aires Gonçalves Subdefensor Público-Geral	**CONTRATADA** Empresa Representante Legal

---

Documento assinado eletronicamente por **RENATA NEGREIROS GAMA CRUVINEL**, **Anagesp - Administração**, em 26/09/2022, às 16:34, conforme art. 1º, III, "b", da Lei 11.419/2006.

ANEXO – IV

MODELO DE PROPOSTA READEQUADA

Processo Interno: ---

Pregão Eletrônico nº --/20--.

Empresa: [Nome da Empresa]

CNPJ: [CNPJ da empresa]

Conta corrente: [Titularidade da empresa]

Endereço: [Endereço da empresa]

Telefone: [Telefone da empresa]

E-mail: [Endereço eletrônico da empresa]

Em atendimento ao Edital do Pregão Eletrônico n.º __/20__ e seus Anexos, apresentamos proposta no valor total de R$ ___ ___ __ [valor por extenso], conforme tabela abaixo:

GRUPO	ITEM	QTD	UND	DESCRIÇÃO	VALOR	
					UNITÁRIO	TOTAL
1	1	100	UND	Switch de Acesso Tipo I		
	2	60	UND	Switch de Acesso Tipo II		
	3	30	UND	Switch de Acesso Tipo III		
	4	20	UND	Switch de Acesso Tipo IV		
	5	20	UND	Switch de Acesso Tipo V		
	6	2	UND	Switch de Distribuição		
	7	80	UND	Transceiver 1000BASE-X		
	8	60	UND	Transceiver 10GBASE-X		
	9	232	UND	Licenças Software de Gerência LAN		
	10	232	SERV	Serviço de instalação especializada LAN		
	11	1	SERV	Serviço de treinamento especializado LAN		
TOTAL GRUPO 1						

GRUPO	ITEM	QTD	UND	DESCRIÇÃO	VALOR	
					UNITÁRIO	TOTAL
2	12	80	UND	Access Point Indoor		
	13	6	UND	Access Point Outdoor		
	14	86	UND	Licenças Software de Gerência WLAN		
	15	86	SERV	Serviço de instalação especializada WLAN		
	16	1	SERV	Serviço de treinamento especializado WLAN		
TOTAL GRUPO 2						

ITEM	QTD	UND	DESCRIÇÃO	VALOR	
				UNITÁRIO	TOTAL
17	100	UND	Cordão Óptico 2 metros		

ITEM	QTD	UND	DESCRIÇÃO	VALOR	
				UNITÁRIO	TOTAL
18	20	UND	Cordão Óptico 20 metros		

Local e data

_____

Assinatura e carimbo

(Responsável da empresa)

Observações:

1. A licitante deverá ajustar a tabela acima de acordo com o(s) Item(ns) para o(s) qual(is) está apresentando a proposta.
2. Emitir em papel que identifique a licitante.