MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DE ALFENAS - UNIFAL-MG
SETOR DE COMPRAS
Rua Gabriel Monteiro da Silva, 700 - Alfenas/MG - CEP 37130-000.
Fone: (35) 3299-1072/1070 - Fax: (35) 3299-1071 - pregao@unifal-mg.edu.br

EDITAL DE LICITAÇÃO
PREGÃO ELETRÔNICO Nº 110/2015
SISTEMA DE REGISTRO DE PREÇOS
PROCESSO Nº 23087.010345/2015-59

1. PREÂMBULO

1.1. A Universidade Federal de Alfenas – UNIFAL-MG, Autarquia de Regime Especial, "ex vi" da Lei nº 11.154, de 29 de julho de 2005, com sede na cidade de Alfenas, na Rua Gabriel Monteiro da Silva, 700, Centro, torna público, para conhecimento dos interessados, que se encontra aberta a Licitação por **PREGÃO ELETRÔNICO nº 110/2015, no SISTEMA DE REGISTRO DE PREÇOS, do tipo MENOR PREÇO UNITÁRIO POR ITEM,** observadas as disposições da Lei nº 10.520 de 17/07/2002, Lei Complementar 123 de 14/12/2006, Lei 11.488, de 15/06/2007, da Lei Complementar 147 de 07 de agosto de 2014, do Decreto nº 5.450 de 31/05/2005, do Decreto nº 6.204 de 05/09/2007 e do Decreto nº 7.892 de 23/01/2013, **Decreto nº 7.174 de 12 de maio de 2010, Decreto 7.546, de 02 de agosto de 2011, Decreto 7.903, de 04 de fevereiro de 2013, Decreto nº 8.186 de 17 de janeiro de 2014, Decreto 8.194, de 12 de fevereiro de 2014,** da Instrução Normativa nº 01, da SLTI/MPOG, de 19/01/2010, da Instrução Normativa nº 02, da SLTI/MPOG, de 16/09/2009, da Instrução Normativa nº 05, da SLTI/MPOG, de 27/06/2014 e da Lei nº 8.666 de 21/06/1993 em sua redação atual e, ainda as condições estipuladas neste Edital.

1.2. Órgão Gerenciador: órgão ou entidade da administração pública federal responsável pela condução do conjunto de procedimentos para registro de preços e gerenciamento da ata de registro de preços dele decorrente.

1.2.1. Universidade Federal de Alfenas – UNIFAL-MG, UASG 153028, Rua Gabriel Monteiro da Silva, 700, Centro, Alfenas – MG, CEP 37130-000.

1.3. Órgão Participante: órgão ou entidade da administração pública federal que participa dos procedimentos iniciais do Sistema de Registro de Preços e integra a ata de registro de preços.

2. OBJETO

2.1. Implantação do **Sistema de Registro de Preços** para possível aquisição futura de ativos de redes e software de gerenciamento de redes, conforme especificações e exigências constantes do Termo de Referência e do Anexo I deste Edital;

2.1.1. Havendo divergências entre a descrição do objeto constante no edital e a descrição do objeto constante no SITE COMPRASNET, "SIASG" OU NOTA DE EMPENHO, prevalecerá, sempre, a descrição deste edital.

2.2. A Ata de Registro de Preços terá validade de **12 (doze) meses**, conforme o limite legal.

2.3. Em atendimento ao Decreto nº 6.204/2007 art. 6º, esta Licitação destina-se exclusivamente à participação de Microempresa, Empresa de Pequeno Porte – EPP ou, conforme art. 34 da Lei 11.488/2007, às sociedades cooperativas.

2.3.1. O caput anterior não se aplica aos itens com valores estimados acima de R$ 80.000,00 e estes serão fracionados em cota de 25% (COTA RESERVADA – ITENS 16, 21, 26, 28, 30, 32, 34, 45, 50 e 52) para participação exclusiva de ME, EPP e MEI, sendo o quantitativo restante de 75% (COTA PRINCIPAL – 15, 20, 25, 27, 29, 31, 33, 44, 49 e 51), aberto para ampla participação, tudo em conformidade com o inciso III, artigo 48 da lei complementar 123/2006, alterado pela Lei Complementar 147/2014;

2.3.1.1. Para os itens 02, 09, 10 e 46, embora tenham valores estimados acima de R$ 80.000,00, não se aplica o sistema de cotas previsto no subitem anterior, por se tratarem de itens não divisíveis.

2.3.1.2. O presente Edital se submete integralmente ao disposto nos artigos 42, 43, 44, 45 e 46 da Lei Complementar 123/2006 e do artigo 1º da Lei Complementar 147/2014, atendendo o direito de prioridade para a Microempresa e Empresa de Pequeno Porte para efeito do desempate quando verificado ao final da disputa de preços.

2.4. Nos termos do artigo 3°, §§ 5° a 10, da Lei n° 8.666, de 1993, e Decreto n° 7.546, de 2011, será aplicada na presente licitação a margem de preferência instituída pelo Decreto n° 7.903, de 04 de fevereiro de 2013, em favor do produto manufaturado nacional para os itens 3, 4, 5, 6, 7, 8, 9, 10, 20, 21, 22, 23, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53 e 54 do Anexo I deste edital.

2.3 Nos termos do artigo 3°, §§ 5° a 10, da Lei n° 8.666, de 1993, e Decreto n° 7.546, de 2011, será aplicada na presente licitação a margem de preferência instituída pelo Decreto n° 8.186, de 17 de janeiro de 2014, para os itens 1, 2, 15, 16, 17, 18, 19 e 24 do Anexo I deste edital.

2.4 Nos termos do artigo 3°, §§ 5° a 10, da Lei n° 8.666, de 1993, e Decreto n° 7.546, de 2011, será aplicada na presente licitação a margem de preferência instituída pelo Decreto n° 8.194, de 12 de fevereiro de 2014, em favor do produto manufaturado nacional para os itens 11, 12, 13 e 14 do Anexo I deste edital .

2.5 Após a aplicação de tais margens, será aplicado o Decreto nº 7.174 de 12 de maio de 2010. No momento do envio da proposta, a licitante deverá manifestar, em campo próprio, se pretende fazer uso do direito de preferência de que tratam o Decreto 7174/2010, de forma virtual conforme funcionalidade disponibilizada no sistema. A manifestação para fins de aplicação do Decreto 7174/2010 implica em responsabilidade da licitante pelo conteúdo declarado.Caso haja licitantes que se declarem portadores de certificados, conforme Decreto nº 7.174 de 12 de maio de 2010 que trata do exercício do direito de preferência em licitações para o setor de informática e automação, aplicar-se-á a seguinte ordem de classificação:

1º - Tecnologia no País + Processo Produtivo Básico + Micro e Pequena Empresas
2º - Tecnologia no País + Processo Produtivo Básico
3º - Tecnologia no País + Micro e Pequena Empresas
4º - Tecnologia no País
5º - Processo Produtivo Básico + Micro e Pequena Empresas
6º - Processo Produtivo Básico

3. DO EDITAL

3.1. A Empresa interessada em participar desta Licitação terá que examinar o Edital e seus Anexos, disponíveis no sitio da Universidade Federal de Alfenas – UNIFAL-MG, no endereço: www.unifal-mg.edu.br/licitacao, ou fazer cópia da via disponível no Setor de Compras desta instituição ou ainda, solicitá-lo através do correio eletrônico: pregao@unifal-mg.edu.br. Alegações de desconhecimento das suas disposições não serão aceitas para justificar eventuais divergências ou erros existentes em seus Documentos de Habilitação ou na Proposta.

3.2. **Só terão valor legal para efeito do Processo Licitatório os Anexos disponibilizados conforme item 3.1**, valendo as demais versões, inclusive a do sitio: www.comprasnet.gov.br, apenas como divulgação;

3.3. **Impugnação do Edital:**

3.3.1. Qualquer pessoa, física ou jurídica, é parte legítima para impugnar este Edital, desde que, com antecedência de até 02 (dois) dias úteis antes da data fixada para abertura da sessão pública, artigo 18, Dec. 5.450/2005;

3.3.1.1. A data limite para impugnação deste edital é dia **27/01/2016**, até as 17 horas.

3.3.2. Caberá ao Pregoeiro e sua Equipe de apoio decidir sobre a petição interposta, no prazo de 24 (vinte e quatro) horas, contadas da data do recebimento da petição, § 1º do artigo 18 do Decreto 5.450/2005;

3.3.3. Quando acolhida a petição contra este Edital, será designada nova data para a realização deste certame;

3.3.4. Os pedidos de esclarecimentos referentes ao processo licitatório deverão ser enviados ao Pregoeiro, até 03 (três) dias úteis anteriores a data fixada para abertura da sessão pública, exclusivamente por meio eletrônico via internet no endereço indicado neste edital, artigo 19 do Decreto 5.450/2005;

3.3.4.1. A data limite para solicitação de esclarecimentos é dia **26/01/2016**, até as 17 horas.

3.3.5. Os pedidos de esclarecimento e impugnação deverão ser enviados exclusivamente por meio eletrônico, através do e-mail pregao@unifal-mg.edu.br;

3.3.6. Todas as solicitações, impugnações, esclarecimentos e recursos deverão ser enviados dentro do horário de expediente normal, das 07h às 17h, de segunda-feira à sexta-feira.

3.3.7. Os pedidos realizados fora do horário de expediente acima serão considerados recebidos no primeiro dia útil imediatamente posterior, sendo utilizada a data e hora de registro no e-mail como comprovação.

4. DO ATO DE DESIGNAÇÃO DO PREGOEIRO E EQUIPE DE APOIO

4.1. Todos os procedimentos desta Licitação serão conduzidos pelo Pregoeiro e sua respectiva Equipe de apoio, designados pela Portaria n° 1.640 de 03 de agosto de 2015;

4.2. O Pregoeiro poderá, ainda, convocar, por meio de Ato administrativo, qualquer servidor da área ou unidade administrativa responsável pela especificação ou recebimento do objeto deste Pregão Eletrônico.

5. DAS CONDIÇÕES GERAIS PARA PARTICIPAÇÃO

5.1. Poderão participar deste Pregão Eletrônico os interessados do ramo pertinente ao objeto licitado, obrigatoriamente, **cadastrados no Sistema Unificado de Cadastro de Fornecedores – SICAF** e que atenderem a todas as demais exigências constantes neste Edital e seus anexos;

5.2. Não serão permitidos a participação no mesmo item de empresas cujos sócios possuam grau de parentesco ou vínculo, capaz de indicar que houve quebra de sigilo das propostas, conforme acórdão TCU - 2725/2010 Plenário.

5.3. **Em caso de a empresa licitante ser a própria fabricante do produto ofertado, deverá ser apresentado o Certificado de Cumprimento de Boas Práticas de Fabricação**, conforme disposto no inciso X do artigo 7º da Lei 9.782/99;

5.4. A licitante deverá cumprir o que determina o Artigo 13, incisos I ao VII do Decreto 5.450/2005;

5.5. A licitante deverá manifestar, em campo próprio do sistema eletrônico Comprasnet, o pleno conhecimento e atendimento às exigências de habilitação previstas no Edital – §2°, Artigo 21, Decreto 5.450/2005;

5.6. A licitante é obrigada e deverá declarar, em campo próprio do sistema eletrônico, afim de que o Sistema gere: Declaração de Conhecimento das Condições Editalícias, Declaração de Inexistência de Fato Superveniente, Declarações de Menor, Declaração do Porte da Empresa quando enquadrar como ME/EPP e Declaração de Elaboração Independente de Proposta; **Declaração de Certificação de Tecnologia do País e/ou Processo Produtivo Básico, caso se enquadre no Decreto nº 7.174 de 12 de maio de 2010.**

5.7. A licitante ao declarar porte ME/EPP e se beneficiar pelo Decreto nº 6.204/2007, assume todas as responsabilidades e conseqüências civis e criminais, isentando o Pregoeiro e sua Equipe de Apoio de culpa, em caso de má-fé ou uso indevido dos benefícios.

5.8. Não poderão participar desta licitação:

5.8.1. Consórcios de empresa, qualquer que seja sua forma de constituição;

5.8.2. As empresas suspensas e impedidas de contratar com a Universidade Federal de Alfenas ou no âmbito da União;

5.8.3. Empresas que foram declaradas inidôneas para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos da punição.

5.9. As licitantes ou seus representantes legais deverão estar **previamente credenciados junto ao órgão provedor,** sendo o uso da senha de acesso de responsabilidade exclusiva do usuário;

5.10. **As especificações do Anexo I deste Edital em nenhum momento serão substituídas pelas descrições resumidas, constantes no Aviso divulgado no sitio** www.comprasnet.gov.br. Em caso de divergência nas especificações, prevalecerão as dos Anexos deste Edital, dos avisos e esclarecimentos lançados no Comprasnet.

6. DAS CONDIÇÕES ESPECIAIS PARA PARTICIPAÇÃO

6.1. A licitante deverá apresentar certificações emitidas por instituições públicas ou privadas credenciadas pelo Instituto Nacional de Metrologia, Normalização e Qualidade Industrial - Inmetro, que atestem, conforme regulamentação específica, a adequação dos seguintes requisitos:

a) segurança para o usuário e instalações;

b) compatibilidade eletromagnética; e

c) consumo de energia.

6.2. A licitante deverá apresentar, ainda, documento contratual de comprovação da origem dos bens importados oferecidos pelos licitantes e da quitação dos tributos de importação a eles referentes, que deve ser apresentada no momento da entrega do objeto, sob pena de rescisão contratual e multa.

7. DATA, HORÁRIO E LOCAL DA SESSÃO PÚBLICA PARA OS LANCES

7.1. DATA: 01/ 02 / 2016

7.2. HORÁRIO: 09:00

7.3. LOCAL: http://www.comprasnet.gov.br

OBS: Todos os horários estipulados neste edital obedecerão ao horário oficial de Brasília.

8. DA REMESSA ELETRÔNICA, ENVIO DAS PROPOSTAS E DOCUMENTOS PARA ACEITAÇÃO

8.1. O envio da proposta poderá ocorrer a partir da data de liberação do edital no Comprasnet, até segundos antes do horário estipulado para início da sessão pública de lances.

8.2. Durante este período, o fornecedor poderá incluir, modificar ou excluir sua proposta.

8.3. Para inclusão, os licitantes credenciados efetuarão o lançamento do **VALOR UNITÁRIO** de cada item da proposta, através do sitio www.comprasnet.gov.br, sendo o valor lançado em campo específico e preenchidos todos os demais campos disponíveis do sistema;

8.4. A licitante será inteiramente responsável por todas as transações assumidas em seu nome no sistema eletrônico, assumindo como verdadeiras e firmes suas propostas e subseqüentes lances, se for o caso, bem como acompanhar as operações no sistema durante a sessão tais como avisos e esclarecimentos, ficando responsável pelo ônus decorrente da perda de negócios diante da inobservância de quaisquer mensagens emitidas pelo sistema, de sua desconexão ou por uso indevido;

8.5. Não serão aceitas as propostas com exigência de faturamento mínimo ou proposta alternativa;

8.6. Não serão admitidos quaisquer acréscimos, supressões ou retificações na proposta, depois de apresentada, nem pedido de desconsideração da mesma, observando o disposto no item 8.4 do Edital;

8.7. Os preços (unitários), em moeda corrente, com duas casas decimais para os centavos, estando neles incluídas todas as despesas diretas e indiretas, tais como frete, impostos etc;

8.8. A Proposta deverá ter validade de 60 (sessenta) dias, a contar da data de sua apresentação.

8.9. A apresentação da Proposta em desacordo com as exigências deste Edital acarretará, sumariamente, a desclassificação da Empresa proponente e sua exclusão do certame;

8.10. No caso de omissões em Propostas, exceto marca e modelo, serão considerados aqueles previstos no Edital.

8.11. Quaisquer tributos, custos e despesas diretos ou indiretos omitidos da Proposta, ou incorretamente cotados, serão considerados como incluídos nos preços, não sendo considerados pleitos de acréscimos, a esse ou a qualquer título, devendo o fornecimento ser efetuado à Universidade Federal de Alfenas – UNIFAL-MG sem ônus adicionais;

8.12. NÃO DEVERÁ SER ENVIADA NOVA PROPOSTA DE PREÇOS (preços negociados), pois todos os lances e valores resultantes de negociações serão registrados no Sistema, gerando uma Ata, a qual será instrumento do processo e a única proposta válida para a licitação, inclusive para conferência do produto no momento de sua entrega.

9. DO CADASTRAMENTO DAS PROPOSTAS

9.1. A proposta deverá conter **OBRIGATORIAMENTE** a **marca** e **fabricante do produto ofertado em seus campos específicos;**

9.1.1. No campo "MARCA" e/ou "descrição detalhada do objeto ofertado" do Sistema Comprasnet poderá, também, informar o MODELO do produto ofertado;

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

9.3. A proposta deverá trazer ainda no campo **"descrição detalhada do objeto ofertado"** as seguintes informações**: Nome Comercial (quando houver),** além das demais informações necessárias para cada item;

9.4. As propostas que apresentem no **"campo descrição detalhada do objeto ofertado"** a informação **"de acordo com o edital"** ou similar serão **consideradas como produto/material ofertado EXATAMENTE igual ao registrado na especificação do Anexo I do Edital.**

10. DA FORMULAÇÃO DOS LANCES

10.1. No dia e horário indicado, o Pregoeiro abrirá a sessão pública, verificando as propostas de preços lançadas no sistema, as quais devem estar em perfeita consonância com as especificações e condições detalhadas no Anexo I – deste Edital;

10.2. Em caso de dificuldade em verificar a aceitabilidade das propostas, o Pregoeiro informará aos participantes através de mensagem via Sistema e encaminhará as propostas para a etapa de lances;

10.3. O encaminhamento das propostas para a fase de lances não implica que estas atende à todas as exigências de especificação, não garantindo assim que estas foram classificadas como previsto no artigo 22 e seguintes do Decreto 5.450/2005;

10.4. Iniciada a etapa competitiva, as licitantes poderão encaminhar lance exclusivamente por meio do sistema eletrônico, sendo o acompanhamento disponibilizado imediatamente;

10.5. As Licitantes poderão oferecer lances sucessivos, observados o horário fixado e as regras de aceitação dos mesmos. Será considerada aceitável a proposta que:

a) Atenda a todos os termos deste Edital;

b) Contenha preço compatível com os praticados no mercado, dentro do estipulado conforme as disponibilidades orçamentárias da UNIFAL-MG.

10.6. Serão aceitos os lances cujos valores forem inferiores ao último lance que tenha sido anteriormente registrado pela licitante, não necessariamente lances menores que o menor lance registrado no sistema;

10.7. Serão aceitos dois ou mais lances de igual valor, prevalecendo aquele que for recebido e registrado em primeiro lugar;

10.8. Sendo efetuado lance, aparentemente inexeqüível, o Pregoeiro alertará a proponente, sobre o valor cotado para o respectivo item, através do sistema, podendo ainda, o lance ser excluído pelo Pregoeiro e posteriormente vir a ser confirmado pela proponente;

10.9. Durante o transcurso da sessão pública, as licitantes serão informadas, em tempo real, do valor do menor lance registrado que tenha sido apresentado pelas demais licitantes, vedada a identificação das mesmas, através de ferramenta do sistema Comprasnet;

10.10. Em caso de desconexão com o Pregoeiro, no decorrer da etapa competitiva do Pregão Eletrônico, o sistema poderá permanecer acessível aos licitantes para o envio dos lances, sendo possível o retorno do pregoeiro para atuação na etapa, sem prejuízo dos atos realizados;

10.11. Quando a desconexão persistir por tempo superior a 10 (dez) minutos, a sessão do Pregão Eletrônico será suspensa e terá reinício somente após comunicação expressa, no sistema eletrônico, aos participantes;

10.12. A etapa de lances será encerrada mediante aviso de fechamento iminente dos lances, emitido pelo sistema eletrônico às licitantes, após o que transcorrerá período de até 30 (trinta) minutos, aleatoriamente determinado também pelo sistema eletrônico, findo o qual será automaticamente encerrada a recepção de lances;

10.13. O Pregoeiro poderá encaminhar contraproposta diretamente à licitante que tenha apresentado o menor lance, através do sistema eletrônico, para que seja obtido preço melhor e assim decidir sobre sua aceitação;

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

10.14.1. A apresentação de novas propostas na forma do **caput** não prejudicará o resultado do certame em relação ao licitante mais bem classificado.

11. DO DIREITO DE PREFERÊNCIA PREVISTO NOS DECRETOS 7.903/2013, 8.186/2014 e 8.194/2014.

11.1. Após a fase de lances, será aplicada a margem de preferência para os produtos manufaturados nacionais tratados pelos **Decretos 7.903/2013 e 8.194/2014, conforme anexo III deste Edital**.

11.1.1. O licitante declarará, durante a fase de cadastramento das propostas, em campo próprio no sistema, que atende ao Processo Produtivo Básico ou à regra de origem a que se referem os **Decretos 7.903/2013** e **8.194/2014**, devendo apresentar cópia da referida declaração no momento da entrega dos documentos exigidos para habilitação.

11.1.2. A margem de preferência normal será aplicada apenas para os produtos manufaturados nacionais, conforme Processo Produtivo Básico aprovado nos termos do Decreto-Lei nº 288, de 28 de fevereiro de 1967, e da Lei nº 8.248, de 23 de outubro de 1991.

11.1.3. A margem de preferência adicional prevista no **decreto 8.194/2014** será aplicada apenas para os produtos manufaturados nacionais, nos termos da clausula anterior, e que atendam os requisitos e os critérios definidos na Portaria Interministerial MDIC/MCTI nº 383, de 26 de abril de 2013.

11.1.4. A margem de preferência adicional de que trata o **decreto 7.903/2013**, será aplicada apenas para os produtos manufaturados nacionais que tenham sido desenvolvidos no País, conforme requisitos e critérios definidos em ato conjunto dos Ministros de Estado do Desenvolvimento, Indústria e Comércio Exterior e da Ciência, Tecnologia e Inovação.

11.1.5. A margem de preferência será calculada sobre o menor preço ofertado de produto manufaturado estrangeiro;

11.1.6. O preço ofertado de produto manufaturado nacional será considerado menor que PE sempre que seu valor for igual ou inferior a PM; e

11.1.7. O preço ofertado de produto manufaturado nacional será considerado maior que PE sempre que seu valor for superior a PM.

11.1.8. Fórmula: PM = PE x (1 + M), sendo:

PM = preço com margem;

PE = menor preço ofertado do produto manufaturado estrangeiro;

M = margem de preferência em percentual, conforme estabelecido no Anexo III.

11.1.9. A margem de preferência não será aplicada caso o preço mais baixo ofertado seja de produto manufaturado nacional.

11.1.10. Para produtos abrangidos por margem de preferência, caso a proposta de menor preço não tenha por objeto produto manufaturado nacional, o sistema automaticamente indicará as propostas de produtos manufaturados nacionais que estão enquadradas dentro da referida margem, para fins de aceitação pelo Pregoeiro.

11.1.11. Nesta situação, a proposta beneficiada pela aplicação da margem de preferência tornar-se-á a proposta classificada em primeiro lugar.

11.2. Após a fase de lances, será aplicada a margem de preferência para os produtos manufaturados nacionais tratados pelo **Decreto 8.186/2014, conforme anexo III deste Edital**;

11.2.1. As margens de preferência normal e adicional serão aplicadas para os itens que:

11.2.1.1. sejam desenvolvidos ou prestados no País por pessoa jurídica constituída em conformidade com o art. 1.126 ao art. 1.133 do Código Civil, instituído pela Lei nº 10.406, de 10 de janeiro de 2002, constantes do Anexo I, classificados segundo a Nomenclatura Brasileira de Serviços, Intangíveis e Outras Operações que Produzam Variações no Patrimônio, instituída pelo Decreto nº 7.708, de 2 de abril de 2012; e

11.2.1.2. tenham recebido o certificado de que trata a Portaria nº 555, de 18 de junho de 2013, do Ministério da Ciência, Tecnologia e Inovação, como resultado de desenvolvimento e inovação tecnológica e serviços correlatos associados prestados pelas titulares dos direitos de licença daqueles programas de computador e serviços correlatos assim certificados, na forma do art. 3º da Lei nº 8.248, de 23 de outubro de 1991, e do art. 5º do Decreto nº 7.174, de 12 de maio de 2010.

11.2.2. A margem de preferência será calculada sobre o menor preço ofertado de produto manufaturado estrangeiro;

11.2.3. O preço ofertado de produto manufaturado nacional será considerado menor que PE sempre que seu valor for igual ou inferior a PM; e

11.2.4. O preço ofertado de produto manufaturado nacional será considerado maior que PE sempre que seu valor for superior a PM.

11.2.5. Fórmula: PM = PE x (1 + M), sendo:

11.2.6. PM = preço com margem;

11.2.7. PE = menor preço ofertado do produto manufaturado estrangeiro;

11.2.8. M = margem de preferência em percentual, conforme estabelecido no Anexo III.

11.3. Após a fase do direito de preferência previsto **nos decretos 7.903/2013, 8.186/2014 e 8.194/2014** e o direito de preferência das microempresas e empresas de pequeno porte verificada nos itens constantes no anexo III, as licitantes serão convocadas, conforme funcionalidade do sistema comprasnet, para aplicação do direito de preferência previsto no **Decreto 7.174/2010** e proceder-se-á, sucessivamente, da seguinte forma:

11.3.1. Se o produto ofertado pela licitante detentora do lance de menor preço para o item não for feito com tecnologia desenvolvida no Brasil e de acordo com o Processo Produtivo Básico- PPB (inciso I do art.5° do Decreto 7.174/2010) e existirem empresas cuja proposta seja até 10% acima da melhor proposta válida e cujo produto atenda ao disposto no inciso I do artigo 5° do Decreto 7.174/2010, estas serão consultadas, na ordem de classificação, sobre o interesse em oferecer o produto por preço igual ou inferior do que o da melhor proposta válida.

11.3.2. Se o produto ofertado pela licitante detentora do lance de menor preço para o item, não for com tecnologia desenvolvida no Brasil (inciso II do art.5° do Decreto 7.174/2010) e existirem empresas cuja proposta seja até 10% acima da melhor proposta válida e cujo produto atenda ao disposto no inciso II do artigo 5° do Decreto 7.174/2010, estas serão consultadas sobre o interesse em oferecer o produto por preço igual ou inferior do que o da melhor proposta válida.

11.3.3. Se o produto ofertado pela licitante detentora do lance de menor preço para o item, não for produzido de acordo com o PPB (inciso III do art.5° do Decreto 7.174/2010) e existirem empresas cuja proposta seja até 10% acima da melhor proposta válida e cujo produto atenda ao disposto no inciso III do artigo 5° do Decreto 7.174/2010, estas serão consultadas sobre o interesse em oferecer o produto por preço igual ou inferior do que o da melhor proposta válida.

11.4. Consideram-se bens com tecnologia desenvolvida no Brasil aqueles cujo desenvolvimento local seja comprovado junto ao Ministério da Ciência e Tecnologia, competindo à licitante comprovar que seu produto se enquadra nesta categoria, no caso de questionamentos. Caso alguma licitante questione o enquadramento da licitante vencedora, arcará com o ônus da prova, pois o Pregoeiro basear-se-á exclusivamente na declaração prestada pela empresa quando de sua expressa opção pelo direito de preferência (quando do encaminhamento de sua proposta).

11.5. A comprovação do atendimento ao PPB é feita mediante a apresentação do documento comprobatório de habilitação à fruição dos incentivos fiscais regulamentados pelo Decreto 5.906/2006 ou Decreto 6.008/2006. Tal comprovação poderá ser feita: por meio de sitio eletrônico do Ministério da Ciência e Tecnologia ou da Superintendência da Zona Franca de Manaus- SUFRAMA; ou por documento expedido para esta finalidade pelo Ministério da Ciência e Tecnologia ou SUFRAMA mediante solicitação dos licitantes. Compete à licitante comprovar que seu produto se enquadra nesta categoria, no caso de questionamentos. Caso alguma licitante questione o enquadramento da licitante vencedora, arcará com o ônus da prova, pois o Pregoeiro basear-se-á exclusivamente na declaração prestada pela empresa quando de sua expressa opção pelo direito de preferência (quando do encaminhamento de sua proposta).

11.5.1. Eventual empate entre propostas, o critério de desempate será aquele previsto no artigo 3º, § 2º, da Lei nº 8.666, de 1993, assegurando-se a preferência, sucessivamente, aos bens:

11.5.2. produzidos no País;

11.5.3. produzidos ou prestados por empresas brasileiras;

11.5.4. produzidos ou prestados por empresas que invistam em pesquisa e no desenvolvimento de tecnologia no País.

11.6. Persistindo o empate, o critério de desempate será o sorteio, em ato público para o qual os licitantes serão convocados, vedado qualquer outro processo.

11.7. Ao final do procedimento, após o encerramento da etapa competitiva, os licitantes poderão reduzir seus preços ao valor da proposta do licitante mais bem classificado.

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

12. DO JULGAMENTO DAS PROPOSTAS DE PREÇOS E ACEITABILIDADE

12.1. A presente Licitação é do tipo **MENOR PREÇO**, sendo vencedora(s) a(s) Licitante(s) que ofertar(em) o **MENOR PREÇO UNITÁRIO POR ITEM,** conforme especificado neste Edital e seus Anexos, respeitadas as determinações legais previstas na Lei Complementar nº 123 de 14 de dezembro de 2006;

12.2. A aceitação da proposta ocorrerá em momento ou data posterior à sessão de lances, a critério do pregoeiro que comunicará às licitantes através do sistema eletrônico;

12.2.1. Na data e hora marcada as licitantes devem acompanhar e atender aos chamados do Pregoeiro via chat;

12.2.2. Valores com mais de duas casas decimais para os centavos, conforme exigido no subitem 8.7 deste Edital, serão arredondados (para baixo) na etapa de aceitação.

12.3. Quando os valores unitários ou totais, se divididos pela quantidade do item, não obtiverem valor com apenas duas casas decimais nos centavos, estes serão arredondados (para baixo) na etapa de aceitação, independentemente de autorização do licitante.

12.4. Quando uma mesma Licitante, enquadrada como ME/EPP/MEI, for vencedora dos itens da cota principal e da cota reservada com valores diferentes, prevalecerá a proposta de menor valor para ambos os itens.

12.5. Se a proposta ou lance de menor valor não atender as especificações solicitadas, inclusive com relação à aceitabilidade do produto, após parecer técnico do interessado na aquisição, ou então, se o licitante desatender as exigências habilitatórias, o pregoeiro examinará a proposta ou o lance subseqüente, verificando a sua aceitabilidade, procedendo a habilitação do proponente na ordem de classificação, e assim sucessivamente, até a apuração de uma proposta ou lance que atenda ao Edital;

12.6. Ocorrendo situação a que se refere o subitem anterior, o pregoeiro poderá negociar com o licitante para que seja obtido menor preço;

12.7. O licitante que não tiver declarado inicialmente, em campo próprio no sistema, que o item atende ao Processo Produtivo Básico ou à regra de origem, ou não entregar a documentação solicitada para o benefício da margem de preferência, será considerado como item manufaturado estrangeiro para fins de classificação.

12.8. Caso a proposta classificada em primeiro lugar tenha se beneficiado da aplicação da margem de preferência, o Pregoeiro solicitará ao licitante que envie imediatamente, por meio eletrônico, com posterior encaminhamento por via postal, o documento comprobatório da caracterização do produto manufaturado nacional.

12.9. Caso o licitante da proposta classificada em primeiro lugar seja inabilitado, ou deixe de cumprir a obrigação prevista no item 12.8, será realizada a reclassificação das propostas, para fins de nova aplicação da margem de preferência.

12.10. Das propostas vencedoras poderão ser solicitados catálogos, folders ou manual do fabricante que deverão ser enviados na forma digital através da opção “Anexo” disponibilizada no Sistema Comprasnet, no prazo máximo de 30 minutos após solicitação.

12.10.1. Os catálogos, folders ou manual do fabricante a que se refere o item anterior deverão apresentar especificação completa, em Língua Portuguesa, incluindo foto do produto ofertado;

12.10.2. O não envio do "Anexo" no prazo estabelecido acarretará na recusa da proposta da empresa solicitada e na aplicação das penalidades previstas no item 23 deste Edital.

12.11. O Pregoeiro poderá solicitar, via chat, na fase de aceitabilidade, amostras dos produtos, objetos desta licitação, que deverão ser entregues, no Almoxarifado Central desta Universidade, em até 04 (quatro) dias úteis.

12.11.1. As amostras serão analisadas pelo Setor Requisitante e/ou Comissão de Avaliação e Recebimento de Materiais a ser nomeada pela Autoridade Competente da Universidade Federal de Alfenas UNIFAL-MG, e sua decisão, com a devida justificativa quando da recusa, deverá ser emitida em até 03 dias úteis;

12.11.2. As licitantes poderão retirar as amostras enviadas e não aceitas, em até 30 dias a contar da data de emissão do laudo; após esse período, as mesmas serão descartadas.

12.11.3. As amostras aprovadas, material permanente, serão deduzidas da quantidade a ser entregue.

12.12. O não atendimento aos chamados via chat ou do fornecimento da amostra será interpretado como descumprimento das normas editalícias ou desinteresse em fornecer o objeto da licitação, acarretará na desclassificação da proposta da empresa solicitada;

12.13. A PROPONENTE que oferecer o menor preço deverá apresentar, após solicitação do pregoeiro, a documentação técnica do fabricante do equipamento comprovando o atendimento a todos os requisitos contidos nas "Características técnicas mínimas obrigatórias" do objeto a ser contratado, com o atendimento das seguintes condições:

12.13.1. Não será aceita Carta do Fornecedor/Distribuidor como comprovação de atendimento a características técnicas e de compatibilidade especificados no termo de referência;

12.13.2. Documentação técnica. Nessa documentação, a PROPONENTE deve fornecer uma planilha ponto-a-ponto indicando documento e página em que consta o cumprimento de cada um dos requisitos das especificações técnicas;

12.13.3. Os documentos devem descrever claramente a referência ao modelo apresentado na proposta, e não serão válidas referências genéricas;

12.13.4. Não serão aceitas referências a futuras atualizações ou versões de produtos para comprovar a existência ou aderência a qualquer quesito desta especificação;

12.13.5. Relação de componentes. Nessa documentação, a PROPONENTE deve fornecer uma lista completa contendo a configuração do equipamento ofertado, incluindo módulos, fontes e acessórios, com as respectivas quantidades de cada item;

12.13.6. A PROPONENTE deve fornecer declaração de que os equipamentos propostos e todos os seus componentes são novos, de primeiro uso e estão em linha de fabricação na data de abertura das propostas;

12.13.7. A PROPONENTE deve fornecer declaração do fabricante de que o equipamento proposto possui a garantia e suporte técnico solicitado no item "Garantia e Suporte" de cada item, conforme descrito no "Anexo I".

12.14. Sendo aceitável a(s) oferta(s), será verificado o atendimento das condições habilitatórias pela(s) Licitante(s) que a(s) tiver formulado;

12.15. O julgamento das propostas será feito por item, sendo aceito, habilitado e homologado o item já analisado e aprovado, podendo os demais itens permanecer na situação "em análise" (funcionalidade do Sistema Comprasnet) até finalização dos mesmos;

12.16. A LICITANTE VENCEDORA, cuja proposta for aceita, deverá **enviar pelo correio eletrônico** pregao@unifal-mg.edu.br**, no prazo máximo de 02 (duas) horas,** após o aceite da proposta:

12.16.1. A Declaração constante do Anexo II, preenchida com os dados cadastrais da empresa, indicando a Razão Social da Empresa Proponente, o número do seu CNPJ, endereço, telefone, fax e e-mail; dados bancários: Banco, Número da Conta e Agência, bem como as informações necessárias para a identificação do Representante Legal da Empresa;

12.17. Não há necessidade de envio de documentos ou propostas via correio.

13. DA HABILITAÇÃO

13.1. Será habilitada a licitante que estiver regularmente cadastrada no SICAF e que esteja com a Regularidade Fiscal Federal, Estadual e Municipal e a Regularidade Trabalhista válidas;

13.1.1. A consulta da regularidade fiscal será verificada "ON LINE", na fase de habilitação, através do SICAF no sítio do Comprasnet. Estando com certidões vencidas, a proponente será comunicada para enviá-las, através correio eletrônico pregao@unifal-mg.edu.br.

13.1.2. A consulta da regularidade trabalhista será realizada através da emissão da Certidão Negativa de Débitos Trabalhistas – CNDT, na fase de habilitação, no sítio do Tribunal Superior do Trabalho, www.tst.jus.br, para atendimento da Lei nº 12.440, de 07 de julho de 2011 e da Resolução do Tribunal Superior do Trabalho nº 1.470, de 24 de agosto de 2011.

13.2. A apresentação das Declarações, exigidas pela Lei 8.666/93 (Atendimento das exigências editalícias, Declaração de Inexistência de fato superveniente), as exigências da CF/88 (Declaração de menor e Declaração de trabalho forçado e degradante), a Declaração de Elaboração Independente de Proposta (IN nº 2 da SLTI/MPOG) e a **Declaração Certificação de Tecnologia do País e/ou Processo Produtivo Básico, caso se enquadre no Decreto nº 7.174 de 12 de maio de 2010** serão consultadas através do campo específico no COMPRASNET, não havendo necessidade de envio;

13.3. O Licitante deverá apresentar cópia da publicação do Certificado CERTICS, na forma do § 3º do art. 8º da Portaria nº555, de 2013, do Ministério da Ciência, Tecnologia e Inovação, caso tenha se beneficiado da aplicação da margem de preferência prevista no **decreto 8.186/2014.**

13.4. O licitante que tiver declarado, durante a fase de cadastramento das propostas, que atende ao Processo Produtivo Básico ou à regra de origem a que se referem os **Decretos 7.903/2013** e **8.194/2014,** deverá apresentar cópia da referida declaração.

13.5. O licitante que se beneficiar da margem de preferência a que se referem os **Decretos 7.903/2013 e 8.194/2014**, deverá apresentar cópia da cópia da portaria interministerial que atesta sua habilitação aos incentivos da Lei nº 8.248, de 1991, ou cópia da Resolução do Conselho de Administração da Superintendência da Zona Franca de Manaus - SUFRAMA que atesta sua habilitação aos incentivos do Decreto-Lei nº 288, de 1967.

13.6. A documentação solicitada deverá ser enviada até o prazo de 02(duas) horas, a contar da solicitação do pregoeiro.

13.7. A apresentação de declaração falsa relativa ao cumprimento dos requisitos de habilitação sujeitará a licitante às sanções previstas no artigo 28 do Decreto nº 5.450, de 31 de maio de 2005;

13.8. O CNPJ indicado nos documentos de habilitação terá que ser, obrigatoriamente, do mesmo estabelecimento da Empresa que efetivamente irá fornecer o objeto da presente Licitação e emitir a respectiva Nota Fiscal / Fatura.

13.9. Se a proposta aceita desatender as exigências habilitatórias e o licitante tiver apresentado proposta que inviabilizou a disputa entre os concorrentes, caracterizando indícios de fraude na licitação (pulo do coelho), a UNIFAL-MG além de outras providências cabíveis aplicará ao infrator as penalidades previstas no artigo 28 do Decreto nº 5.450, de 31 de maio de 2005, e poderá anular a licitação para aquele item, caso contrário o pregoeiro voltará à fase de aceitação e examinará a proposta ou o lance subseqüente, verificando a aceitabilidade da proposta, procedendo a habilitação do proponente na ordem de classificação, e assim sucessivamente, até a apuração de uma proposta que atenda ao Edital.

14. DA INTERPOSIÇÃO DE RECURSOS

14.1. As licitantes poderão interpor recursos, mediante manifestação prévia, após habilitação da proposta, devendo apresentar sucintamente suas razões, exclusivamente no âmbito do sistema eletrônico, em formulários próprios, sendo que, ao final da sessão pública, o pregoeiro informará os prazos legais para registro da razão do recurso para a licitante com intenção de recurso aceita e para os demais licitantes registrarem as contra-razões;

14.1.1. O prazo de registro da intenção de recurso será informado para cada item habilitado, sendo que os itens que estiverem na situação “em análise” terão seus prazos abertos após habilitação dos mesmos, não impedindo o andamento da licitação;

14.1.2. A licitante dispõe do prazo de 03 (três) dias para apresentação dos recursos, sendo eles escritos por meio eletrônico, sendo disponibilizados a todos os participantes;

14.1.3. As demais licitantes poderão apresentar contra-razões em até 03 (três) dias contados a partir do término do prazo do recorrente;

14.1.4. A decisão do Pregoeiro será motivada e submetida à apreciação da autoridade competente;

14.1.5. O acolhimento do recurso importará a invalidação apenas dos atos que não sejam passíveis de aproveitamento;

14.2. A falta de manifestação imediata e motivada do licitante importará na decadência do recurso;

14.3. Os autos do processo permanecerão com vistas franqueadas aos interessados no Setor de Compras da UNIFAL-MG, Rua Gabriel Monteiro da Silva, 700 - Centro – Alfenas/MG.

14.4. Constatado o atendimento pleno às exigências editalícias, será declarada a Proponente Vencedora;

14.5. Da sessão lavrar-se-á ata circunstanciada, na qual serão registradas as ocorrências relevantes e a indicação do lance vencedor, divulgada no sistema eletrônico.

15. DA ADJUDICAÇÃO E DA HOMOLOGAÇÃO

15.1. Depois de declarada a Proponente Vencedora ser-lhe-á adjudicado o objeto desta licitação para o qual apresentou proposta;

15.2. A adjudicação do objeto do presente certame será realizada pelo Pregoeiro sempre que não houver recurso, e a homologação, de responsabilidade da autoridade competente, só podendo ser realizada depois da adjudicação do objeto ao proponente vencedor ou, quando houver recursos, após o devido julgamento.

16. DA ATA DE REGISTRO DE PREÇOS

16.1. A classificação será mantida durante o período de validade da Ata, a partir da data de sua publicação, exceto nos casos em que houver exclusão do SRP (Sistema de Registro de Preços), a título de penalidade imposta pela Administração;

16.2. Homologado o resultado da licitação, a UNIFAL-MG, convocará os interessados para assinatura da Ata de Registro de Preços, que terá efeito de compromisso de fornecimento nas condições estabelecidas, podendo ser assinada por certificação digital, conforme § 1º do art. 5º do Decreto 7.892 de 23/01/2013.

16.3. A Ata de Registro de Preços terá validade de 12 (doze) meses a partir do registro da homologação no sitio do Comprasnet e no Sistema SIASG, podendo ser registrado uma única data de vigência para todos os itens da licitação ou uma data para cada item homologado.

16.3.1. É vedado efetuar acréscimos nos quantitativos fixados pela ata de registro de preços, inclusive o acréscimo de que trata o § 1º do art. 65 da Lei nº 8.666, de 1993.

16.4. Após a homologação da licitação, o registro de preços observará, entre outras, as seguintes condições:

16.4.1. será incluído, na respectiva ata, o registro dos licitantes que aceitarem cotar os bens ou serviços com preços iguais ao do licitante vencedor na sequência da classificação do certame;

16.4.2. o preço registrado com indicação dos fornecedores será divulgado no Portal de Compras do Governo federal e ficará disponibilizado durante a vigência da ata de registro de preços; e

16.4.3. a ordem de classificação dos licitantes registrados na ata deverá ser respeitada nas contratações.

16.5. O registro a que se refere o caput tem por objetivo a formação de cadastro de reserva, no caso de exclusão do primeiro colocado da ata, nas hipóteses previstas nos arts. 20 e 21.

16.6. Serão registrados na ata de registro de preços, nesta ordem:

16.6.1. preços e quantitativos do licitante mais bem classificado durante a etapa competitiva; e

16.6.2. os preços e quantitativos dos licitantes que tiverem aceito cotar seus bens ou serviços em valor igual ao do licitante mais bem classificado.

16.7. Se houver mais de um licitante na situação de que trata o inciso II do § 2º, serão classificados segundo a ordem da última proposta apresentada durante a fase competitiva.

16.8. Constarão da Ata de Registro de Preços, todas as informações necessárias à:

a) Identificação do processo;

b) Caracterização do objeto;

c) Identificação das empresas;

d) Preços ofertados pelas classificadas, item a item;

e) Direitos e responsabilidades das partes.

16.9. A ARP será lavrada em tantas vias quantas forem as empresas classificadas;

16.10. É obrigatória a assinatura da ARP pelas partes envolvidas, no prazo máximo de 05 (cinco) dias úteis a contar da convocação da UNIFAL-MG, aplicando-se, em caso de descumprimento, o disposto no art. 7º, da Lei 10.520/2002.

16.11. Se o contratado não assinar a Ata de Registro de Preços na presença do Chefe da Divisão de Material e Patrimônio a assinatura do representante legal deverá ser reconhecida junto ao Tabelionato de Notas, até que seja disponibilizada a assinatura por certificação digital, **conforme § 1º do art. 5º do Decreto 7.892 de 23/01/2013.**

17. DAS COMPETÊNCIAS DO ÓRGÃO GERENCIADOR

17.1. Registrar sua intenção de registro de preços no Portal de Compras do Governo federal;

17.2. Consolidar informações relativas à estimativa individual e total de consumo, promovendo a adequação dos respectivos termos de referência ou projetos básicos encaminhados para atender aos requisitos de padronização e racionalização;

17.3. Promover atos necessários à instrução processual para a realização do procedimento licitatório;

17.4. Realizar pesquisa de mercado para identificação do valor estimado da licitação e consolidar os dados das pesquisas de mercado realizadas pelos órgãos e entidades participantes;

17.5. Confirmar junto aos órgãos participantes a sua concordância com o objeto a ser licitado, inclusive quanto aos quantitativos e termo de referência ou projeto básico;

17.6. Realizar o procedimento licitatório;

17.7. Gerenciar a ata de registro de preços;

17.8. Conduzir eventuais renegociações dos preços registrados;

17.9. Aplicar, garantida a ampla defesa e o contraditório, as penalidades decorrentes de infrações no procedimento licitatório; e

17.10. Aplicar, garantida a ampla defesa e o contraditório, as penalidades decorrentes do descumprimento do pactuado na ata de registro de preços ou do descumprimento das obrigações contratuais, em relação às suas próprias contratações.

18. DAS COMPETÊNCIAS DO ÓRGÃO PARTICIPANTE

18.1. Garantir que os atos relativos a sua inclusão no registro de preços estejam formalizados e aprovados pela autoridade competente;

18.2. Manifestar, junto ao órgão gerenciador, mediante a utilização da Intenção de Registro de Preços, sua concordância com o objeto a ser licitado, antes da realização do procedimento licitatório; e

18.3. Tomar conhecimento da ata de registros de preços, inclusive de eventuais alterações, para o correto cumprimento de suas disposições.

18.4. Cabe ao órgão participante aplicar, garantida a ampla defesa e o contraditório, as penalidades decorrentes do descumprimento do pactuado na ata de registro de preços ou do descumprimento das obrigações contratuais, em relação às suas próprias contratações, informando as ocorrências ao órgão gerenciador.

19. DA UTILIZAÇÃO DA ATA DE REGISTRO DE PREÇOS

19.1. Desde que devidamente justificada a vantagem, a ata de registro de preços, durante sua vigência, poderá ser utilizada por qualquer órgão ou entidade da administração pública federal que não tenha participado do certame licitatório, mediante anuência da UNIFAL-MG.

19.2. Caberá ao fornecedor beneficiário da ata de registro de preços, observadas as condições nela estabelecidas, optar pela aceitação ou não do fornecimento decorrente de adesão, desde que não prejudique as obrigações presentes e futuras decorrentes da ata, assumidas com a UNIFAL-MG e órgãos participantes.

19.3. As aquisições ou contratações adicionais a que se refere este artigo não poderão exceder, por órgão ou entidade, a cem por cento dos quantitativos dos itens do Anexo I do Edital e registrados na ata de registro de preços da UNIFAL-MG e órgãos participantes.

19.4. O quantitativo decorrente das adesões à ata de registro de preços não poderá exceder, na totalidade, ao quíntuplo do quantitativo de cada item registrado na ata de registro de preços, independente do número de órgãos não participantes que aderirem.

19.5. A UNIFAL-MG somente autorizará adesão à ata após a primeira aquisição ou contratação, exceto quando, justificadamente, não houver previsão no edital para aquisição ou contratação.

19.6. Após a autorização da UNIFAL-MG, o órgão não participante deverá efetivar a aquisição ou contratação solicitada em até 90 (noventa) dias, observado o prazo de vigência da ata.

19.7. Compete ao órgão não participante os atos relativos à cobrança do cumprimento pelo fornecedor 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.

19.8. É vedada aos órgãos e entidades da administração pública federal a adesão a ata de registro de preços gerenciada por órgão ou entidade municipal, distrital ou estadual.

19.9. É facultada aos órgãos ou entidades municipais, distritais ou estaduais a adesão a ata de registro de preços da Universidade Federal de Alfenas / UNIFAL-MG.

20. DA ENTREGA DO OBJETO

20.1. Orgão Gerenciador: UASG 153028: Locais e horários para entrega: Almoxarifado Central da Universidade Federal de Alfenas – UNIFAL-MG, Rua Pio XII, 794 – Centro- Alfenas/MG – CEP 37130-000, das 7h às 10h30 e das 13h às 16h30 horas, em dias úteis, e, será recebido:

20.1.1. Provisoriamente: Será recebido pelo Almoxarifado Central, sem a verificação do conteúdo (quando embalados) apenas verificando a quantidade de volumes constante na NF-E - Nota Fiscal Eletrônica/Danfe, no ato do recebimento do material para efeito de posterior verificação de conformidade do material com as especificações constantes do edital e seus anexos, mediante a emissão do Termo de Recebimento Provisório, desde que:

20.1.1.1. Esteja compatível com esta licitação e não exista a cobrança de frete;

20.1.1.2. Estejam os produtos embalados de acordo com a nota fiscal/empenho, não enviando materiais/produtos de notas fiscais/empenhos diferentes numa mesma embalagem;

20.1.1.3. Não apresente avaria ou adulteração;

20.1.1.4. Seja o material da mesma marca e oferecida na proposta inicial, possua as mesmas características da amostra enviada, sob pena de devolução;

20.1.1.5. Seja entregue em embalagem original, contendo a data e número do lote de fabricação, informando, inclusive, seu prazo de validade:

20.1.1.5.1. Serão aceitos somente os produtos cujos prazos de validade tenham, no mínimo, 80% de validade no ato da entrega.

20.1.1.6. Esteja identificado quanto ao número da licitação, nome da Empresa, número do item a que se refere e outras informações de acordo com a legislação pertinente.

20.1.2. Definitivamente: Pelo Requisitante, após o decurso do prazo de observação ou vistoria da quantidade e qualidade dos materiais fornecidos que comprove a adequação do objeto aos termos exigidos, mediante emissão de Termo de Recebimento Definitivo.

20.2. A entrega dos materiais deverá ocorrer em perfeita consonância com o estipulado no ofício de encaminhamento da nota de empenho à empresa, no que se refere ao local de entrega.

20.2.1. Para que não haja desatendimento da exigência do item 20.2. deste Edital, alertamos às Licitantes que aguardem o recebimento do ofício e da nota de empenho e se abstenham de fazer a entrega de materiais com base em consulta ao Portal de Transparência do Governo Federal.

20.3. Após o recebimento dos materiais, mesmo que definitivamente, se, a qualquer tempo, durante a sua utilização normal, vier a se constatar discrepância com as especificações, proceder-se-á a imediata substituição dos mesmos, com ônus por exclusiva responsabilidade e custo da adjudicatária;

20.4. Prazo para entrega: até 30 (trinta) dias corridos para nacionais e até 60 (sessenta) dias para importados, contados da data do recebimento da Nota de Empenho/Contrato.

20.5. A Licitante vencedora se obriga a cumprir plenamente o previsto no artigo 71 da lei 8666/93 e suas alterações posteriores.

21. ESPECIFICAÇÕES

21.1 As soluções a serem fornecidas deverão atender aos requisitos elencados a seguir:

21.1.1 A solução a ser ofertada para cada um dos itens deve ser da marca Extreme Networks, devido a quase totalidade dos ativos de redes instalados na CONTRATANTE ser deste fabricante. O processo de padronização destes equipamentos teve início em 2010, tendo a marca sido adotada por ser a vencedora do certame licitatório realizado na época;

21.1.2 Os itens 3, 4, 5, 6, 7, 8, 11, 12, 20, 21, 22, 23, 47, 48, 49, 50 ,51, 52, 53 e 54 devem ser da marca Extreme Networks ou 100% compatíveis, compatibilidade esta que deve ser comprovada mediante documentação oficial do fabricante;

21.1.3 Todos os itens do certame, exceto os itens 1, 2 e 24 devem ser totalmente compatíveis com a Solução de Gerenciamento NetSight Base 500, já adquirida e em operação na CONTRATANTE;

21.1.4 As **Controladoras Wireless** especificados nos itens 9 e 10, os Pontos de Acesso especificado nos itens 25, 26, 27, 28, 29, 30, 31, 32, 33 e 34 e os injetores dos itens 13 e 14 devem ser totalmente compatíveis com os Access Points Extreme Networks 3715i e 3825e em operação na CONTRATANTE;

21.1.5 Os itens 1, 2 e 24 devem ser totalmente compatíveis com os Switches Extreme Networks Summit 450e, 460 e 480, Pontos de Acesso IdentiFi 3715i e 3825 e Controlador Wireless V2110, em operação na CONTRATANTE.

22. DA GARANTIA

22.1. A garantia deverá ser pelo período mínimo de 1 (um) ano;

22.1.1. Para os itens 9, 10, 20, 21, 22, 23, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44 e 45 o período mínimo de garantia deverá ser de 60 (sessenta) meses, conforme descrito no anexo I deste edital.

22.1.2. Para o item 46 o período mínimo de garantia deverá ser de 36 (trinta e seis) meses, conforme descrito no anexo I deste edital.

22.2. As despesas com o transporte (ida e volta) do equipamento defeituoso será de responsabilidade da proponente ou do fabricante;

23. DAS SANÇÕES ADMINISTRATIVAS

23.1. Comete infração administrativa, nos termos da Lei nº 10.520, de 2002, o licitante/adjudicatário que:

23.1.1. não aceitar/retirar a nota de empenho, ou não assinar a ata de registro de preço e/ou o termo de contrato, quando convocado dentro do prazo de validade da proposta;

23.1.2. apresentar documentação falsa;

23.1.3. deixar de entregar os documentos exigidos no certame;

23.1.4. ensejar o retardamento da execução do objeto;

23.1.5. não mantiver a proposta;

23.1.6. cometer fraude fiscal;

23.1.7. comportar-se de modo inidôneo;

23.2. Considera-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de participação, quanto ao enquadramento como ME/EPP ou o conluio entre os licitantes, em qualquer momento da licitação, mesmo após o encerramento da fase de lances.

23.3. O licitante/adjudicatário que cometer qualquer das infrações discriminadas no subitem anterior e na forma dos artigos 77 a 80 da Lei 8.666/93, ficará sujeito, sem prejuízo da responsabilidade civil e criminal, garantida a prévia defesa, às seguintes sanções previstas nos artigos 81 a 88 da Lei 8.666/93, artigo 7º da Lei 10.520/02, no artigo 28 do Decreto 5.450/05 e do artigo 14 do Decreto 3.555/00:

23.3.1. Advertência

23.3.2. Multa:

23.3.2.1. Multa de mora no percentual correspondente a 0,5% (zero vírgula cinco por cento), calculada sobre o valor remanescente do contrato, por dia de inadimplência, até o limite de 15 (quinze) dias úteis de atraso na entrega do material caracterizando inexecução parcial; e

23.3.2.2. Compensatória no valor de 10% (dez por cento), sobre o valor remanescente do contrato.

23.3.3. Suspensão temporária de participação em licitação com a Administração;

23.3.4. Impedimento de licitar e contratar no âmbito da União;

23.3.5. Declaração de inidoneidade.

23.4. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa ao licitante/adjudicatário, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente na Lei nº 9.784, de 1999.

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

23.6. As penalidades serão obrigatoriamente registradas no SICAF.

24. DA CONTRATAÇÃO

24.1. A contratação formalizar-se-á mediante a emissão da Nota de Empenho e Contrato, conforme minuta anexa;

24.2. A Nota de Empenho será encaminhada ao 1° classificado para o item na Ata de Registro de Preços, quando da necessidade da aquisição do material.

24.3. Será confeccionado contrato entre as partes quando houver compromisso futuro ou quando os preços ultrapassarem os limites das modalidades de licitação;

24.4. Farão parte da contratação as declarações disponibilizadas pelo COMPRASNET, o Edital e seus Anexos e a Ata de Registro de Preços.

24.5. Conforme disposto no item 8.8 da Instrução Normativa nº 05, de 21/07/95, do Ministério da Administração Federal e Reforma do Estado, será feita, pela UNIFAL-MG, a consulta junto ao SICAF (Sistema de Cadastramento Unificado de Fornecedores), previamente à contratação a ser feito para a **LICITANTE VENCEDORA**, a qual deverá manter este seu Cadastro atualizado;

25. DAS OBRIGAÇÕES DA CONTRATANTE

25.1. A UNIFAL-MG fará a conferência de todo o material adquirido;

25.2. A CONTRATANTE se obriga a efetuar o pagamento nas condições e preços pactuados;

25.3. A CONTRATANTE se reserva o direito de rejeitar os equipamentos e materiais entregues, se em desacordo com os termos deste Edital.

26. DO PAGAMENTO

26.1. O documento Fiscal terá que ser emitido obrigatoriamente com o número de inscrição no CNPJ apresentado para a Habilitação, não se admitindo documento Fiscal emitido com outro CNPJs, mesmo aqueles de filiais ou matriz;

26.2. O pagamento será efetuado no prazo máximo de 10 (dez) dias úteis, contados da data do recebimento definitivo e pela apresentação do documento fiscal, desde que atendidas às exigências deste Edital e o disposto no item 8.8 da Instrução Normativa nº 05, de 21/07/95, do Ministério da Administração Federal e Reforma do Estado, mediante crédito em Conta corrente bancária da **LICITANTE VENCEDORA**, através do Banco do Brasil S/A;

26.3. Antes de cada pagamento à contratada, será realizada consulta ao SICAF para verificar a manutenção das condições de habilitação exigidas no edital.

26.4. Constatando-se, junto ao SICAF, a situação de irregularidade da contratada, será providenciada sua advertência, por escrito, para que, no prazo de 5 (cinco) dias, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da contratante.

26.5. Não havendo regularização ou sendo a defesa considerada improcedente, a contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência da contratada, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

26.6. Persistindo a irregularidade, a contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada à contratada a ampla defesa.

26.7. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso a contratada não regularize sua situação junto ao SICAF.

26.8. Considerar-se-á como último dia útil para pagamento, o de emissão da respectiva Ordem Bancária pelo SIAFI (Sistema da administração Financeira do Governo Federal);

26.9. No pagamento serão observadas as retenções, de acordo com a legislação e normas vigentes, no âmbito da União, Estado e Município;

26.10. Poderá ser deduzido do documento Fiscal o valor de multa aplicada;

26.11. Nenhum pagamento será efetuado à **LICITANTE VENCEDORA** enquanto pendente de liquidação ou qualquer obrigação financeira que lhe for imposta, em virtude de penalidade ou inadimplência.

26.12. Nos casos de eventuais atrasos de pagamento, desde que a Contratada não tenha concorrido, de alguma forma, para tanto, fica convencionado que a taxa de compensação financeira devida pela Contratante, entre a data do vencimento e o efetivo adimplemento da parcela, é calculada mediante a aplicação da seguinte fórmula:

EM = I x N x VP, sendo:

EM = Encargos moratórios;

N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;

VP = Valor da parcela a ser paga.

I = Índice de compensação financeira = 0,00016438, assim apurado:

I = (TX) I = (6/100) I = 0,00016438

365 TX = Percentual da taxa anual = 6%.

27. DA REVISÃO DOS PREÇOS

27.1. A revisão dos preços dar-se-á, para a manutenção do equilíbrio econômico-financeiro da Ata, ou a qualquer tempo, em decorrência de eventual redução daqueles praticados no mercado, ou de fato, que eleve o custo dos serviços ou bens registrados, cabendo à UNIFAL-MG promover negociações junto aos fornecedores, conforme determinação do Decreto nº 7.892 de 23/01/2013;

27.2. Quando o preço inicialmente registrado, por motivo superveniente, tornar-se superior ao preço praticado no mercado, a UNIFAL-MG deverá:

27.2.1. Convocar o fornecedor visando a negociação para redução de preços e sua adequação ao praticado pelo mercado.

27.2.1.1. Frustrada a negociação, o fornecedor será liberado do compromisso assumido.

27.2.2. A revisão dos preços deverá ser devidamente justificada e acompanhada de documentos comprobatórios, a qual deverá ser aceita pela UNIFAL-MG ou pela empresa/ contratada;

27.2.3. A UNIFAL-MG se reserva o direito de solicitar a "lista de preços do fabricante".

27.3. Quando o preço de mercado tornar-se superior aos preços registrados e o fornecedor, mediante requerimento devidamente comprovado, não puder cumprir o compromisso, a UNIFAL-MG poderá:

27.3.1.1. Liberar o fornecedor do compromisso assumido, sem aplicação da penalidade, confirmando a veracidade dos motivos e comprovantes apresentados, e se a comunicação ocorrer antes do pedido de fornecimento;

27.3.2. Não havendo êxito nas negociações, a UNIFAL-MG revogará a Ata de Registro de Preços, adotando as medidas cabíveis para obtenção da contratação mais vantajosa.

28. DAS DISPOSIÇÕES GERAIS

28.1. A participação neste certame implica na aceitação de todas as condições estabelecidas neste Edital, bem como no Decreto 5.450 de 31 de maio de 2005;

28.2. Deverão ser observadas, no que couber, as exigências de caráter de **SUSTENTABILIDADE AMBIENTAL** constantes na **IN 01/2010** e demais normas específicas, dentre as seguintes:

28.2.1. Que os bens sejam constituídos, no todo ou em parte, por material reciclado, atóxico, biodegradável, conforme ABNT NBR – 15448-1 e 15448-2;

28.2.2. Que sejam observados os requisitos ambientais para a obtenção de certificação do Instituto Nacional de Metrologia, Normalização e Qualidade Industrial – INMETRO como produtos sustentáveis ou de menor impacto ambiental em relação aos seus similares;

28.2.3. Que os bens devam ser, preferencialmente, acondicionados em embalagem individual adequada, com o menor volume possível, que utilize materiais recicláveis, de forma a garantir a máxima proteção durante o transporte e o armazenamento;

28.2.4. Que os bens não contenham substâncias perigosas em concentração acima da recomendada na diretiva RoHS (Restriction of Certain Hazardous Substances), tais como mercúrio (Hg), chumbo (Pb), cromo hexavalente (Cr(VI)), cádmio (Cd), bifenil-polibromados (PBBs), éteres difenil-polibromados (PBDEs);

28.2.5. Que sejam utilizados produtos atóxicos ou, quando não disponíveis no mercado, de menor toxicidade;

28.2.6. Que sejam adotadas tecnologias menos agressivas ao meio ambiente;

28.2.7. Que os bens sejam econômicos quanto ao consumo de energia;

28.2.8. Que seja racionalizado o uso de matérias-primas;

28.3. A presente Licitação somente poderá vir a ser revogada por razões de interesse público, decorrentes de fato superveniente devidamente comprovado, ou anulada no todo ou em parte, por ilegalidade de ofício ou por provocação de terceiros, mediante parecer escrito e devidamente fundamentado;

28.4. O Objeto da presente Licitação poderá sofrer acréscimos, conforme previsto no Parágrafo 1º, do Art. 65 da Lei 8.666/93 e Parágrafo 2º, inciso II do mesmo Artigo, de acordo com a redação dada pela Lei 9648/98;

28.5. O Pregoeiro, no interesse da Administração, poderá relevar omissões puramente formais observadas na documentação e Proposta, desde que não contrariem a Legislação vigente e não comprometa a lisura da Licitação, sendo possível a promoção de diligência destinada a esclarecer ou a complementar a instrução do processo;

28.6. Ocorrendo, em qualquer hipótese, a negativa do fornecimento do Objeto desta licitação por parte da LICITANTE VENCEDORA, o mesmo poderá ser adjudicado às Licitantes remanescentes, na ordem de classificação e de acordo com as Propostas apresentadas, sem prejuízo às demais sanções previstas em lei;

28.7. Quaisquer esclarecimentos sobre dúvidas eventualmente suscitadas, relativas às orientações contidas no presente Edital, poderão ser solicitadas, por escrito, ao pregoeiro, exclusivamente por meio eletrônico via internet, através do e-mail: pregao@unifal-mg.edu.br;

28.8. No caso de ocorrência de feriado nacional, estadual ou municipal, ou de falta de expediente na Instituição, no dia previsto para a Abertura da Sessão Pública, o ato ficará automaticamente transferido para o primeiro dia útil seguinte, no mesmo horário;

28.9. As Licitantes arcarão com todos os custos decorrentes da elaboração e apresentação das propostas, independente da condução ou resultado do Processo Licitatório;

28.10. Na contagem dos prazos estabelecidos neste Edital excluir-se-á o dia do início e se incluirá o do vencimento;

28.11. Os casos omissos serão resolvidos com base na Lei nº 10.520/2002, Decreto nº 3.931/01 e Decreto 5.450/2005, nos regulamentos que vierem a ser adotados e, ainda, nas normas técnicas gerais ou especiais aplicáveis.

28.12. O foro para dirimir quaisquer litígios decorrentes desta Licitação é o da Justiça Federal, Subseção Judiciária de Varginha/MG, "ex vi" do artigo 109, I, da Constituição da República.

Alfenas, 18 de janeiro de 2016.

Helena Maria dos Santos Couto
Pró-Reitora Adjunta de Administração e Finanças
- UNIFAL-MG -

ANEXO I

PREGÃO ELETRÔNICO 110/2015

SIGE	Item	Descrição	UN	Qtd. Licitada	Valor Unitário R$	Valor Total R$
68997	1	Atualização Plataforma de Gerenciamento LICENSE, UPGRADE NMS-500 TO NMS-ADV-500 – Tipo 2 1. Características Gerais: 1.1 A solução deve ter características de atualização da Plataforma de Gerenciamento Tipo 1, UPGRADE NMS-BASE-500 TO NMS-500 2. Licenciamento: 2.1 Todas as licenças necessárias para o funcionamento da solução devem ser fornecidas, incluindo sistema operacional, banco de dados, etc. 2.2 Deve permitir que, no mínimo, 25 usuários administrativos acessem a ferramenta de gerenciamento simultaneamente; 2.1.3 A plataforma deve ser licenciada para gerência de, no mínimo, 500 (quinhentos) dispositivos IP do ambiente de rede; 2.1.4 Cada pilha de switches deve ser contabilizada como 1 (um) endereço IP, independentemente da quantidade de unidades na pilha. 3. Funcionalidades Gerais: 3.1 A plataforma de gerência deve permitir a integração da gerência da rede em uma única plataforma de gerenciamento, de forma centralizada. 3.2 A plataforma deve possuir arquitetura cliente servidor, com interface WEB ou java podendo ser acessível através de browser WEB padrão. 3.3 A plataforma deve possibilitar a configuração de diferentes perfis de administradores. Deve ser possível ainda criar usuários com perfil de administração e outros de apenas visualização. 3.4 A plataforma deve permitir o gerenciamento de configurações, desempenho e falhas na rede. 3.5 A plataforma deve permitir sua instalação em pelo menos uma das plataformas abaixo: 3.5.1 Windows em versões 32 ou 64 bits. 3.5.2 LINUX: SuSE Linux versão 10 ou mais recente nas plataformas 32 ou 64 bits. 3.5.3 LINUX: Red Hat Enterprise Linux versão 5 ou mais recente e nas plataformas de 32 ou 64 bits. 3.5.4 LINUX: Ubuntu versão 11 ou mais recente nas plataformas 32 ou 64 bits. 3.5.5 Appliance virtual Vmware ESXi 4 64 bits ou superior. 3.5.6 Appliance virtual Hyper-V. 3.7 A plataforma de gerenciamento deve suportar o protocolo SNMP de gerenciamento de versão 1, 2 e 3. 3.8 A plataforma de gerenciamento fornecida deve ser capaz de gerenciar equipamentos de outros fabricantes, pelo menos de forma básica. 3.9 A plataforma de gerenciamento deve permitir o descobrimento de equipamentos presentes em uma ou mais sub-redes, a fim de garantir uma auditoria constante na infraestrutura de TI. 3.10 A plataforma de gerenciamento deve permitir a criação de topologias/mapas da infraestrutura de rede através de protocolos de descobrimento. 3.11 O mapa deve	un	1		

		permitir a identificação de problemas na infraestrutura de rede através de mudança de cores. 3.12 permitir a visão agrupada da topologia conforme configuração do usuário. 3.13 A plataforma de gerenciamento deve permitir a criação, edição, remoção de VLANs nos dispositivo e associação das portas as mesmas. 3.14 A plataforma de gerenciamento deve permitir a identificação do status das portas dos dispositivos up ou down, tecnologia e velocidade das portas. 3.15 A plataforma de gerenciamento deve permitir a configuração de alarmes quando algum trap/evento ocorrer na rede. 3.16 A plataforma deve permitir a configuração gráfica de um servidor SMTP externo para o envio de informações de gerenciamento da plataforma. 3.17 A plataforma de gerenciamento deve permitir envio de e-mail ou execução de um script ou programa integrado com a plataforma para alertas. 3.18 A plataforma deve permitir o gerenciamento dos dispositivos através de uma página WEB. 3.19 A plataforma de gerenciamento deve permitir a localização de um dispositivo da rede baseado nos argumentos endereço IP, endereço MAC, user name e sub-rede. 3.20 A solução deverá prover recursos de "troubleshooting" capaz de mostrar por meio do RMON, dados presentes nos switches como performance ou estatísticas de utilização. 3.21 A plataforma de gerenciamento deve permitir o gerenciamento das configurações de filas e priorização de tráfego dos dispositivos da rede. 3.22 A plataforma de gerenciamento deve permitir a criação de perfis de classificação do tráfego nos dispositivos, baseado em usuários. 3.23 A plataforma de gerenciamento deve permitir a criação e o gerenciamento de políticas de acesso a rede nos dispositivos. 3.24 A plataforma de gerenciamento deve suportar e gerenciar graficamente as características de autenticação padrão IEEE 802.1X e via MAC. 3.25 A plataforma de gerenciamento deve permitir a configuração para atribuição de perfil de usuário com regras e QoS especifico conforme autenticação do usuário. 3.26 A plataforma de gerenciamento deve permitir a configuração gráfica de rate limit nos equipamentos gerenciados. 3.27 A plataforma de gerenciamento deve permitir a configuração estática e dinâmica da funcionalidade MAC Locking ou Port Security, para executar o LOCK de MAC Address na rede. 3.28 A plataforma de gerenciamento deve permitir a configuração gráfica de vários métodos de autenticação, atendendo, no mínimo, a configuração da autenticação WEB, autenticação MAC e autenticação IEEE 802.1X. 3.29 A plataforma deve permitir o inventário detalhado de atributos dos dispositivos da rede, atendendo, no mínimo, números seriais, versão do sistema operacional e memória. 3.30 A plataforma de gerenciamento deve permitir o armazenamento das configurações dos dispositivos. 3.31 A plataforma de gerenciamento deve permitir o agendamento da função de armazenamento de configuração de determinados elementos da rede. O agendamento deve ter periodicidade mínima de um dia. 3.32 A plataforma deve permitir a comparação da configuração atual do dispositivo com a configuração armazenada na plataforma. 3.33.				

		Deve permitir o upgrade do sistema operacional ou Boot Prom dos dispositivos, unitariamente e para um grupo de dispositivos, inclusive podendo agendar um dia e horário para que este upgrade aconteça automaticamente. 3.34 A plataforma deve permitir a execução do reset dos dispositivos. 3.35 A plataforma deve permitir restaurar a configuração armazenada. Deve ser possível ainda aplicar essa configuração em um equipamento em processo de substituição. 3.36 A plataforma deve ser capaz de coletar e exibir informações de Netflow recebidas dos equipamentos de rede. 3.37 A plataforma deve ser acessível através de dispositivos móveis tais como iPad, iPhone e Android. 3.38 A plataforma deve possuir capacidade de importar mapas ou plantas de cada localidade. 3.39 A plataforma deve permitir a visualização da localização de determinado usuário em um mapa carregado na plataforma. 3.40 A plataforma deve ser capaz de controlar e gerenciar todas as funcionalidades presentes nos Controladores Wireless, Sensores WIPS e Access Points em uma mesma console de gerenciamento. 3.41 O software deve ter capacidade de gerenciar no mínimo 5000 Access Points (APs). 3.42 O software de gerenciamento deve implantar a gerência de configuração através de interface gráfica dos controladores wireless, sensores WIPS e access points. 3.43 O software de gerenciamento deve permitir a configuração de parâmetros de QoS nos controladores wireless e access points. 3.44 O software de gerenciamento deve permitir a configuração de regras de controle de acesso nos controladores wireless e access points. 3.45. Deve implementar a gerência de configuração centralizada de soluções wireless. 3.46. Deve suportar a cobertura de rádio frequência de cada AP, facilitando a localização de problemas. 3.47. Deve possibilitar a visualização de informações de clientes incluindo: Endereço MAC, potência do sinal, taxa de transmissão, SSID, canais utilizados e AP e controladores aos quais está associado. 3.48 A plataforma deverá prover relatórios sobre os sensores que trabalham de forma dedicada (“full-time”) monitorando o ambiente de RF de forma continua. 3.50 A plataforma deverá prover relatórios sobre os sensores que trabalham de forma parcial monitorando o ambiente de RF de forma continua. 3.51 A plataforma deve prover relatórios contendo a autoclassificação de clientes e equipamentos externos ao ambiente da contratante permitindo uma coexistência no ambiente de RF. 3.52 Deve apresentar relatórios com as seguintes categorias de ameaças de um ambiente wireless: Rogue AP; Redes Ad hoc; Injeção de Pacotes; Negação de Serviço (DoS); MAC Spoofing; man-in the-midlle; Quebra de chave. 3.53. Permitir captura de pacotes no ambiente WiFi e integrar com analisador de pacotes Wireshark. 3.54. Ilustrar na planta da contratante a visualização de cobertura do ambiente de RF, bem como, distribuição de canais em 2.4 GHz e 5.0GHz. 3.55. Alertar sobre problemas de interferência de RF ou intermitência de conectividade existente no ambiente. 3.56 A plataforma de gerência deve ser capaz de fornecer relatórios históricos de tráfego de wireless. 3.57 A plataforma de gerência deve fornecer				

		dashboards da rede cabeada e sem fio, com capacidades de detalhamento. 3.58 A plataforma de gerência deve fornecer detalhes de identidade e informações de acesso. 3.59 A plataforma de gerência deve fornecer relatórios customizados para histórico e dados em tempo real. 3.60 A plataforma de gerência deve fornecer visualização e busca de clientes e seus dispositivos móveis. 3.61 A plataforma de gerência deve fornecer uma visibilidade abrangente de todos os dispositivos móveis na infraestrutura. 3.62. Deve fornecer XML APIs abertas para integração com aplicações de terceiros. 4. Garantia: 4.1 A Atualização Plataforma de Gerenciamento Tipo 2 deve permitir atualizações e suporte técnico pelo período mínimo de 12 (doze) meses. 4.2. Os chamados técnicos deverão ser gerenciados pelo fornecedor em horário comercial na modalidade 8x5 (oito horas por dia, cinco dias por semana), através de telefone gratuito. Também deve ser disponibilizado endereço de e-mail para abertura dos chamados técnicos. 4.3 A empresa deverá possuir pelo menos 1 (um) Engenheiro apto a prestar serviços de suporte técnico no equipamento proposto. O Engenheiro deverá possuir registro junto ao CREA e certificação no produto comprovada pelo fabricante. 4.4 O Fabricante deverá disponibilizar gratuitamente, suporte e atualizações dos softwares, firmwares e sistema operacional para correção de bugs e implementações de segurança; 4.5 Fornecer os softwares e suas atualizações, firmwares, sistema operacional através de meio eletrônico ou magnético sem ônus adicionais. 5. Compatibilidade: 5.1 A Atualização Plataforma de Gerenciamento Tipo 2 especificada neste item deve ser totalmente compatível com os Switches Extreme Networks Summit 450e, 460 e 480, Pontos de Acesso IdentiFi 3715i e 3825 e Controlador Wireless V2110. Referência: Marca Extreme Network, modelo LICENSE, UPGRADE NMS-500 TO NMS-ADV-500 ou de melhor qualidade. (TCU, Acórdão 2401/2006, 9.3.2 – Plenário).				
689962		Atualização Plataforma de Gerenciamento, UPGRADE NMS-BASE-500 TO NMS-500 1. Características Gerais: 1.1 A solução deve ter características de atualização da plataforma de gerenciamento Extreme Networks NetSight Base 500. 2. Licenciamento: 2.1 Todas as licenças necessárias para o funcionamento da solução devem ser fornecidas, incluindo sistema operacional, banco de dados, etc. 2.2 Deve permitir que, no mínimo, 25 usuários administrativos acessem a ferramenta de gerenciamento simultaneamente; 2.1.3 A plataforma deve ser licenciada para gerência de, no mínimo, 500 (quinhentos) dispositivos IP do ambiente de rede; 2.1.4 Cada pilha de switches deve ser contabilizada como 1 (um) endereço IP, independentemente da quantidade de unidades na pilha. 3. Funcionalidades Gerais: 3.1 A plataforma de gerência deve permitir a integração da gerência da rede em uma única plataforma de gerenciamento, de forma centralizada. 3.2 A plataforma deve possuir arquitetura cliente servidor, com interface WEB ou java podendo ser acessível através de browser WEB padrão. 3.3 A plataforma deve possibilitar a configuração de diferentes perfis de administradores. Deve	un	1		

		ser possível ainda criar usuários com perfil de administração e outros de apenas visualização. 3.4 A plataforma deve permitir o gerenciamento de configurações, desempenho e falhas na rede. 3.5 A plataforma deve permitir sua instalação em pelo menos uma das plataformas abaixo: 3.5.1 Windows em versões 32 ou 64 bits. 3.5.2 LINUX: SuSE Linux versão 10 ou mais recente nas plataformas 32 ou 64 bits. 3.5.3 LINUX: Red Hat Enterprise Linux versão 5 ou mais recente e nas plataformas de 32 ou 64 bits. 3.5.4 LINUX: Ubuntu versão 11 ou mais recente nas plataformas 32 ou 64 bits. 3.5.5 Appliance virtual Vmware ESXi 4 64 bits ou superior. 3.5.6 Appliance virtual Hyper-V. 3.7 A plataforma de gerenciamento deve suportar o protocolo SNMP de gerenciamento de versão 1, 2 e 3. 3.8 A plataforma de gerenciamento fornecida deve ser capaz de gerenciar equipamentos de outros fabricantes, pelo menos de forma básica. 3.9 A plataforma de gerenciamento deve permitir o descobrimento de equipamentos presentes em uma ou mais sub-redes, a fim de garantir uma auditoria constante na infraestrutura de TI. 3.10 A plataforma de gerenciamento deve permitir a criação de topologias/mapas da infraestrutura de rede através de protocolos de descobrimento. 3.11 O mapa deve permitir a identificação de problemas na infraestrutura de rede através de mudança de cores. 3.12. Permitir a visão agrupada da topologia conforme configuração do usuário. 3.13 A plataforma de gerenciamento deve permitir a criação, edição, remoção de VLANs nos dispositivo e associação das portas as mesmas. 3.14 A plataforma de gerenciamento deve permitir a identificação do status das portas dos dispositivos up ou down, tecnologia e velocidade das portas. 3.15 A plataforma de gerenciamento deve permitir a configuração de alarmes quando algum trap/evento ocorrer na rede. 3.16 A plataforma deve permitir a configuração gráfica de um servidor SMTP externo para o envio de informações de gerenciamento da plataforma. 3.17 A plataforma de gerenciamento deve permitir envio de e-mail ou execução de um script ou programa integrado com a plataforma para alertas. 3.18 A plataforma deve permitir o gerenciamento dos dispositivos através de uma página WEB. 3.19 A plataforma de gerenciamento deve permitir a localização de um dispositivo da rede baseado nos argumentos endereço IP, endereço MAC, user name e sub-rede. 3.20 A solução deverá prover recursos de "troubleshooting" capaz de mostrar por meio do RMON, dados presentes nos switches como performance ou estatísticas de utilização. 3.21 A plataforma de gerenciamento deve permitir o gerenciamento das configurações de filas e priorização de tráfego dos dispositivos da rede. 3.22 A plataforma de gerenciamento deve permitir a criação de perfis de classificação do tráfego nos dispositivos, baseado em usuários. 3.23 A plataforma de gerenciamento deve permitir a criação e o gerenciamento de políticas de acesso a rede nos dispositivos. 3.24 A plataforma de gerenciamento deve suportar e gerenciar graficamente as características de autenticação padrão IEEE 802.1X e via MAC. 3.25 A plataforma de gerenciamento deve permitir a configuração				

		para atribuição de perfil de usuário com regras e QoS especifico conforme autenticação do usuário. 3.26 A plataforma de gerenciamento deve permitir a configuração gráfica de rate limit nos equipamentos gerenciados. 3.27 A plataforma de gerenciamento deve permitir a configuração estática e dinâmica da funcionalidade MAC Locking ou Port Security, para executar o LOCK de MAC Address na rede. 3.28 A plataforma de gerenciamento deve permitir a configuração gráfica de vários métodos de autenticação, atendendo, no mínimo, a configuração da autenticação WEB, autenticação MAC e autenticação IEEE 802.1X. 3.29 A plataforma deve permitir o inventário detalhado de atributos dos dispositivos da rede, atendendo, no mínimo, números seriais, versão do sistema operacional e memória. 3.30 A plataforma de gerenciamento deve permitir o armazenamento das configurações dos dispositivos. 3.31 A plataforma de gerenciamento deve permitir o agendamento da função de armazenamento de configuração de determinados elementos da rede. O agendamento deve ter periodicidade mínima de um dia. 3.32 A plataforma deve permitir a comparação da configuração atual do dispositivo com a configuração armazenada na plataforma. 3.33. Deve permitir o upgrade do sistema operacional ou Boot Prom dos dispositivos, unitariamente e para um grupo de dispositivos, inclusive podendo agendar um dia e horário para que este upgrade aconteça automaticamente. 3.34 A plataforma deve permitir a execução do reset dos dispositivos. 3.35 A plataforma deve permitir restaurar a configuração armazenada. Deve ser possível ainda aplicar essa configuração em um equipamento em processo de substituição. 3.36 A plataforma deve ser capaz de coletar e exibir informações de Netflow recebidas dos equipamentos de rede. 3.37 A plataforma deve ser acessível através de dispositivos móveis tais como iPad, iPhone e Android. 3.38 A plataforma deve possuir capacidade de importar mapas ou plantas de cada localidade. 3.39 A plataforma deve permitir a visualização da localização de determinado usuário em um mapa carregado na plataforma. 3.40 A plataforma deve ser capaz de controlar e gerenciar todas as funcionalidades presentes nos Controladores Wireless, Sensores WIPS e Access Points em uma mesma console de gerenciamento. 3.41 O software deve ter capacidade de gerenciar no mínimo 5000 Access Points (APs). 3.42 O software de gerenciamento deve implantar a gerência de configuração através de interface gráfica dos controladores wireless, sensores WIPS e access points. 3.43 O software de gerenciamento deve permitir a configuração de parâmetros de QoS nos controladores wireless e access points. 3.44 O software de gerenciamento deve permitir a configuração de regras de controle de acesso nos controladores wireless e access points. 3.45. Deve implementar a gerência de configuração centralizada de soluções wireless. 3.46. Deve suportar a cobertura de rádio frequência de cada AP, facilitando a localização de problemas. 3.47. Deve possibilitar a visualização de informações de clientes incluindo: Endereço MAC, potência do sinal, taxa de transmissão, SSID, canais utilizados e AP e				

		controladores aos quais está associado. 3.48 A plataforma deverá prover relatórios sobre os sensores que trabalham de forma dedicada (“full-time”) monitorando o ambiente de RF de forma continua. 3.50 A plataforma deverá prover relatórios sobre os sensores que trabalham de forma parcial monitorando o ambiente de RF de forma continua. 3.51 A plataforma deve prover relatórios contendo a autoclassificação de clientes e equipamentos externos ao ambiente da contratante permitindo uma coexistência no ambiente de RF. 3.52 Deve apresentar relatórios com as seguintes categorias de ameaças de um ambiente wireless: Rogue AP; Redes Ad hoc; Injeção de Pacotes; Negação de Serviço (DoS); MAC Spoofing; man-in the-midlle; Quebra de chave. 3.53. Permitir captura de pacotes no ambiente WiFi e integrar com analisador de pacotes Wireshark. 3.54. Alertar sobre problemas de interferência de RF ou intermitência de conectividade existente no ambiente. 3.55 A plataforma de gerência deve ser capaz de fornecer relatórios históricos de tráfego de wireless. 3.56 A plataforma de gerência deve fornecer dashboards da rede cabeada e sem fio, com capacidades de detalhamento. 3.57 A plataforma de gerência deve fornecer detalhes de identidade e informações de acesso. 3.58 A plataforma de gerência deve fornecer relatórios customizados para histórico e dados em tempo real. 3.59 A plataforma de gerência deve fornecer visualização e busca de clientes e seus dispositivos móveis. 3.60 A plataforma de gerência deve fornecer uma visibilidade abrangente de todos os dispositivos móveis na infraestrutura. 4. Garantia: 4.1 A Atualização Plataforma de Gerenciamento Tipo 1 deve permitir atualizações e suporte técnico pelo período mínimo de 12 (doze) meses. 4.2. Os chamados técnicos deverão ser gerenciados pelo fornecedor em horário comercial na modalidade 8x5 (oito horas por dia, cinco dias por semana), através de telefone gratuito. Também deve ser disponibilizado endereço de e-mail para abertura dos chamados técnicos. 4.3 A empresa deverá possuir pelo menos 1 (um) Engenheiro apto a prestar serviços de suporte técnico no equipamento proposto. O Engenheiro deverá possuir registro junto ao CREA e certificação no produto comprovada pelo fabricante. 4.4 O Fabricante deverá disponibilizar gratuitamente, suporte e atualizações dos softwares, firmwares e sistema operacional para correção de bugs e implementações de segurança; 4.5 Fornecer os softwares e suas atualizações, firmwares, sistema operacional através de meio eletrônico ou magnético sem ônus adicionais 5. Compatibilidade: 5.1 A Atualização Plataforma de Gerenciamento Tipo 1 especificada neste item deve ser totalmente compatível com os Switches Extreme Networks Summit 450e, 460 e 480, Pontos de Acesso IdentiFi 3715i e 3825 e Controlador Wireless V2110. Referência: Marca Extreme Network, modelo UPGRADE NMS-BASE-500 TO NMS-500 ou de melhor qualidade. (TCU, Acórdão 2401/2006, 9.3.2 – Plenário).				
68967	3	Cabo de Empilhamento de 0.5 metro 1. Características Gerais: 1.1 Cabo de empilhamento com	un	60		

		velocidade mínima de 40Gbps; 1.2 Comprimento mínimo 0,5 metros; 2. Garantia: 2.1 O Cabo deverá possuir garantia do fabricante pelo período mínimo de 12 (doze) meses. 2.2. Nos casos de troca equipamentos defeituosos, os mesmos devem ser enviados no próximo dia útil subsequente a abertura do chamado e comprovação do defeito, sem quaisquer custos adicionais. 2.3. Os chamados técnicos deverão ser gerenciados pelo fornecedor em horário comercial na modalidade 8x5 (oito horas por dia, cinco dias por semana), através de telefone gratuito. Também deve ser disponibilizado endereço de e-mail para abertura dos chamados técnicos. 2.4 A empresa deverá possuir pelo menos 1 (um) Engenheiro apto a prestar serviços de suporte técnico no equipamento proposto. O Engenheiro deverá possuir registro junto ao CREA e certificação no produto comprovada pelo fabricante. 3. Compatibilidade: 3.1 Deve ser obrigatoriamente do mesmo fabricante, compatível e peça original dos Switches de Acesso.				
68968	4	Cabo de Empilhamento de 1.5 metros 1. Características Gerais: 1.1 Cabo de empilhamento com velocidade mínima de 40Gbps; 1.2 Comprimento mínimo 1,5 metros; 2. Garantia: 2.1 O Cabo deverá possuir garantia do fabricante pelo período mínimo de 12 (doze) meses. 2.2. Nos casos de troca equipamentos defeituosos, os mesmos devem ser enviados no próximo dia útil subsequente a abertura do chamado e comprovação do defeito, sem quaisquer custos adicionais. 2.3. Os chamados técnicos deverão ser gerenciados pelo fornecedor em horário comercial na modalidade 8x5 (oito horas por dia, cinco dias por semana), através de telefone gratuito. Também deve ser disponibilizado endereço de e-mail para abertura dos chamados técnicos. 2.4 A empresa deverá possuir pelo menos 1 (um) Engenheiro apto a prestar serviços de suporte técnico no equipamento proposto. O Engenheiro deverá possuir registro junto ao CREA e certificação no produto comprovada pelo fabricante. 3. Compatibilidade: 3.1 Deve ser obrigatoriamente do mesmo fabricante, compatível e peça original dos Switches de Acesso.	un	30		
68977	5	Cabo Passivo QSFP+ de 1 metro, 1m QSFP+ Passive Copper Cable 1. Características Gerais: 1.1 Cabo de Cobre PASSIVO 40 Gigabit Ethernet; 1.2 Formato Hot-Pluggable padrão QSFP+ (ambos os lados); 1.3 Comprimento mínimo 1 metros; 2. Garantia: 2.1 O Cabo deverá possuir garantia do fabricante pelo período mínimo de 12 (doze) meses. 2.2. Nos casos de troca equipamentos defeituosos, os mesmos devem ser enviados no próximo dia útil subsequente a abertura do chamado e comprovação do defeito, sem quaisquer custos adicionais. 2.3. Os chamados técnicos deverão ser gerenciados pelo fornecedor em horário comercial na modalidade 8x5 (oito horas por dia, cinco dias por semana), através de telefone gratuito. Também deve ser disponibilizado endereço de e-mail para abertura dos chamados técnicos. 2.4 A empresa deverá possuir pelo menos 1 (um) Engenheiro apto a prestar serviços de suporte técnico no equipamento proposto. O Engenheiro deverá possuir registro junto ao CREA e certificação no produto comprovada pelo fabricante. 3. Compatibilidade: 3.1 Deve ser obrigatoriamente do mesmo fabricante,	un	5		

		compatível e peça original dos Switches Distribuição. Referência: Marca Extreme Network, modelo 1m QSFP+ Passive Copper Cable ou de melhor qualidade. (TCU, Acórdão 2401/2006, 9.3.2 – Plenário).				
689786		Cabo Passivo QSFP+ de 3 metros, 3m QSFP+ Passive Copper Cable 1. Características Gerais: 1.1 Cabo de Cobre PASSIVO 40 Gigabit Ethernet; 1.2 Formato Hot-Pluggable padrão QSFP+ (ambos os lados); 1.3 Comprimento mínimo 3 metros; 2. Garantia: 2.1 O Cabo deverá possuir garantia do fabricante pelo período mínimo de 12 (doze) meses. 2.2. Nos casos de troca equipamentos defeituosos, os mesmos devem ser enviados no próximo dia útil subsequente a abertura do chamado e comprovação do defeito, sem quaisquer custos adicionais. 2.3. Os chamados técnicos deverão ser gerenciados pelo fornecedor em horário comercial na modalidade 8x5 (oito horas por dia, cinco dias por semana), através de telefone gratuito. Também deve ser disponibilizado endereço de e-mail para abertura dos chamados técnicos. 2.4 A empresa deverá possuir pelo menos 1 (um) Engenheiro apto a prestar serviços de suporte técnico no equipamento proposto. O Engenheiro deverá possuir registro junto ao CREA e certificação no produto comprovada pelo fabricante. 3. Compatibilidade: 3.1 Deve ser obrigatoriamente do mesmo fabricante, compatível e peça original dos Switches Distribuição. Referência: Marca Extreme Network, modelo 3m QSFP+ Passive Copper Cable ou de melhor qualidade. (TCU, Acórdão 2401/2006, 9.3.2 – Plenário).	6	un	10		
689757		Cabo Passivo SFP+ de 1 metro, SFP+ Cable Assembly 1M 1. Características Gerais: 1.1 Cabo de Cobre PASSIVO 10 Gigabit Ethernet; 1.2 Formato Hot-Pluggable padrão SFP+ (ambos os lados); 1.3 Comprimento mínimo 1 metro; 2. Garantia: 2.1 O Cabo deverá possuir garantia do fabricante pelo período mínimo de 12 (doze) meses. 2.2. Nos casos de troca equipamentos defeituosos, os mesmos devem ser enviados no próximo dia útil subsequente a abertura do chamado e comprovação do defeito, sem quaisquer custos adicionais. 2.3. Os chamados técnicos deverão ser gerenciados pelo fornecedor em horário comercial na modalidade 8x5 (oito horas por dia, cinco dias por semana), através de telefone gratuito. Também deve ser disponibilizado endereço de e-mail para abertura dos chamados técnicos. 2.4 A empresa deverá possuir pelo menos 1 (um) Engenheiro apto a prestar serviços de suporte técnico no equipamento proposto. O Engenheiro deverá possuir registro junto ao CREA e certificação no produto comprovada pelo fabricante. 3. Compatibilidade: 3.1 Deve ser obrigatoriamente do mesmo fabricante, compatível e peça original dos Switches Distribuição. Referência: Marca Extreme Network, modelo SFP+ Cable Assembly 1M ou de melhor qualidade. (TCU, Acórdão 2401/2006, 9.3.2 – Plenário).	7	un	1		
689768		Cabo Passivo SFP+ de 3 metros, SFP+ Cable Assembly 3M 1. Características Gerais: 1.1 Cabo de Cobre PASSIVO 10 Gigabit Ethernet; 1.2 Formato Hot-Pluggable padrão SFP+ (ambos os lados); 1.3 Comprimento mínimo 3 metros; 2. Garantia: 2.1 O Cabo deverá possuir garantia do fabricante pelo período mínimo de 12 (doze) meses. 2.2. Nos casos de troca equipamentos defeituosos, os mesmos	8	un	1		

		devem ser enviados no próximo dia útil subsequente a abertura do chamado e comprovação do defeito, sem quaisquer custos adicionais. 2.3. Os chamados técnicos deverão ser gerenciados pelo fornecedor em horário comercial na modalidade 8x5 (oito horas por dia, cinco dias por semana), através de telefone gratuito. Também deve ser disponibilizado endereço de e-mail para abertura dos chamados técnicos. 2.4 A empresa deverá possuir pelo menos 1 (um) Engenheiro apto a prestar serviços de suporte técnico no equipamento proposto. O Engenheiro deverá possuir registro junto ao CREA e certificação no produto comprovada pelo fabricante. 3. Compatibilidade: 3.1 Deve ser obrigatoriamente do mesmo fabricante, compatível e peça original dos Switches Distribuição. Referência: Marca Extreme Network, modelo SFP+ Cable Assembly 3M ou de melhor qualidade. (TCU, Acórdão 2401/2006, 9.3.2 – Plenário).				
689839		Controlador Wireless C25 WLAN CONTROLLER Tipo 1 1. Características Básicas Exigidas: 1.1 Deve ser fornecido em hardware do tipo appliance, dedicado à funcionalidade de gerenciamento e controle de APs, possuindo firmware ou sistema operacional próprio; 1.2 Deve possuir fonte de alimentação interna com seleção automática de tensão (110-220 VAC); 1.3 Permitir ser montado em rack padrão de 19 (dezenove) polegadas, incluindo todos os acessórios necessários; 1.4 Deve ser fornecido com, no mínimo, 02 (duas) portas 10/100/1000BASE-T com conectores RJ-45 fêmea para trafego de dados; 1.5 Portas de console ou de gerenciamento não serão computadas para atender essa exigência; 2. Capacidade de Controle de Access Points: 2.1 Gerenciar, no mínimo, 16 (dezesseis) Access Points (APs) simultaneamente; 2.2 Permitir a expansão do número de access points wireless através de licenças de software, sem exigir a troca de hardware ou Host VMWare; 2.3 Permitir a expansão da capacidade através de licenças de software para no mínimo um total de 48 APs por controlador; 2.4 Capacidade de gerenciar no mínimo 1024 (mil e vinte e quatro) usuários simultaneamente por controlador. 3. Modo de Operação: 3.1 O controlador WLAN poderá estar instalado em qualquer ponto da infraestrutura de rede e deve possuir a capacidade de controlar APs instalados na mesma localidade e em localidade remota através de rede WAN; 3.2 Na ocorrência de inoperância de um AP, o controlador WLAN deverá ajustar automaticamente a potência dos APs adjacentes, de modo a prover a cobertura da área não assistida; 3.3 Se controlador principal falhar, os APs relacionados no controlador principal devem ser gerenciados pelo controlador redundante sem a necessidade de intervenção ou reconfiguração; 3.4 Deve permitir sua configuração em alta disponibilidade (HA) com outro controlador de igual capacidade; 3.5 Quando um dos controladores de um par configurado como HA falhar, o controlador que restar deverá ter capacidade de assumir todos os APs e usuários do controlador com falha, adicionalmente aos APs adotados por ele e não permitindo que a rede wireless se torne inoperante; 3.6 Caso necessite de licença de software ou hardware adicional para a implementação de HA a mesma deve ser fornecida; 3.7	9	un	2		

		Implantar sistema de balanceamento de carga para associação de clientes entre APs próximos, para otimizar a performance; 3.8 Detectar áreas de sombra de cobertura e efetuar os devidos ajustes para sua correção automaticamente; 3.9 Ajustar dinamicamente o nível de potência e canal de rádio dos APs, de modo a otimizar o tamanho da célula de RF, garantindo a performance e escalabilidade; 3.10 Implantar Dynamic Radio Management (DRM) ou função semelhante de controle de rádio frequência (Canal e potência); 3.11 Implantar modo de operação com encaminhamento de tráfego diretamente no Access Point (AP), ou seja, switching no AP; 3.12 Implantar modo de operação tunelado do tráfego wireless diretamente no controlador wireless; 3.13 Deve ser possível usar os dois modos (Switching no AP e tráfego tunelado) simultaneamente; 4. Roteamento: 4.1 Deve possibilitar a configuração de rotas estáticas e OSPF; 4.2 Deve possuir DHCP relay; 5. Gerenciamento: 5.1 Implantar: RFC 3164 Syslog; SSH v2 Secure Shell v2; Telnet; TFTP; CLI (Command Line Interface); 5.2 Permitir a atualização remota do sistema operacional e dos arquivos de configuração utilizados no equipamento; 5.3 Permitir a configuração e gerenciamento seguro por meio de browser padrão (HTTPS); 5.4 Possuir porta de console para gerenciamento e configuração via linha de comando CLI ou interface Ethernet dedicada ao gerenciamento via CLI do controlador; 5.5 Permitir o armazenamento de sua configuração em memória não volátil, podendo, numa queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior à queda de alimentação; 5.6 Possuir ferramentas de debug e log de eventos para depuração e gerenciamento em primeiro nível; 5.7 Possibilitar a obtenção da configuração do equipamento através do protocolo SNMP; 6. Segurança e QoS: 6.1 Implementar em conjunto com os Access Points: 6.1.1 O padrão IEEE 802.11a; 6.1.2 O padrão IEEE 802.11b; 6.1.3 O padrão IEEE 802.11g; 6.1.4 O padrão IEEE 802.11n; 6.1.15 O padrão IEEE 802.11ac; 6.1.6 O padrão IEEE 802.11h; 6.1.7 O padrão IEEE 802.11i; 6.1.8 O padrão IEEE 802.1d; 6.1.9 RFC 2865 Radius; 6.1.10 RFC 2866 Radius Accounting; 6.1.11 RFC 2165, 2608 SLP; 6.1.12 RFC 2131 DHCP; 6.1.13 RFC 2328 OSPF; 6.1.14 RFC 1350 TFTP Protocol; 6.1.15 RFC 1155 MIB-I; 6.1.16 RFC 1213 MIB-II; 6.1.17 RFC 3576 Dynamic Authentication Extensions; 6.1.18 RFC 1305 NTP; 6.2 Deve implementar mecanismo do tipo RF Auto-Tuning, ou seja, associar dinamicamente o canal de comunicação e a potência de transmissão dos rádios dos access points e ainda reajustar estes parâmetros de forma automática sempre que for necessário; 6.3 Deve implementar servidor DHCP; 6.4 Implantar, em conjunto com o Ponto de Acesso, Qualidade de Serviço com suporte a IEEE 802.11e e WMM; 6.5 Implantar suporte a CAC (CallAdmissionControl); 6.6 Possibilitar roaming com integridade de sessão, dando suporte a aplicações em tempo real, tais como, VoWLAN e streaming de vídeo; 6.7 Implantar suporte a economia de energia com o uso do UAPSD (Unscheduled Automatic Power Save Delivery);				

		6.8 Implantar, em conjunto com o AP, o fast roaming seguro; 6.9 Implantar 802.1Q; 6.10 Implantar padrão 802.1p; 6.11 Implantar mapeamento de QoS de pacotes marcados na rede cabeada com TOS/DSCP para a rede wireless através de WMM; 6.12 Implantar protocolo de autenticação para controle do acesso administrativo ao equipamento utilizando servidor RADIUS ou TACACS+; 6.13 Suportar a autenticação com geração dinâmica de chaves criptográficas por sessão e por usuário; 6.14 Implantar listas de controle de acesso ou funcionalidade similar de controle; 6.15 Implantar filtros de acesso à rede baseados em endereços MAC; 6.16 Implantar associação dinâmica de usuário a VLAN, com base nos parâmetros da etapa de autenticação; 6.17 Implantar associação dinâmica de filtros ou ACL e de QoS, com base nos parâmetros da etapa de autenticação; 6.18 Implantar IEEE 802.11i; 6.19 Implantar IEEE 802.1X, para autenticação de clientes wireless, com pelo menos os seguintes métodos EAP: EAP-TTLS, PEAP e EAP-TLS; 6.20 Implantar a integração com RADIUS Server que suporte os métodos EAP citados; 6.21 Implantar a limitação de banda por usuário ou grupo; 6.22 Implantar, em conjunto com o AP, WEP, chaves estáticas e dinâmicas; 6.23 Implantar, em conjunto com o AP, WPA com algoritmo de criptografia TKIP; 6.24 Implantar, em conjunto com o AP, WPA2 com algoritmo de criptografia AES; 6.25 Deve possuir localmente no controlador, portal web para autenticação dos usuários visitantes, sendo possível a customização com informações e características visuais (mensagem, logo, banner, etc); 6.26 Deverá disponibilizar usuário específico para a administração e gerência do portal web, sendo que este usuário não deve ter acesso as outras informações e configurações do controlador; 6.27 O portal web de autenticação, bem como a ferramenta de administração e gerência devem ser acessadas via web nativo, sem a necessidade de instalação de nenhum software ou plug-in adicional; 6.28 A base de usuários visitantes deve ser interno ao controlador, não sendo necessário alterações (inclusão/exclusão/alteração) na base de dados dos usuários Active Directory/LDAP; 6.29 A ferramenta de criação dos usuários visitantes deverá ter uma página onde constem as informações de conta e políticas de uso da instituição, sendo possível a impressão destas informações para entrega ao visitante no momento do registro; 6.30 A criação das contas de visitantes deve possibilitar a criação de no mínimo os seguintes parâmetros: 6.30.1 Nome do usuário; 6.30.3 Senha; 6.30.2 Data de início e término de validade; 6.30.3 Tempo de sessão; 6.30.4 Horário permitido; 6.31 Deve permitir o uso de captive portal externo ao controlador. Caso sejam necessárias licenças ou hardware específico os mesmos devem ser fornecidos. 7. Garantia: 7.1 O Controlador Wireless deverá possuir garantia do fabricante pelo período mínimo de 60 (sessenta) meses. 7.2. Nos casos de troca equipamentos defeituosos, os mesmos devem ser enviados no próximo dia útil subsequente a abertura do chamado e comprovação do defeito, sem quaisquer custos adicionais. 7.3. Os				

		chamados técnicos deverão ser gerenciados pelo fornecedor em horário comercial na modalidade 8x5 (oito horas por dia, cinco dias por semana), através de telefone gratuito. Também deve ser disponibilizado endereço de e-mail para abertura dos chamados técnicos. 7.4 A empresa deverá possuir pelo menos 1 (um) Engenheiro apto a prestar serviços de suporte técnico no equipamento proposto. O Engenheiro deverá possuir registro junto ao CREA e certificação no produto comprovada pelo fabricante. 7.5 O Fabricante deverá disponibilizar gratuitamente, suporte e atualizações dos softwares, firmwares e sistema operacional para correção de bugs e implementações de segurança. 7.6. Fornecer os softwares e suas atualizações, firmwares, sistema operacional através de meio eletrônico ou magnético sem ônus adicionais. 8. Compatibilidade 8.1. Os componentes do Controlador Wireless deverão ser homologados pelo fabricante. Não será aceita a adição ou subtração de qualquer componente não original de fábrica para adequação do equipamento; Todos os componentes deverão ser compatíveis entre si, com o conjunto do equipamento e com suas funcionalidades, sem a utilização de adaptadores, fresagens, pinturas, usinagens em geral, furações, emprego de adesivos, fitas adesivas ou quaisquer outros procedimentos ou emprego de materiais inadequados ou que visem adaptar forçadamente o equipamento ou suas partes que sejam fisicamente ou logicamente incompatíveis. (Será aceito o regime de OEM desde que comprovado pelo próprio fabricante). 8.2 O Controlador Wireless especificado neste item deve ser totalmente compatível com os Access Points Extreme Networks 3715i e 3825e. 8.3 O Controlador Wireless especificado neste item deve ser totalmente compatível com a Solução de Gerenciamento NetSight Base 500. Referência: Marca Extreme Network, modelo C25 WLAN CONTROLLER ou de melhor qualidade. (TCU, Acórdão 2401/2006, 9.3.2 – Plenário).				
68984	10	Controlador Wireless WS-C5210 Tipo 2 1. Características Básicas Exigidas: 1.1 Deve ser fornecido em hardware do tipo appliance, dedicado à funcionalidade de gerenciamento e controle de APs, possuindo firmware ou sistema operacional próprio; 1.2 Deve possuir fonte de alimentação interna, redundante e com seleção automática de tensão (110-220 VAC); 1.3 Permitir ser montado em rack padrão de 19 (dezenove) polegadas, incluindo todos os acessórios necessários; 1.4 Deve ser fornecido com, no mínimo, 02 (duas) portas 10/100/1000BASE-T com conectores RJ-45 fêmea para trafego de dados; 1.5 Deve possuir mais 2 (duas) interfaces SFP+ para inserção de interfaces 10 Gigabit Ethernet; 1.6 Portas de console ou de gerenciamento não serão computadas para atender essa exigência; 2. Capacidade de Controle de Access Points: 2.1 Gerenciar, no mínimo, 100 (cem) Access Points (APs) simultaneamente; 2.2 Permitir a expansão do número de access points wireless através de licenças de software, sem exigir a troca de hardware ou Host VMWare; 2.3 Permitir a expansão da capacidade através de licenças de software para no mínimo um total de 1000 APs por controlador; 2.4 Capacidade de gerenciar no mínimo	un	2		

		16.000 (dezesseis mil) usuários simultaneamente por controlador; 3. Modo de Operação: 3.1 O controlador WLAN poderá estar instalado em qualquer ponto da infraestrutura de rede e deve possuir a capacidade de controlar APs instalados na mesma localidade e em localidade remota através de rede WAN; 3.2 Na ocorrência de inoperância de um AP, o controlador WLAN deverá ajustar automaticamente a potência dos APs adjacentes, de modo a prover a cobertura da área não assistida; 3.3 Se controlador principal falhar, os APs relacionados no controlador principal devem ser gerenciados pelo controlador redundante sem a necessidade de intervenção ou reconfiguração; 3.4 Deve permitir sua configuração em alta disponibilidade (HA) com outro controlador de igual capacidade; 3.5 Quando um dos controladores de um par configurado como HA falhar, o controlador que restar deverá ter capacidade de assumir todos os APs e usuários do controlador com falha, adicionalmente aos APs adotados por ele e não permitindo que a rede wireless se torne inoperante; 3.6 Caso necessite de licença de software ou hardware adicional para a implementação de HA a mesma deve ser fornecida; 3.7 Implantar sistema de balanceamento de carga para associação de clientes entre APs próximos, para otimizar a performance; 3.8 Detectar áreas de sombra de cobertura e efetuar os devidos ajustes para sua correção automaticamente; 3.9 Ajustar dinamicamente o nível de potência e canal de rádio dos APs, de modo a otimizar o tamanho da célula de RF, garantindo a performance e escalabilidade; 3.10 Implantar Dynamic Radio Management (DRM) ou função semelhante de controle de rádio frequência (Canal e potência); 3.11 Implantar modo de operação com encaminhamento de tráfego diretamente no Access Point (AP), ou seja, switching no AP; 3.12 Implantar modo de operação tunelado do tráfego wireless diretamente no controlador wireless; 3.13 Deve ser possível usar os dois modos (Switching no AP e tráfego tunelado) simultaneamente; 4. Roteamento: 4.1 Deve possibilitar a configuração de rotas estáticas e OSPF; 4.2 Deve possuir DHCP relay; 5. Gerenciamento: 5.1 Implantar RFC 3164 Syslog; SSH v2 Secure Shell v2; Telnet; TFTP; CLI (Command Line Interface); 5.2 Permitir a atualização remota do sistema operacional e dos arquivos de configuração utilizados no equipamento; 5.3 Permitir a configuração e gerenciamento seguro por meio de browser padrão (HTTPS); 5.4 Possuir porta de console para gerenciamento e configuração via linha de comando CLI ou interface Ethernet dedicada ao gerenciamento via CLI do controlador; 5.5 Permitir o armazenamento de sua configuração em memória não volátil, podendo, numa queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior à queda de alimentação; 5.6 Possuir ferramentas de debug e log de eventos para depuração e gerenciamento em primeiro nível; 5.7 Possibilitar a obtenção da configuração do equipamento através do protocolo SNMP; 6. Segurança e QoS: 6.1 Implementar em conjunto com os Access Points: 6.1.1 O padrão IEEE 802.11a; 6.1.2 O padrão IEEE 802.11b; 6.1.3 O				

		padrão IEEE 802.11g; 6.1.4 O padrão IEEE 802.11n; 6.1.15 O padrão IEEE 802.11ac; 6.1.6 O padrão IEEE 802.11h; 6.1.7 O padrão IEEE 802.11i; 6.1.8 O padrão IEEE 802.1d; 6.1.9 RFC 2865 Radius; 6.1.10 RFC 2866 Radius Accounting; 6.1.11 RFC 2165, 2608 SLP; 6.1.12 RFC 2131 DHCP; 6.1.13 RFC 2328 OSPF; 6.1.14 RFC 1350 TFTP Protocol; 6.1.15 RFC 1155 MIB-I; 6.1.16 RFC 1213 MIB-II; 6.1.17 RFC 3576 Dynamic Authentication Extensions; 6.1.18 RFC 1305 NTP; 6.2 Deve implementar mecanismo do tipo RF Auto-Tuning, ou seja, associar dinamicamente o canal de comunicação e a potência de transmissão dos rádios dos access points e ainda reajustar estes parâmetros de forma automática sempre que for necessário; 6.3 Deve implementar servidor DHCP; 6.4 Implantar, em conjunto com o Ponto de Acesso, Qualidade de Serviço com suporte a IEEE 802.11e e WMM; 6.5 Implantar suporte a CAC (CallAdmissionControl); 6.6 Possibilitar roaming com integridade de sessão, dando suporte a aplicações em tempo real, tais como, VoWLAN e streaming de vídeo; 6.7 Implantar suporte a economia de energia com o uso do UAPSD (Unscheduled Automatic Power Save Delivery); 6.8 Implantar, em conjunto com o AP, o fast roaming seguro; 6.9 Implantar 802.1Q; 6.10 Implantar padrão 802.1p; 6.11 Implantar mapeamento de QoS de pacotes marcados na rede cabeada com TOS/DSCP para a rede wireless através de WMM; 6.12 Implantar protocolo de autenticação para controle do acesso administrativo ao equipamento utilizando servidor RADIUS ou TACACS+; 6.13 Suportar a autenticação com geração dinâmica de chaves criptográficas por sessão e por usuário; 6.14 Implantar listas de controle de acesso ou funcionalidade similar de controle; 6.15 Implantar filtros de acesso à rede baseados em endereços MAC; 6.16 Implantar associação dinâmica de usuário a VLAN, com base nos parâmetros da etapa de autenticação; 6.17 Implantar associação dinâmica de filtros ou ACL e de QoS, com base nos parâmetros da etapa de autenticação; 6.18 Implantar IEEE 802.11i; 6.19 Implantar IEEE 802.1X, para autenticação de clientes wireless, com pelo menos os seguintes métodos EAP: EAP-TTLS, PEAP e EAP-TLS; 6.20 Implantar a integração com RADIUS Server que suporte os métodos EAP citados; 6.21 Implantar a limitação de banda por usuário ou grupo; 6.22 Implantar, em conjunto com o AP, WEP, chaves estáticas e dinâmicas; 6.23 Implantar, em conjunto com o AP, WPA com algoritmo de criptografia TKIP; 6.24 Implantar, em conjunto com o AP, WPA2 com algoritmo de criptografia AES; 6.25 Deve possuir localmente no controlador, portal web para autenticação dos usuários visitantes, sendo possível a customização com informações e características visuais (mensagem, logo, banner, etc); 6.26 Deverá disponibilizar usuário específico para a administração e gerência do portal web, sendo que este usuário não deve ter acesso as outras informações e configurações do controlador; 6.27 O portal web de autenticação, bem como a ferramenta de administração e gerência devem ser acessadas via web nativo, sem a necessidade de instalação de				

		nenhum software ou plug-in adicional; 6.28 A base de usuários visitantes deve ser interno ao controlador, não sendo necessário alterações (inclusão/exclusão/alteração) na base de dados dos usuários Active Directory/LDAP; 6.29 A ferramenta de criação dos usuários visitantes deverá ter uma página onde constem as informações de conta e políticas de uso da instituição, sendo possível a impressão destas informações para entrega ao visitante no momento do registro; 6.30 A criação das contas de visitantes deve possibilitar a criação de no mínimo os seguintes parâmetros: 6.30.1 Nome do usuário; 6.30.3 Senha; 6.30.2 Data de início e término de validade; 6.30.3 Tempo de sessão; 6.30.4 Horário permitido; 6.31 Deve permitir o uso de captive portal externo ao controlador. Caso sejam necessárias licenças ou hardware específico os mesmos devem ser fornecidos. 7. Garantia: 7.1 O Controlador Wireless deverá possuir garantia do fabricante pelo período mínimo de 60 (sessenta) meses. 7.2. Nos casos de troca equipamentos defeituosos, os mesmos devem ser enviados no próximo dia útil subsequente a abertura do chamado e comprovação do defeito, sem quaisquer custos adicionais. 7.3. Os chamados técnicos deverão ser gerenciados pelo fornecedor em horário comercial na modalidade 8x5 (oito horas por dia, cinco dias por semana), através de telefone gratuito. Também deve ser disponibilizado endereço de e-mail para abertura dos chamados técnicos. 7.4 A empresa deverá possuir pelo menos 1 (um) Engenheiro apto a prestar serviços de suporte técnico no equipamento proposto. O Engenheiro deverá possuir registro junto ao CREA e certificação no produto comprovada pelo fabricante. 7.5 O Fabricante deverá disponibilizar gratuitamente, suporte e atualizações dos softwares, firmwares e sistema operacional para correção de bugs e implementações de segurança. 7.6. Fornecer os softwares e suas atualizações, firmwares, sistema operacional através de meio eletrônico ou magnético sem ônus adicionais. 8. Compatibilidade 8.1. Os componentes do Controlador Wireless deverão ser homologados pelo fabricante. Não será aceita a adição ou subtração de qualquer componente não original de fábrica para adequação do equipamento; Todos os componentes deverão ser compatíveis entre si, com o conjunto do equipamento e com suas funcionalidades, sem a utilização de adaptadores, fresagens, pinturas, usinagens em geral, furações, emprego de adesivos, fitas adesivas ou quaisquer outros procedimentos ou emprego de materiais inadequados ou que visem adaptar forçadamente o equipamento ou suas partes que sejam fisicamente ou logicamente incompatíveis. (Será aceito o regime de OEM desde que comprovado pelo próprio fabricante). 8.2 O Controlador Wireless especificado neste item deve ser totalmente compatível com os Access Points Extreme Networks 3715i e 3825e. 8.3 O Controlador Wireless especificado neste item deve ser totalmente compatível com a Solução de Gerenciamento NetSight Base 500. Referência: Marca Extreme Network, modelo WS-C5210 ou de melhor qualidade. (TCU, Acórdão 2401/2006, 9.3.2 – Plenário).				

68979	11	Fonte de Alimentação Tipo 1 Summit 715W AC PSU FB 1. Características Gerais: 1.1 Fonte de alimentação interna que trabalhe em 100V-240V, 50/60 Hz, com detecção automática de tensão e frequência, hot-swappable. 2. Garantia: 2.1 A Fonte de Alimentação deverá possuir garantia do fabricante pelo período mínimo de 12 (doze) meses. 2.2. Nos casos de troca equipamentos defeituosos, os mesmos devem ser enviados no próximo dia útil subsequente a abertura do chamado e comprovação do defeito, sem quaisquer custos adicionais. 2.3. Os chamados técnicos deverão ser gerenciados pelo fornecedor em horário comercial na modalidade 8x5 (oito horas por dia, cinco dias por semana), através de telefone gratuito. Também deve ser disponibilizado endereço de e-mail para abertura dos chamados técnicos. 2.4 A empresa deverá possuir pelo menos 1 (um) Engenheiro apto a prestar serviços de suporte técnico no equipamento proposto. O Engenheiro deverá possuir registro junto ao CREA e certificação no produto comprovada pelo fabricante. 3. Compatibilidade: 3.2 Deve ser obrigatoriamente do mesmo fabricante, compatível e peça original do Switch Distribuição 48 portas (PoE+): Tipo 2. Referência: Marca Extreme Network, modelo Summit 715W AC PSU FB ou de melhor qualidade. (TCU, Acórdão 2401/2006, 9.3.2 – Plenário).	un	5		
68980	12	Fonte de Alimentação Tipo 2 BD 8806 600W/900W PSU 1. Características Gerais: 1.1 Fonte de alimentação interna AC 110/220V, 60Hz. 1.2. Deve ser redundante e hot swappable, deve trabalhar em load sharing de modo que a falha de uma fonte não deve implicar na parada de nenhuma função do equipamento. 1.3. Fornecer cabo de alimentação, padrão NEMA 5-15P, compatível com a fonte de alimentação ofertada. 2. Garantia: 2.1 A Fonte de Alimentação deverá possuir garantia do fabricante pelo período mínimo de 12 (doze) meses. 2.2. Nos casos de troca equipamentos defeituosos, os mesmos devem ser enviados no próximo dia útil subsequente a abertura do chamado e comprovação do defeito, sem quaisquer custos adicionais. 2.3. Os chamados técnicos deverão ser gerenciados pelo fornecedor em horário comercial na modalidade 8x5 (oito horas por dia, cinco dias por semana), através de telefone gratuito. Também deve ser disponibilizado endereço de e-mail para abertura dos chamados técnicos. 2.4 A empresa deverá possuir pelo menos 1 (um) Engenheiro apto a prestar serviços de suporte técnico no equipamento proposto. O Engenheiro deverá possuir registro junto ao CREA e certificação no produto comprovada pelo fabricante. 3. Compatibilidade: 3.1 Deve ser obrigatoriamente do mesmo fabricante, compatível e peça original do Switch Extreme Networks BlackDiamond 8806. Referência: Marca Extreme Network, modelo BD 8806 600W/900W PSU ou de melhor qualidade. (TCU, Acórdão 2401/2006, 9.3.2 – Plenário).	un	2		
68994	13	Injetor PoE PD-3501G-ENT Tipo 1 1. Características Gerais: 1.1 Possuir pelo menos 1 (uma) porta Gigabit Ethernet; 1.2 Deve ser padrão IEEE 802.3af; 1.3 Deve ser totalmente compatível e do mesmo	un	50		

		fabricante dos pontos de acesso indoor 2. Garantia: 2.1 O Injector PoE deverá possuir garantia do fabricante pelo período mínimo de 12 (doze) meses. 2.2. Nos casos de troca equipamentos defeituosos, os mesmos devem ser enviados no próximo dia útil subsequente a abertura do chamado e comprovação do defeito, sem quaisquer custos adicionais. 2.3. Os chamados técnicos deverão ser gerenciados pelo fornecedor em horário comercial na modalidade 8x5 (oito horas por dia, cinco dias por semana), através de telefone gratuito. Também deve ser disponibilizado endereço de e-mail para abertura dos chamados técnicos. 2.4 A empresa deverá possuir pelo menos 1 (um) Engenheiro apto a prestar serviços de suporte técnico no equipamento proposto. O Engenheiro deverá possuir registro junto ao CREA e certificação no produto comprovada pelo fabricante. 3. Compatibilidade: Deve ser obrigatoriamente do mesmo fabricante, compatível e peça original dos Pontos de Acesso Indoor. Referência: Marca Extreme Network, modelo PD-3501G-ENT ou de melhor qualidade. (TCU, Acórdão 2401/2006, 9.3.2 – Plenário).				
68995	14	Injetor PoE PD-9001GO-ENT Tipo 2 1. Características Gerais: 1.1 Possuir pelo menos 1 (uma) porta Gigabit Ethernet; 1.2 Deve ser padrão IEEE 802.3at (30W); 1.3 Deve ser totalmente compatível e do mesmo fabricante do ponto de acesso outdoor. 2. Garantia: 2.1 O Injector PoE deverá possuir garantia do fabricante pelo período mínimo de 12 (doze) meses. 2.2. Nos casos de troca equipamentos defeituosos, os mesmos devem ser enviados no próximo dia útil subsequente a abertura do chamado e comprovação do defeito, sem quaisquer custos adicionais. 2.3. Os chamados técnicos deverão ser gerenciados pelo fornecedor em horário comercial na modalidade 8x5 (oito horas por dia, cinco dias por semana), através de telefone gratuito. Também deve ser disponibilizado endereço de e-mail para abertura dos chamados técnicos. 2.4 A empresa deverá possuir pelo menos 1 (um) Engenheiro apto a prestar serviços de suporte técnico no equipamento proposto. O Engenheiro deverá possuir registro junto ao CREA e certificação no produto comprovada pelo fabricante 3. Compatibilidade: Deve ser obrigatoriamente do mesmo fabricante, compatível e peça original do Ponto de Acesso Outdoor. Referência: Marca Extreme Network, modelo PD-9001GO-ENT ou de melhor qualidade. (TCU, Acórdão 2401/2006, 9.3.2 – Plenário).	un	6		
68988	15	Licença para Controlador Wireless WS-APCAP-100 - Tipo 4 1. Características Gerais: 1.1 Licença adicional para adição de, no mínimo, 100 pontos de acesso no controlador wireless tipo 2. 2. Garantia: 2.1 A Licença deve permitir atualizações e suporte técnico pelo período mínimo de 12 (doze) meses. 2.2. Os chamados técnicos deverão ser gerenciados pelo fornecedor em horário comercial na modalidade 8x5 (oito horas por dia, cinco dias por semana), através de telefone gratuito. Também deve ser disponibilizado endereço de e-mail para abertura dos chamados técnicos. 2.3 A empresa deverá	tes	3		

		possuir pelo menos 1 (um) Engenheiro apto a prestar serviços de suporte técnico no equipamento proposto. O Engenheiro deverá possuir registro junto ao CREA e certificação no produto comprovada pelo fabricante. 2.4 O Fabricante deverá disponibilizar gratuitamente, suporte e atualizações dos softwares, firmwares e sistema operacional para correção de bugs e implementações de segurança; 2.5 Fornecer os softwares e suas atualizações, firmwares, sistema operacional através de meio eletrônico ou magnético sem ônus adicionais. 3. Compatibilidade: 3.1 Deve ser obrigatoriamente do mesmo fabricante, compatível e software original do Controlador Wireless Tipo 2. Referência: Marca Extreme Network, modelo WS-APCAP-100 ou de melhor qualidade. (TCU, Acórdão 2401/2006, 9.3.2 – Plenário). **(COTA PRINCIPAL)**				
68988	16	Licença para Controlador Wireless WS-APCAP-100 - Tipo 4 1. Características Gerais: 1.1 Licença adicional para adição de, no mínimo, 100 pontos de acesso no controlador wireless tipo 2. 2. Garantia: 2.1 A Licença deve permitir atualizações e suporte técnico pelo período mínimo de 12 (doze) meses. 2.2. Os chamados técnicos deverão ser gerenciados pelo fornecedor em horário comercial na modalidade 8x5 (oito horas por dia, cinco dias por semana), através de telefone gratuito. Também deve ser disponibilizado endereço de e-mail para abertura dos chamados técnicos. 2.3 A empresa deverá possuir pelo menos 1 (um) Engenheiro apto a prestar serviços de suporte técnico no equipamento proposto. O Engenheiro deverá possuir registro junto ao CREA e certificação no produto comprovada pelo fabricante. 2.4 O Fabricante deverá disponibilizar gratuitamente, suporte e atualizações dos softwares, firmwares e sistema operacional para correção de bugs e implementações de segurança; 2.5 Fornecer os softwares e suas atualizações, firmwares, sistema operacional através de meio eletrônico ou magnético sem ônus adicionais. 3. Compatibilidade: 3.1 Deve ser obrigatoriamente do mesmo fabricante, compatível e software original do Controlador Wireless Tipo 2. Referência: Marca Extreme Network, modelo WS-APCAP-100 ou de melhor qualidade. (TCU, Acórdão 2401/2006, 9.3.2 – Plenário). **(COTA RESERVADA ME/EPP/MEI) – VINCULADO AO ITEM 15**	tes	1		
68986	17	Licença para Controlador Wireless WS-APCAP-16 - Tipo 2 1. Características Gerais: 1.1 Licença adicional para adição de, no mínimo, 16 pontos de acesso no controlador wireless tipo 1. 2. Garantia: 2.1 A Licença deve permitir atualizações e suporte técnico pelo período mínimo de 12 (doze) meses. 2.2. Os chamados técnicos deverão ser gerenciados pelo fornecedor em horário comercial na modalidade 8x5 (oito horas por dia, cinco dias por semana), através de telefone gratuito. Também deve ser disponibilizado endereço de e-mail para abertura dos chamados técnicos. 2.3 A empresa deverá possuir pelo menos 1 (um) Engenheiro apto a prestar serviços de suporte técnico no equipamento proposto. O Engenheiro deverá possuir registro junto ao CREA e certificação no produto comprovada	un	2		

		pelo fabricante. 2.4 O Fabricante deverá disponibilizar gratuitamente, suporte e atualizações dos softwares, firmwares e sistema operacional para correção de bugs e implementações de segurança; 2.5 Fornecer os softwares e suas atualizações, firmwares, sistema operacional através de meio eletrônico ou magnético sem ônus adicionais. 3. Compatibilidade: 3.1 Deve ser obrigatoriamente do mesmo fabricante, compatível e software original do Controlador Wireless Tipo 1. Referência: Marca Extreme Network, modelo WS-APCAP-16 ou de melhor qualidade. (TCU, Acórdão 2401/2006, 9.3.2 – Plenário).				
68985	18	Licença para Controlador Wireless WS-APCAP-1 - Tipo 1 1. Características Gerais: 1.1 Licença adicional para adição de, no mínimo, 1 ponto de acesso no controlador wireless tipo 1. 2. Garantia: 2.1 A Licença deve permitir atualizações e suporte técnico pelo período mínimo de 12 (doze) meses. 2.2. Os chamados técnicos deverão ser gerenciados pelo fornecedor em horário comercial na modalidade 8x5 (oito horas por dia, cinco dias por semana), através de telefone gratuito. Também deve ser disponibilizado endereço de e-mail para abertura dos chamados técnicos. 2.3 A empresa deverá possuir pelo menos 1 (um) Engenheiro apto a prestar serviços de suporte técnico no equipamento proposto. O Engenheiro deverá possuir registro junto ao CREA e certificação no produto comprovada pelo fabricante. 2.4 O Fabricante deverá disponibilizar gratuitamente, suporte e atualizações dos softwares, firmwares e sistema operacional para correção de bugs e implementações de segurança; 2.5 Fornecer os softwares e suas atualizações, firmwares, sistema operacional através de meio eletrônico ou magnético sem ônus adicionais. 3. Compatibilidade: 3.1 Deve ser obrigatoriamente do mesmo fabricante, compatível e software original do Controlador Wireless Tipo 1. Referência: Marca Extreme Network, modelo WS-APCAP-1 ou de melhor qualidade. (TCU, Acórdão 2401/2006, 9.3.2 – Plenário).	un	2		
68987	19	Licença para Controlador Wireless WS-APCAP-25 - Tipo 3 1. Características Gerais: 1.1 Licença adicional para adição de, no mínimo, 25 pontos de acesso no controlador wireless tipo 2. 2. Garantia: 2.1 A Licença deve permitir atualizações e suporte técnico pelo período mínimo de 12 (doze) meses. 2.2. Os chamados técnicos deverão ser gerenciados pelo fornecedor em horário comercial na modalidade 8x5 (oito horas por dia, cinco dias por semana), através de telefone gratuito. Também deve ser disponibilizado endereço de e-mail para abertura dos chamados técnicos. 2.3 A empresa deverá possuir pelo menos 1 (um) Engenheiro apto a prestar serviços de suporte técnico no equipamento proposto. O Engenheiro deverá possuir registro junto ao CREA e certificação no produto comprovada pelo fabricante. 2.4 O Fabricante deverá disponibilizar gratuitamente, suporte e atualizações dos softwares, firmwares e sistema operacional para correção de bugs e implementações de segurança; 2.5 Fornecer os softwares e suas atualizações, firmwares, sistema operacional através de meio eletrônico ou	un	4		

		magnético sem ônus adicionais. 3. Compatibilidade: 3.1 Deve ser obrigatoriamente do mesmo fabricante, compatível e software original do Controlador Wireless Tipo 2. Referência: Marca Extreme Network, modelo WS-APCAP-25 ou de melhor qualidade. (TCU, Acórdão 2401/2006, 9.3.2 – Plenário).				
68972	20	Módulo com portas 10GBASE-T Summit X460-G2 VIM-2t 1. Características Gerais: 1.1 Módulo com 2 (duas) portas de 10 Gigabit Ethernet BASE-T. 2. Garantia: 2.1 O Módulo deverá possuir garantia do fabricante pelo período mínimo de 60 (sessenta) meses. 2.2. Nos casos de troca equipamentos defeituosos, os mesmos devem ser enviados no próximo dia útil subsequente a abertura do chamado e comprovação do defeito, sem quaisquer custos adicionais. 2.3. Os chamados técnicos deverão ser gerenciados pelo fornecedor em horário comercial na modalidade 8x5 (oito horas por dia, cinco dias por semana), através de telefone gratuito. Também deve ser disponibilizado endereço de e-mail para abertura dos chamados técnicos. 2.4 A empresa deverá possuir pelo menos 1 (um) Engenheiro apto a prestar serviços de suporte técnico no equipamento proposto. O Engenheiro deverá possuir registro junto ao CREA e certificação no produto comprovada pelo fabricante. 2.5 O Fabricante deverá disponibilizar gratuitamente, suporte e atualizações dos softwares, firmwares e sistema operacional para correção de bugs e implementações de segurança; 2.6 Fornecer os softwares e suas atualizações, firmwares, sistema operacional através de meio eletrônico ou magnético sem ônus adicionais. 3. Compatibilidade: 3.1. Os componentes do Módulo deverão ser homologados pelo fabricante. Não será aceita a adição ou subtração de qualquer componente não original de fábrica para adequação do equipamento; 14.2 Todos os componentes do Módulo deverão ser compatíveis entre si, com o conjunto do equipamento e com suas funcionalidades, sem a utilização de adaptadores, fresagens, pinturas, usinagens em geral, furações, emprego de adesivos, fitas adesivas ou quaisquer outros procedimentos ou emprego de materiais inadequados ou que visem adaptar forçadamente o equipamento ou suas partes que sejam fisicamente ou logicamente incompatíveis. (Será aceito o regime de OEM desde que comprovado pelo próprio fabricante). Referência: Marca Extreme Network, modelo Summit X460-G2 VIM-2t ou de melhor qualidade. (TCU, Acórdão 2401/2006, 9.3.2 – Plenário). **(COTA PRINCIPAL)**	un	19		
68972	21	Módulo com portas 10GBASE-T Summit X460-G2 VIM-2t 1. Características Gerais: 1.1 Módulo com 2 (duas) portas de 10 Gigabit Ethernet BASE-T. 2. Garantia: 2.1 O Módulo deverá possuir garantia do fabricante pelo período mínimo de 60 (sessenta) meses. 2.2. Nos casos de troca equipamentos defeituosos, os mesmos devem ser enviados no próximo dia útil subsequente a abertura do chamado e comprovação do defeito, sem quaisquer custos adicionais. 2.3. Os chamados técnicos deverão ser gerenciados pelo fornecedor em horário comercial na modalidade 8x5 (oito horas por dia, cinco dias por	un	6		

		semana), através de telefone gratuito. Também deve ser disponibilizado endereço de e-mail para abertura dos chamados técnicos. 2.4 A empresa deverá possuir pelo menos 1 (um) Engenheiro apto a prestar serviços de suporte técnico no equipamento proposto. O Engenheiro deverá possuir registro junto ao CREA e certificação no produto comprovada pelo fabricante. 2.5 O Fabricante deverá disponibilizar gratuitamente, suporte e atualizações dos softwares, firmwares e sistema operacional para correção de bugs e implementações de segurança; 2.6 Fornecer os softwares e suas atualizações, firmwares, sistema operacional através de meio eletrônico ou magnético sem ônus adicionais. 3. Compatibilidade: 3.1. Os componentes do Módulo deverão ser homologados pelo fabricante. Não será aceita a adição ou subtração de qualquer componente não original de fábrica para adequação do equipamento; 14.2 Todos os componentes do Módulo deverão ser compatíveis entre si, com o conjunto do equipamento e com suas funcionalidades, sem a utilização de adaptadores, fresagens, pinturas, usinagens em geral, furações, emprego de adesivos, fitas adesivas ou quaisquer outros procedimentos ou emprego de materiais inadequados ou que visem adaptar forçadamente o equipamento ou suas partes que sejam fisicamente ou logicamente incompatíveis. (Será aceito o regime de OEM desde que comprovado pelo próprio fabricante). Referência: Marca Extreme Network, modelo Summit X460-G2 VIM-2t ou de melhor qualidade. (TCU, Acórdão 2401/2006, 9.3.2 – Plenário). **(COTA RESERVADA ME/EPP/MEI) – VINCULADO AO ITEM 20**				
68973	22	Módulo com portas 40GBASE-X Summit X460-G2 VIM-2q 1. Características Gerais: 1.1 Módulo com 2 (duas) portas de 40GBASE-X QSFP+. 1.2. Deve suportar transceiver do tipo 40GBASE-SR4 e 40GBASE-LR4. 2. Garantia: 2.1 O Módulo deverá possuir garantia do fabricante pelo período mínimo de 60 (sessenta) meses. 2.2. Nos casos de troca equipamentos defeituosos, os mesmos devem ser enviados no próximo dia útil subsequente a abertura do chamado e comprovação do defeito, sem quaisquer custos adicionais. 2.3. Os chamados técnicos deverão ser gerenciados pelo fornecedor em horário comercial na modalidade 8x5 (oito horas por dia, cinco dias por semana), através de telefone gratuito. Também deve ser disponibilizado endereço de e-mail para abertura dos chamados técnicos. 2.4 A empresa deverá possuir pelo menos 1 (um) Engenheiro apto a prestar serviços de suporte técnico no equipamento proposto. O Engenheiro deverá possuir registro junto ao CREA e certificação no produto comprovada pelo fabricante. 2.5 O Fabricante deverá disponibilizar gratuitamente, suporte e atualizações dos softwares, firmwares e sistema operacional para correção de bugs e implementações de segurança; 2.6 Fornecer os softwares e suas atualizações, firmwares, sistema operacional através de meio eletrônico ou magnético sem ônus adicionais. 3. Compatibilidade: 3.1. Os componentes do Módulo deverão ser homologados pelo fabricante. Não será aceita a adição ou subtração de qualquer	un	10		

		componente não original de fábrica para adequação do equipamento; 14.2 Todos os componentes do Módulo deverão ser compatíveis entre si, com o conjunto do equipamento e com suas funcionalidades, sem a utilização de adaptadores, fresagens, pinturas, usinagens em geral, furações, emprego de adesivos, fitas adesivas ou quaisquer outros procedimentos ou emprego de materiais inadequados ou que visem adaptar forçadamente o equipamento ou suas partes que sejam fisicamente ou logicamente incompatíveis. (Será aceito o regime de OEM desde que comprovado pelo próprio fabricante). Referência: Marca Extreme Network, modelo Summit X460-G2 VIM-2q ou de melhor qualidade. (TCU, Acórdão 2401/2006, 9.3.2 – Plenário).				
68971	23	Módulo de Empilhamento Summit X460-G2 VIM-2ss 1. Características Gerais: 1.1 Módulo com 2 (duas) portas específicas para empilhamento. Tais portas devem possuir largura de banda agregada mínima de 40Gbps. 2. Garantia: 2.1 O Módulo deverá possuir garantia do fabricante pelo período mínimo de 60 (sessenta) meses. 2.2. Nos casos de troca equipamentos defeituosos, os mesmos devem ser enviados no próximo dia útil subsequente a abertura do chamado e comprovação do defeito, sem quaisquer custos adicionais. 2.3. Os chamados técnicos deverão ser gerenciados pelo fornecedor em horário comercial na modalidade 8x5 (oito horas por dia, cinco dias por semana), através de telefone gratuito. Também deve ser disponibilizado endereço de e-mail para abertura dos chamados técnicos. 2.4 A empresa deverá possuir pelo menos 1 (um) Engenheiro apto a prestar serviços de suporte técnico no equipamento proposto. O Engenheiro deverá possuir registro junto ao CREA e certificação no produto comprovada pelo fabricante. 2.5 O Fabricante deverá disponibilizar gratuitamente, suporte e atualizações dos softwares, firmwares e sistema operacional para correção de bugs e implementações de segurança; 2.6 Fornecer os softwares e suas atualizações, firmwares, sistema operacional através de meio eletrônico ou magnético sem ônus adicionais. 3. Compatibilidade: 3.1. Os componentes do Módulo deverão ser homologados pelo fabricante. Não será aceita a adição ou subtração de qualquer componente não original de fábrica para adequação do equipamento; 14.2 Todos os componentes do Módulo deverão ser compatíveis entre si, com o conjunto do equipamento e com suas funcionalidades, sem a utilização de adaptadores, fresagens, pinturas, usinagens em geral, furações, emprego de adesivos, fitas adesivas ou quaisquer outros procedimentos ou emprego de materiais inadequados ou que visem adaptar forçadamente o equipamento ou suas partes que sejam fisicamente ou logicamente incompatíveis. (Será aceito o regime de OEM desde que comprovado pelo próprio fabricante). Referência: Marca Extreme Network, modelo Summit X460-G2 VIM-2ss ou de melhor qualidade. (TCU, Acórdão 2401/2006, 9.3.2 – Plenário).	un	25		
68998	24	Plataforma de Controle de Acesso e Admissão IA-ES-3K 1. Características Gerais: 1.1 A solução	un	1		

		deverá ser do mesmo fabricante da plataforma de gerenciamento NMS-BASE-500, NMS-500 e NMS-ADV-500, permitindo seu gerenciamento através da mesma. 1.2. Deverá ser fornecida em formato OVA compatível com servidor VMware ESXi 4.0, 4.1, 5.0 ou 5.1. 2. Funcionalidades Gerais: 2.1 Deve permitir a verificação e uso em no mínimo 3.000 dispositivos/usuários. 2.2. Implementar controle de acesso à rede através de autenticação e da verificação de requisitos pré-estabelecidos, de forma a permitir, ou não, a conexão de dispositivos/usuários à rede. 2.3 O processo de autenticação deverá seguir o padrão IEEE 802.1X ou método similar que utilize protocolo seguro SSL em conjunto com servidor de políticas, e deverá permitir a alteração da VLAN do usuário conforme o perfil do mesmo. 2.4 A solução deverá ser compatível com, no mínimo, os seguintes softwares: 2.4.1 Microsoft Windows 2000, XP e Vista; 2.4.2 Anti-vírus Mcafee e Symantec. 2.5 Permitir a verificação dos seguintes itens nas estações de trabalho com sistema operacional Windows: 2.5.1 Versão do Windows e Service Pack; 2.5.2 Chaves do Registro do Windows; 2.5.3 Pacotes de atualização do Windows aplicados; 2.5.4 Existência de software antivírus instalado; 2.5.5 Status do software antivírus (habilitado ou desabilitado); 2.5.6 Se a versão e as bases de assinaturas do antivírus estão atualizadas; 2.6 Permitir autenticação e autorização de usuários utilizando a base LDAP atualmente implantada através de servidor de autenticação RADIUS. 2.7. Suportar a configuração de diversas funções, incluindo visitantes e convidados, e permitir políticas de admissão diferentes para cada função. 2.8. Suportar o controle de acesso para redes cabeadas e sem fio. 2.9. Possibilitar o acesso a convidados através de autorização explícita do funcionário responsável pelo convidado. 2.10. Permitir a criação de políticas customizáveis conforme o sistema operacional da estação sendo validada ou conforme o domínio de segurança configurado. 2.11. Suportar varredura de vulnerabilidades em dispositivos com ou sem agentes instalados. No caso de dispositivos sem agentes, será aceita solução que trabalhe com agentes temporários ou através de scans de rede. 2.12. Permitir a segregação de funções administrativas, conforme perfil de acesso (administrador de rede, administrador de segurança, help desk, etc). Essa função pode ser realizada via Ferramenta de Administração. 2.13. Permitir o backup e a restauração das políticas e configurações, diretamente no equipamento da solução ou via Ferramenta de Administração. 2.14. Suportar o envio de alarmes para um servidor SYSLOG externo. 2.15 Capacidade de visualização das seguintes informações: 2.15.1 Nome do Usuário; 2.15.2 Endereço MAC do usuário; 2.15.3 Endereço IP do usuário; 2.15.3 Perfil do usuário; 2.15.4 Sistema Operacional do usuário; 2.15.5 Resultado do processo de controle de acesso à rede. 2.16. Prover relatórios de conformidade de usuários e estações com a política de acesso. 2.17. Prover relatórios com as seguintes informações: 2.17.1 Atividades de login dos usuários; 2.17.2 Condições de erro; 2.17.3 Dispositivos/usuários em quarentena				

		ou não autorizados; 2.17.4 Dispositivos/usuários autenticados com sucesso; 2.17.5 Dispositivos/usuários não autenticados. 2.18. Permitir a exportação de relatórios via HTML ou CSV. 3. Garantia: 3.1 A Plataforma de Controle de Acesso e Admissão deve permitir atualizações e suporte técnico pelo período mínimo de 12 (doze) meses. 3.2. Os chamados técnicos deverão ser gerenciados pelo fornecedor em horário comercial na modalidade 8x5 (oito horas por dia, cinco dias por semana), através de telefone gratuito. Também deve ser disponibilizado endereço de e-mail para abertura dos chamados técnicos. 3.3 A empresa deverá possuir pelo menos 1 (um) Engenheiro apto a prestar serviços de suporte técnico no equipamento proposto. O Engenheiro deverá possuir registro junto ao CREA. 3.4 O Fabricante deverá disponibilizar gratuitamente, suporte e atualizações dos softwares, firmwares e sistema operacional para correção de bugs e implementações de segurança; 3.5 Fornecer os softwares e suas atualizações, firmwares, sistema operacional através de meio eletrônico ou magnético sem ônus adicionais. 4. Compatibilidade: 4.1 A Plataforma de Controle de Acesso e Admissão especificada neste item deve ser totalmente compatível com os Switches Extreme Networks Summit 450e, 460 e 480, Pontos de Acesso IdentiFi 3715i e 3825 e Controlador Wireless V2110. 4.2. Deverá ser do mesmo fabricante e totalmente gerenciável via Plataforma de Gerenciamento NMS-BASE-500, NMS-500 e NMS-ADV-500. Referência: Marca Extreme Network, modelo IA-ES-3K ou de melhor qualidade. (TCU, Acórdão 2401/2006, 9.3.2 – Plenário).				
68991	25	Ponto de Acesso Indoor WS-AP3715e Tipo 3: 1. Características Básicas: 1.1 Ponto de Acesso deve atender simultaneamente aos padrões: IEEE 802.11a; IEEE 802.11b; IEEE 802.11g; IEEE 802.11n; 1.2 Permitir a conexão simultânea de dispositivos configurados nos padrões: IEEE 802.11b/g/n; IEEE 802.11a/n; 1.3 Implantar funcionamento simultâneo dos rádios 2.4Ghz e 5.0 Ghz; 1.4 Implantar todas as seguintes taxas de transmissão e fallback automático: 1.4.1 IEEE 802.11a: 54, 48, 36, 24, 18, 12, 9 e 6 Mbps; 1.4.2 IEEE 802.11b: 11, 55, 2 e 1 Mbps; 1.4.3 IEEE 802.11g: 54, 48, 36, 24, 18, 12, 11, 9, 6, 55, 2 e 1 Mbps; 1.4.4 IEEE 802.11n: 300, 270, 180, 120, 60, 45, 30 e 15 Mbps; 1.4.5 IEEE 802.11n: 450, 300, 270, 180, 120, 60, 45, 30 e 15 Mbps; 1.5. Possuir e acompanhar componentes que permita sua fixação em teto e parede; 1.6 Ponto de Acesso devem ser eficientemente energizados e usar até 12.8 Watts com todas as funcionalidades habilitadas. 1.7. Ponto de Acesso deve suportar performance em conexão cabeada de 60000pps. 1.8. Ponto de Acesso deve implementar instalação plug and play. 1.9. Ponto de Acesso deve implementar análise de espectro RF. 1.10. Ponto de Acesso deve implementar um modo hibrido de operação que seja capaz de suportar varredura de segurança e atender os clientes no mesmo rádio. 1.11. Transmissão máxima de potência de cada rádio deve ser de pelo menos 26dBm em 2.4 GHz em 5 GHz. 1.12. Deve implementar associação de policies para clientes, sem precisar de	un	15		

		segmentação VIA SSIDs dedicados. 2. Portas de Rede: 2.1 Possuir pelo menos 2 (duas) portas Gigabit Ethernet 10/100/1000 Mbps, auto-sensing, com conector RJ-45 Fêmea para dados, não sendo aceito portas de gerência; 2.2 Permitir sua energização, pela interface de rede descrita no item anterior, através de um único injetor padrão IEEE 802.3af PoE. 2.3 O AP deve permitir sua operação em capacidade máxima mesmo quando energizado através do injetor PoE; 2.4 Suportar sua energização através de fonte externa ou interna que opere com tensão de entrada para a fonte, em 110-200Vac; 3. LED's e Sinalização: 3.1 Possuir LEDs indicativos do estado de operação; 3.2 Possuir LEDs indicativos da atividade dos rádios; 3.3 Possuir LEDs indicativos da atividade da interface Gigabit Ethernet; 4. Antenas: 4.1. Possuir 6 (seis) antenas externas ao AP, em conformidade com o padrão IEEE 802.11a/b/g/n; 4.2. Possuir ganho de, pelo menos, 3dBi para 2.4. GHz; 4.3. Possuir ganho de, pelo menos, 3dBi para 5.0 GHz; 4.4 Que implante padrão de irradiação omnidirecional; 4.5. Que implante operação simultânea em 3x3:3 MIMO; 5. Modo de Operação: 5.1 Implantar modo de operação onde o AP possa estar remotamente conectado ao controlador wireless tanto de forma direta em uma rede de camada 2 ou em qualquer ponto de uma rede segmentada em subredes de camada 3; 5.2 O ponto de acesso deve permitir sua operação através da conexão a um controlador principal e a um controlador secundário; 5.3 Selecionar automaticamente o canal de transmissão; 5.4 Ajustar dinamicamente o nível de potência e canal de rádio; 5.5 Possuir suporte a pelo menos 8 SSIDs para 2.4Ghz e 8 SSIDs para 5.0Ghz; 5.6 Permitir habilitar e desabilitar a divulgação do SSID; 5.7 Deve implementar Fast Roaming ou funcionalidade similar de forma a garantir o Roaming sem perda de conexão; 5.8 Não deve haver licença restringindo o número de usuários por AP. 5.9 Implantar a pilha de protocolos TCP/IP; 5.10 Implantar VLANs conforme padrão IEEE 802.1Q; 5.11 Implantar cliente DHCP, para configuração automática de rede; 5.12 Configurar-se automaticamente ao ser conectado na rede; 6. Gerenciamento: 6.1 Possuir porta de console para configuração; 6.2 Permitir via controlador wireless, a atualização remota do sistema operacional; 6.3 Permitir via controlador wireless, a atualização remota dos arquivos de configuração utilizados no equipamento; 6.4 Implantar funcionamento em modo gerenciado pelo controlador wireless; 7. Segurança e QoS: 7.1 Possuir entrada para dispositivo antifurto do tipo Kensingtonlock ou similar; 7.2 Implementar varredura de Rádio Frequência nas tecnologias 802.11a, 802.11b/g e 802.11n para identificação de AP não autorizados (rogues); 7.3 Implementar varredura de Rádio Frequência nas tecnologias 802.11a, 802.11b/g e 802.11n para identificação de interferências nos canais na rede WLAN; 7.4 Implementar IEEE 802.1x de acesso do próprio AP a rede cabeada; 7.5 Implementar autenticação com geração dinâmica de chaves criptográficas por sessão e por usuário; 7.6 Implementar em conjunto com o Controlador WLAN, WEP, chaves estáticas e dinâmicas; 7.7				

		Implementar em conjunto com o Controlador WLAN, WPA com algoritmo de criptografia TKIP e MIC; 7.8 Implementar em conjunto com o Controlador WLAN, WPA2 com algoritmo de criptografia AES; 7.9 Implementar padrão IEEE 802.11e WMM da Wi-Fi Alliance para priorização de tráfego, suportando aplicações em tempo real, tais como VoIP e vídeo; 7.10 O sistema de monitoração e controle de RF deve possuir mecanismos de detecção e prevenção de intrusos no ambiente wireless; 7.11 Implantar modo de operação onde o WIPS possa estar remotamente conectado ao controlador wireless tanto de forma direta em uma rede de camada 2 ou em qualquer ponto de uma rede segmentada em sub-redes de camada 3; 7.12 O WIPS deve permitir sua operação através da conexão a um controlador principal ou controlador secundário, realizando detecção de: 7.12.1 Rogue AP; 7.12.2 Honeypot; 7.12.3 Packet Injection; 7.12.4 Redes Ad Hoc; 7.12.5 Main-in-the-middle; 7.12.6 Negação de Serviço (DoS); 7.12.7 MAC Spoofing; 7.12.8 Tentativa de quebra de chaves; 7.12.9 Reconhecimento de rede; 8. Certificações: 8.1 Possuir certificação da Wi-Fi Alliance. 8.2. Possuir certificação/homologação da ANATEL. 9. Garantia: 9.1 O Ponto de Acesso deverá possuir garantia do fabricante pelo período mínimo de 60 (sessenta) meses. 9.2. Nos casos de troca equipamentos defeituosos, os mesmos devem ser enviados no próximo dia útil subsequente a abertura do chamado e comprovação do defeito, sem quaisquer custos adicionais. 9.3. Os chamados técnicos deverão ser gerenciados pelo fornecedor em horário comercial na modalidade 8x5 (oito horas por dia, cinco dias por semana), através de telefone gratuito. Também deve ser disponibilizado endereço de e-mail para abertura dos chamados técnicos. 9.4 A empresa deverá possuir pelo menos 1 (um) Engenheiro apto a prestar serviços de suporte técnico no equipamento proposto. O Engenheiro deverá possuir registro junto ao CREA e certificação no produto comprovada pelo fabricante. 9.5 O Fabricante deverá disponibilizar gratuitamente, suporte e atualizações dos softwares, firmwares e sistema operacional para correção de bugs e implementações de segurança. 9.6. Fornecer os softwares e suas atualizações, firmwares, sistema operacional através de meio eletrônico ou magnético sem ônus adicionais. 10. Compatibilidade: 10.1. Os componentes do Ponto de Acesso deverão ser homologados pelo fabricante. Não será aceita a adição ou subtração de qualquer componente não original de fábrica para adequação do equipamento; Todos os componentes deverão ser compatíveis entre si, com o conjunto do equipamento e com suas funcionalidades, sem a utilização de adaptadores, fresagens, pinturas, usinagens em geral, furações, emprego de adesivos, fitas adesivas ou quaisquer outros procedimentos ou emprego de materiais inadequados ou que visem adaptar forçadamente o equipamento ou suas partes que sejam fisicamente ou logicamente incompatíveis. (Será aceito o regime de OEM desde que comprovado pelo próprio fabricante). 10.2 O Ponto de Acesso especificado neste item deve ser				

		totalmente compatível com o Controlador Wireless Extreme Networks V2110. 10.3 O Ponto de Acesso especificado neste item deve ser totalmente compatível com a Solução de Gerenciamento NetSight Base 500. Referência: Marca Extreme Network, modelo WS-AP3715e ou de melhor qualidade. (TCU, Acórdão 2401/2006, 9.3.2 – Plenário). **(COTA PRINCIPAL)**				
68991	26	Ponto de Acesso Indoor WS-AP3715e Tipo 3: 1. Características Básicas: 1.1 Ponto de Acesso deve atender simultaneamente aos padrões: IEEE 802.11a; IEEE 802.11b; IEEE 802.11g; IEEE 802.11n; 1.2 Permitir a conexão simultânea de dispositivos configurados nos padrões: IEEE 802.11b/g/n; IEEE 802.11a/n; 1.3 Implantar funcionamento simultâneo dos rádios 2.4Ghz e 5.0 Ghz; 1.4 Implantar todas as seguintes taxas de transmissão e fallback automático: 1.4.1 IEEE 802.11a: 54, 48, 36, 24, 18, 12, 9 e 6 Mbps; 1.4.2 IEEE 802.11b: 11, 55, 2 e 1 Mbps; 1.4.3 IEEE 802.11g: 54, 48, 36, 24, 18, 12, 11, 9, 6, 55, 2 e 1 Mbps; 1.4.4 IEEE 802.11n: 300, 270, 180, 120, 60, 45, 30 e 15 Mbps; 1.4.5 IEEE 802.11n: 450, 300, 270, 180, 120, 60, 45, 30 e 15 Mbps; 1.5. Possuir e acompanhar componentes que permita sua fixação em teto e parede; 1.6 Ponto de Acesso devem ser eficientemente energizados e usar até 12.8 Watts com todas as funcionalidades habilitadas. 1.7. Ponto de Acesso deve suportar performance em conexão cabeada de 60000pps. 1.8. Ponto de Acesso deve implementar instalação plug and play. 1.9. Ponto de Acesso deve implementar análise de espectro RF. 1.10. Ponto de Acesso deve implementar um modo hibrido de operação que seja capaz de suportar varredura de segurança e atender os clientes no mesmo rádio. 1.11. Transmissão máxima de potência de cada rádio deve ser de pelo menos 26dBm em 2.4 GHz em 5 GHz. 1.12. Deve implementar associação de policies para clientes, sem precisar de segmentação VIA SSIDs dedicados. 2. Portas de Rede: 2.1 Possuir pelo menos 2 (duas) portas Gigabit Ethernet 10/100/1000 Mbps, auto-sensing, com conector RJ-45 Fêmea para dados, não sendo aceito portas de gerência; 2.2 Permitir sua energização, pela interface de rede descrita no item anterior, através de um único injetor padrão IEEE 802.3af PoE. 2.3 O AP deve permitir sua operação em capacidade máxima mesmo quando energizado através do injetor PoE; 2.4 Suportar sua energização através de fonte externa ou interna que opere com tensão de entrada para a fonte, em 110-200Vac; 3. LED’s e Sinalização: 3.1 Possuir LEDs indicativos do estado de operação; 3.2 Possuir LEDs indicativos da atividade dos rádios; 3.3 Possuir LEDs indicativos da atividade da interface Gigabit Ethernet; 4. Antenas: 4.1. Possuir 6 (seis) antenas externas ao AP, em conformidade com o padrão IEEE 802.11a/b/g/n; 4.2. Possuir ganho de, pelo menos, 3dBi para 2.4. GHz; 4.3. Possuir ganho de, pelo menos, 3dBi para 5.0 GHz; 4.4 Que implante padrão de irradiação omnidirecional; 4.5. Que implante operação simultânea em 3x3:3 MIMO; 5. Modo de Operação: 5.1 Implantar modo de operação onde o AP possa estar remotamente conectado ao controlador wireless tanto de forma direta em uma rede de	un	5		

		camada 2 ou em qualquer ponto de uma rede segmentada em subredes de camada 3; 5.2 O ponto de acesso deve permitir sua operação através da conexão a um controlador principal e a um controlador secundário; 5.3 Selecionar automaticamente o canal de transmissão; 5.4 Ajustar dinamicamente o nível de potência e canal de rádio; 5.5 Possuir suporte a pelo menos 8 SSIDs para 2.4Ghz e 8 SSIDs para 5.0Ghz; 5.6 Permitir habilitar e desabilitar a divulgação do SSID; 5.7 Deve implementar Fast Roaming ou funcionalidade similar de forma a garantir o Roaming sem perda de conexão; 5.8 Não deve haver licença restringindo o número de usuários por AP. 5.9 Implantar a pilha de protocolos TCP/IP; 5.10 Implantar VLANs conforme padrão IEEE 802.1Q; 5.11 Implantar cliente DHCP, para configuração automática de rede; 5.12 Configurar-se automaticamente ao ser conectado na rede; 6. Gerenciamento: 6.1 Possuir porta de console para configuração; 6.2 Permitir via controlador wireless, a atualização remota do sistema operacional; 6.3 Permitir via controlador wireless, a atualização remota dos arquivos de configuração utilizados no equipamento; 6.4 Implantar funcionamento em modo gerenciado pelo controlador wireless; 7. Segurança e QoS: 7.1 Possuir entrada para dispositivo antifurto do tipo Kensingtonlock ou similar; 7.2 Implementar varredura de Rádio Frequência nas tecnologias 802.11a, 802.11b/g e 802.11n para identificação de AP não autorizados (rogues); 7.3 Implementar varredura de Rádio Frequência nas tecnologias 802.11a, 802.11b/g e 802.11n para identificação de interferências nos canais na rede WLAN; 7.4 Implementar IEEE 802.1x de acesso do próprio AP a rede cabeada; 7.5 Implementar autenticação com geração dinâmica de chaves criptográficas por sessão e por usuário; 7.6 Implementar em conjunto com o Controlador WLAN, WEP, chaves estáticas e dinâmicas; 7.7 Implementar em conjunto com o Controlador WLAN, WPA com algoritmo de criptografia TKIP e MIC; 7.8 Implementar em conjunto com o Controlador WLAN, WPA2 com algoritmo de criptografia AES; 7.9 Implementar padrão IEEE 802.11e WMM da Wi-Fi Alliance para priorização de tráfego, suportando aplicações em tempo real, tais como VoIP e vídeo; 7.10 O sistema de monitoração e controle de RF deve possuir mecanismos de detecção e prevenção de intrusos no ambiente wireless; 7.11 Implantar modo de operação onde o WIPS possa estar remotamente conectado ao controlador wireless tanto de forma direta em uma rede de camada 2 ou em qualquer ponto de uma rede segmentada em sub-redes de camada 3; 7.12 O WIPS deve permitir sua operação através da conexão a um controlador principal ou controlador secundário, realizando detecção de: 7.12.1 Rogue AP; 7.12.2 Honeypot; 7.12.3 Packet Injection; 7.12.4 Redes Ad Hoc; 7.12.5 Main-in-the-middle; 7.12.6 Negação de Serviço (DoS); 7.12.7 MAC Spoofing; 7.12.8 Tentativa de quebra de chaves; 7.12.9 Reconhecimento de rede; 8. Certificações: 8.1 Possuir certificação da Wi-Fi Alliance. 8.2. Possuir certificação/homologação da ANATEL. 9. Garantia: 9.1 O Ponto de Acesso deverá possuir garantia do				

		fabricante pelo período mínimo de 60 (sessenta) meses. 9.2. Nos casos de troca equipamentos defeituosos, os mesmos devem ser enviados no próximo dia útil subsequente a abertura do chamado e comprovação do defeito, sem quaisquer custos adicionais. 9.3. Os chamados técnicos deverão ser gerenciados pelo fornecedor em horário comercial na modalidade 8x5 (oito horas por dia, cinco dias por semana), através de telefone gratuito. Também deve ser disponibilizado endereço de e-mail para abertura dos chamados técnicos. 9.4 A empresa deverá possuir pelo menos 1 (um) Engenheiro apto a prestar serviços de suporte técnico no equipamento proposto. O Engenheiro deverá possuir registro junto ao CREA e certificação no produto comprovada pelo fabricante. 9.5 O Fabricante deverá disponibilizar gratuitamente, suporte e atualizações dos softwares, firmwares e sistema operacional para correção de bugs e implementações de segurança. 9.6. Fornecer os softwares e suas atualizações, firmwares, sistema operacional através de meio eletrônico ou magnético sem ônus adicionais. 10. Compatibilidade: 10.1. Os componentes do Ponto de Acesso deverão ser homologados pelo fabricante. Não será aceita a adição ou subtração de qualquer componente não original de fábrica para adequação do equipamento; Todos os componentes deverão ser compatíveis entre si, com o conjunto do equipamento e com suas funcionalidades, sem a utilização de adaptadores, fresagens, pinturas, usinagens em geral, furações, emprego de adesivos, fitas adesivas ou quaisquer outros procedimentos ou emprego de materiais inadequados ou que visem adaptar forçadamente o equipamento ou suas partes que sejam fisicamente ou logicamente incompatíveis. (Será aceito o regime de OEM desde que comprovado pelo próprio fabricante). 10.2 O Ponto de Acesso especificado neste item deve ser totalmente compatível com o Controlador Wireless Extreme Networks V2110. 10.3 O Ponto de Acesso especificado neste item deve ser totalmente compatível com a Solução de Gerenciamento NetSight Base 500. Referência: Marca Extreme Network, modelo WS-AP3715e ou de melhor qualidade. (TCU, Acórdão 2401/2006, 9.3.2 – Plenário). **(COTA RESERVADA ME/EPP/MEI) – VINCULADO AO ITEM 25**				
68989	27	Ponto de Acesso Indoor WS-AP3715i Tipo 1: 1. Características Básicas: 1.1 Ponto de Acesso deve atender simultaneamente aos padrões: IEEE 802.11a; IEEE 802.11b; IEEE 802.11g; IEEE 802.11n; 1.2. Permitir a conexão simultânea de dispositivos configurados nos padrões: IEEE 802.11b/g/n; IEEE 802.11a/n; 1.3. Implantar funcionamento simultâneo dos rádios 2.4Ghz e 5.0 Ghz; 1.4. Implantar todas as seguintes taxas de transmissão e fallback automático: 1.4.1. IEEE 802.11a: 54, 48, 36, 24, 18, 12, 9 e 6 Mbps; 1.4.2. IEEE 802.11b: 11, 55, 2 e 1 Mbps; 1.4.3. IEEE 802.11g: 54, 48, 36, 24, 18, 12, 11, 9, 6, 55, 2 e 1 Mbps; 1.4.4. IEEE 802.11n: 300, 270, 180, 120, 60, 45, 30 e 15 Mbps; 1.4.5. IEEE 802.11n: 450, 300, 270, 180, 120, 60, 45, 30 e 15 Mbps; 1.5. Possuir e acompanhar componentes que permita sua fixação em teto e parede; 1.6. Ponto de Acesso devem ser eficientemente energizados e usar até 12.8	un	15		

		Watts com todas as funcionalidades habilitadas. 1.7. Ponto de Acesso deve suportar performance em conexão cabeada de 60000pps. 1.8. Ponto de Acesso deve implementar instalação plug and play. 1.9. Ponto de Acesso deve implementar análise de espectro RF. 1.10. Ponto de Acesso deve implementar um modo hibrido de operação que seja capaz de suportar varredura de segurança e atender os clientes no mesmo rádio. 1.11. Transmissão máxima de potência de cada rádio deve ser de pelo menos 26dBm em 2.4 GHz e em 5 GHz. 1.12. Deve implementar associação de policies para clientes, sem precisar de segmentação VIA SSIDs dedicados. 2. Portas de Rede: 2.1 Possuir pelo menos 2 (duas) portas Gigabit Ethernet 10/100/1000 Mbps, auto-sensing, com conector RJ-45 Fêmea para dados, não sendo aceito portas de gerência; 2.2 Permitir sua energização, pela interface de rede descrita no item anterior, através de um único injetor padrão IEEE 802.3af PoE. 2.3 O ponto de acesso deve permitir sua operação em capacidade máxima mesmo quando energizado através do injetor PoE; 2.4 O ponto de acesso deve permitir sua energização através de fonte externa ou interna que opere com tensão de entrada para a fonte, em 110-200Vac; 3. LED's e Sinalização: 3.1 Possuir LEDs indicativos do estado de operação; 3.2 Possuir LEDs indicativos da atividade dos rádios; 3.3 Possuir LEDs indicativos da atividade da interface Gigabit Ethernet; 4. Antenas: 4.1 Possuir antenas internas ao ponto de acesso, em conformidade com o padrão IEEE 802.11a/b/g/n; 4.2 Com ganho de, pelo menos, 5dBi para 2.4 GHz; 4.3. Com ganho de, pelo menos, 5dBi para 5.0 GHz; 4.4 Que implante padrão de irradiação omnidirecional; 4.1.5 Que implante operação simultânea em 3x3:3 MIMO; 5. Modo de Operação: 5.1 Implantar modo de operação onde o AP possa estar remotamente conectado ao controlador wireless tanto de forma direta em uma rede de camada 2 ou em qualquer ponto de uma rede segmentada em subredes de camada 3; 5.2 O ponto de acesso deve permitir sua operação através da conexão a um controlador principal e a um controlador secundário; 5.3 Selecionar automaticamente o canal de transmissão; 5.4 Ajustar dinamicamente o nível de potência e canal de rádio; 5.5 Possuir suporte a pelo menos 8 SSIDs para 2.4Ghz e 8 SSIDs para 5.0Ghz; 5.6 Permitir habilitar e desabilitar a divulgação do SSID; 5.7 Deve implementar Fast Roaming ou funcionalidade similar de forma a garantir o Roaming sem perda de conexão; 5.8 Não deve haver licença restringindo o número de usuários por AP. 5.9 Implantar a pilha de protocolos TCP/IP; 5.10 Implantar VLANs conforme padrão IEEE 802.1Q; 5.11 Implantar cliente DHCP, para configuração automática de rede; 5.12 Configurar-se automaticamente ao ser conectado na rede; 6. Gerenciamento: 6.1 Possuir porta de console para configuração; 6.2 Permitir via controlador wireless, a atualização remota do sistema operacional; 6.3 Permitir via controlador wireless, a atualização remota dos arquivos de configuração utilizados no equipamento; 6.4 Implantar funcionamento em modo gerenciado pelo controlador wireless; 7. Segurança e QoS: 7.1 Possuir entrada para dispositivo antifurto do tipo				

		Kensingtonlock ou similar; 7.2 Implementar varredura de Rádio Frequência nas tecnologias 802.11a, 802.11b/g e 802.11n para identificação de AP não autorizados (rogues); 7.3 Implementar varredura de Rádio Frequência nas tecnologias 802.11a, 802.11b/g e 802.11n para identificação de interferências nos canais na rede WLAN; 7.4 Implementar IEEE 802.1x de acesso do próprio AP a rede cabeada; 7.5 Implementar autenticação com geração dinâmica de chaves criptográficas por sessão e por usuário; 7.6 Implementar em conjunto com o Controlador WLAN, WEP, chaves estáticas e dinâmicas; 7.7 Implementar em conjunto com o Controlador WLAN, WPA com algoritmo de criptografia TKIP e MIC; 7.8 Implementar em conjunto com o Controlador WLAN, WPA2 com algoritmo de criptografia AES; 7.9 Implementar padrão IEEE 802.11e WMM da Wi-Fi Alliance para priorização de tráfego, suportando aplicações em tempo real, tais como VoIP e vídeo; 7.10 O sistema de monitoração e controle de RF deve possuir mecanismos de detecção e prevenção de intrusos no ambiente wireless; 7.11 Implantar modo de operação onde o WIPS possa estar remotamente conectado ao controlador wireless tanto de forma direta em uma rede de camada 2 ou em qualquer ponto de uma rede segmentada em subredes de camada 3; 7.12 O WIPS deve permitir sua operação através da conexão a um controlador principal ou controlador secundário, realizando detecção de: 7.12.1 Rogue AP; 7.12.2 Honeypot; 7.12.3 Packet Injection; 7.12.4 Redes Ad Hoc; 7.12.5 Main-in-the-middle; 7.12.6 Negação de Serviço (DoS); 7.12.7 MAC Spoofing; 7.12.8 Tentativa de quebra de chaves; 7.12.9 Reconhecimento de rede; 8. Certificações: 8.1 Possuir certificação da Wi-Fi Alliance. 8.2. Possuir certificação/homologação da ANATEL. 9. Garantia: 9.1 O Ponto de Acesso deverá possuir garantia do fabricante pelo período mínimo de 60 (sessenta) meses. 9.2. Nos casos de troca equipamentos defeituosos, os mesmos devem ser enviados no próximo dia útil subsequente a abertura do chamado e comprovação do defeito, sem quaisquer custos adicionais. 9.3. Os chamados técnicos deverão ser gerenciados pelo fornecedor em horário comercial na modalidade 8x5 (oito horas por dia, cinco dias por semana), através de telefone gratuito. Também deve ser disponibilizado endereço de e-mail para abertura dos chamados técnicos. 9.4 A empresa deverá possuir pelo menos 1 (um) Engenheiro apto a prestar serviços de suporte técnico no equipamento proposto. O Engenheiro deverá possuir registro junto ao CREA e certificação no produto comprovada pelo fabricante. 9.5 O Fabricante deverá disponibilizar gratuitamente, suporte e atualizações dos softwares, firmwares e sistema operacional para correção de bugs e implementações de segurança. 9.6. Fornecer os softwares e suas atualizações, firmwares, sistema operacional através de meio eletrônico ou magnético sem ônus adicionais. 10. Compatibilidade: 10.1. Os componentes do Ponto de Acesso deverão ser homologados pelo fabricante. Não será aceita a adição ou subtração de qualquer componente não original de fábrica para adequação				

		do equipamento; Todos os componentes deverão ser compatíveis entre si, com o conjunto do equipamento e com suas funcionalidades, sem a utilização de adaptadores, fresagens, pinturas, usinagens em geral, furações, emprego de adesivos, fitas adesivas ou quaisquer outros procedimentos ou emprego de materiais inadequados ou que visem adaptar forçadamente o equipamento ou suas partes que sejam fisicamente ou logicamente incompatíveis. (Será aceito o regime de OEM desde que comprovado pelo próprio fabricante). 10.2 O Ponto de Acesso especificado neste item deve ser totalmente compatível com o Controlador Wireless Extreme Networks V2110. 10.3 O Ponto de Acesso especificado neste item deve ser totalmente compatível com a Solução de Gerenciamento NetSight Base 500. Referência: Marca Extreme Network, modelo WS-AP3715i ou de melhor qualidade. (TCU, Acórdão 2401/2006, 9.3.2 – Plenário). **(COTA PRINCIPAL)**				
68989	28	Ponto de Acesso Indoor WS-AP3715i Tipo 1: 1. Características Básicas: 1.1 Ponto de Acesso deve atender simultaneamente aos padrões: IEEE 802.11a; IEEE 802.11b; IEEE 802.11g; IEEE 802.11n; 1.2. Permitir a conexão simultânea de dispositivos configurados nos padrões: IEEE 802.11b/g/n; IEEE 802.11a/n; 1.3. Implantar funcionamento simultâneo dos rádios 2.4Ghz e 5.0 Ghz; 1.4. Implantar todas as seguintes taxas de transmissão e fallback automático: 1.4.1. IEEE 802.11a: 54, 48, 36, 24, 18, 12, 9 e 6 Mbps; 1.4.2. IEEE 802.11b: 11, 55, 2 e 1 Mbps; 1.4.3. IEEE 802.11g: 54, 48, 36, 24, 18, 12, 11, 9, 6, 55, 2 e 1 Mbps; 1.4.4. IEEE 802.11n: 300, 270, 180, 120, 60, 45, 30 e 15 Mbps; 1.4.5. IEEE 802.11n: 450, 300, 270, 180, 120, 60, 45, 30 e 15 Mbps; 1.5. Possuir e acompanhar componentes que permita sua fixação em teto e parede; 1.6. Ponto de Acesso devem ser eficientemente energizados e usar até 12.8 Watts com todas as funcionalidades habilitadas. 1.7. Ponto de Acesso deve suportar performance em conexão cabeada de 60000pps. 1.8. Ponto de Acesso deve implementar instalação plug and play. 1.9. Ponto de Acesso deve implementar análise de espectro RF. 1.10. Ponto de Acesso deve implementar um modo hibrido de operação que seja capaz de suportar varredura de segurança e atender os clientes no mesmo rádio. 1.11. Transmissão máxima de potência de cada rádio deve ser de pelo menos 26dBm em 2.4 GHz e em 5 GHz. 1.12. Deve implementar associação de policies para clientes, sem precisar de segmentação VIA SSIDs dedicados. 2. Portas de Rede: 2.1 Possuir pelo menos 2 (duas) portas Gigabit Ethernet 10/100/1000 Mbps, auto-sensing, com conector RJ-45 Fêmea para dados, não sendo aceito portas de gerência; 2.2 Permitir sua energização, pela interface de rede descrita no item anterior, através de um único injetor padrão IEEE 802.3af PoE. 2.3 O ponto de acesso deve permitir sua operação em capacidade máxima mesmo quando energizado através do injetor PoE; 2.4 O ponto de acesso deve permitir sua energização através de fonte externa ou interna que opere com tensão de entrada para a fonte, em 110-200Vac; 3. LED’s e Sinalização: 3.1 Possuir LEDs indicativos do estado de operação; 3.2	un	5		

		Possuir LEDs indicativos da atividade dos rádios; 3.3 Possuir LEDs indicativos da atividade da interface Gigabit Ethernet; 4. Antenas: 4.1 Possuir antenas internas ao ponto de acesso, em conformidade com o padrão IEEE 802.11a/b/g/n; 4.2 Com ganho de, pelo menos, 5dBi para 2.4 GHz; 4.3. Com ganho de, pelo menos, 5dBi para 5.0 GHz; 4.4 Que implante padrão de irradiação omnidirecional; 4.1.5 Que implante operação simultânea em 3x3:3 MIMO; 5. Modo de Operação: 5.1 Implantar modo de operação onde o AP possa estar remotamente conectado ao controlador wireless tanto de forma direta em uma rede de camada 2 ou em qualquer ponto de uma rede segmentada em subredes de camada 3; 5.2 O ponto de acesso deve permitir sua operação através da conexão a um controlador principal e a um controlador secundário; 5.3 Selecionar automaticamente o canal de transmissão; 5.4 Ajustar dinamicamente o nível de potência e canal de rádio; 5.5 Possuir suporte a pelo menos 8 SSIDs para 2.4Ghz e 8 SSIDs para 5.0Ghz; 5.6 Permitir habilitar e desabilitar a divulgação do SSID; 5.7 Deve implementar Fast Roaming ou funcionalidade similar de forma a garantir o Roaming sem perda de conexão; 5.8 Não deve haver licença restringindo o número de usuários por AP. 5.9 Implantar a pilha de protocolos TCP/IP; 5.10 Implantar VLANs conforme padrão IEEE 802.1Q; 5.11 Implantar cliente DHCP, para configuração automática de rede; 5.12 Configurar-se automaticamente ao ser conectado na rede; 6. Gerenciamento: 6.1 Possuir porta de console para configuração; 6.2 Permitir via controlador wireless, a atualização remota do sistema operacional; 6.3 Permitir via controlador wireless, a atualização remota dos arquivos de configuração utilizados no equipamento; 6.4 Implantar funcionamento em modo gerenciado pelo controlador wireless; 7. Segurança e QoS: 7.1 Possuir entrada para dispositivo antifurto do tipo Kensingtonlock ou similar; 7.2 Implementar varredura de Rádio Frequência nas tecnologias 802.11a, 802.11b/g e 802.11n para identificação de AP não autorizados (rogues); 7.3 Implementar varredura de Rádio Frequência nas tecnologias 802.11a, 802.11b/g e 802.11n para identificação de interferências nos canais na rede WLAN; 7.4 Implementar IEEE 802.1x de acesso do próprio AP a rede cabeada; 7.5 Implementar autenticação com geração dinâmica de chaves criptográficas por sessão e por usuário; 7.6 Implementar em conjunto com o Controlador WLAN, WEP, chaves estáticas e dinâmicas; 7.7 Implementar em conjunto com o Controlador WLAN, WPA com algoritmo de criptografia TKIP e MIC; 7.8 Implementar em conjunto com o Controlador WLAN, WPA2 com algoritmo de criptografia AES; 7.9 Implementar padrão IEEE 802.11e WMM da Wi-Fi Alliance para priorização de tráfego, suportando aplicações em tempo real, tais como VoIP e vídeo; 7.10 O sistema de monitoração e controle de RF deve possuir mecanismos de detecção e prevenção de intrusos no ambiente wireless; 7.11 Implantar modo de operação onde o WIPS possa estar remotamente conectado ao controlador wireless tanto de forma direta em uma rede de camada 2 ou em qualquer ponto de uma rede segmentada				

		em subredes de camada 3; 7.12 O WIPS deve permitir sua operação através da conexão a um controlador principal ou controlador secundário, realizando detecção de: 7.12.1 Rogue AP; 7.12.2 Honeypot; 7.12.3 Packet Injection; 7.12.4 Redes Ad Hoc; 7.12.5 Main-in-the-middle; 7.12.6 Negação de Serviço (DoS); 7.12.7 MAC Spoofing; 7.12.8 Tentativa de quebra de chaves; 7.12.9 Reconhecimento de rede; 8. Certificações: 8.1 Possuir certificação da Wi-Fi Alliance. 8.2. Possuir certificação/homologação da ANATEL. 9. Garantia: 9.1 O Ponto de Acesso deverá possuir garantia do fabricante pelo período mínimo de 60 (sessenta) meses. 9.2. Nos casos de troca equipamentos defeituosos, os mesmos devem ser enviados no próximo dia útil subsequente a abertura do chamado e comprovação do defeito, sem quaisquer custos adicionais. 9.3. Os chamados técnicos deverão ser gerenciados pelo fornecedor em horário comercial na modalidade 8x5 (oito horas por dia, cinco dias por semana), através de telefone gratuito. Também deve ser disponibilizado endereço de e-mail para abertura dos chamados técnicos. 9.4 A empresa deverá possuir pelo menos 1 (um) Engenheiro apto a prestar serviços de suporte técnico no equipamento proposto. O Engenheiro deverá possuir registro junto ao CREA e certificação no produto comprovada pelo fabricante. 9.5 O Fabricante deverá disponibilizar gratuitamente, suporte e atualizações dos softwares, firmwares e sistema operacional para correção de bugs e implementações de segurança. 9.6. Fornecer os softwares e suas atualizações, firmwares, sistema operacional através de meio eletrônico ou magnético sem ônus adicionais. 10. Compatibilidade: 10.1. Os componentes do Ponto de Acesso deverão ser homologados pelo fabricante. Não será aceita a adição ou subtração de qualquer componente não original de fábrica para adequação do equipamento; Todos os componentes deverão ser compatíveis entre si, com o conjunto do equipamento e com suas funcionalidades, sem a utilização de adaptadores, fresagens, pinturas, usinagens em geral, furações, emprego de adesivos, fitas adesivas ou quaisquer outros procedimentos ou emprego de materiais inadequados ou que visem adaptar forçadamente o equipamento ou suas partes que sejam fisicamente ou logicamente incompatíveis. (Será aceito o regime de OEM desde que comprovado pelo próprio fabricante). 10.2 O Ponto de Acesso especificado neste item deve ser totalmente compatível com o Controlador Wireless Extreme Networks V2110. 10.3 O Ponto de Acesso especificado neste item deve ser totalmente compatível com a Solução de Gerenciamento NetSight Base 500. Referência: Marca Extreme Network, modelo WS-AP3715i ou de melhor qualidade. (TCU, Acórdão 2401/2006, 9.3.2 – Plenário). **(COTA RESERVADA ME/EPP/MEI) – VINCULADO AO ITEM 27**				
68992	29	Ponto de Acesso Indoor WS-AP3825e Tipo 4: 1. Características Básicas: 1.1 Ponto de Acesso deve atender simultaneamente aos padrões: IEEE 802.11a; IEEE 802.11b; IEEE 802.11g; IEEE 802.11n; IEEE 802.11ac; 1.2 Permitir a conexão simultânea de dispositivos configurados nos padrões: IEEE	un	38		

		802.11b/g/n; IEEE 802.11a/n; IEEE 802.11ac; 1.3 Implantar funcionamento simultâneo dos rádios 2.4Ghz e 5.0 Ghz; 1.4 Implantar todas as seguintes taxas de transmissão e fallback automático: 1.4.1 IEEE 802.11a: 54, 48, 36, 24, 18, 12, 9 e 6 Mbps; 1.4.2 IEEE 802.11b: 11, 55, 2 e 1 Mbps; 1.4.3 IEEE 802.11g: 54, 48, 36, 24, 18, 12, 11, 9, 6, 55, 2 e 1 Mbps; 1.4.4 IEEE 802.11n: 300, 270, 180, 120, 60, 45, 30 e 15 Mbps; 1.4.5 IEEE 802.11n: 450, 300, 270, 180, 120, 60, 45, 30 e 15 Mbps; 1.4.6 IEEE 802.11ac: 1300, 866.7, 780, 390, 260, 130, 97.5, 65 e 32.5 Mbps; 1.5 Possuir e acompanhar componentes que permita sua fixação em teto e parede; 1.6 Ponto de Acesso devem ser eficientemente energizados e usar até 12.95 Watts com todas as funcionalidades habilitadas. 1.7 Ponto de Acesso deve suportar performance em conexão cabeada de 75000pps. 1.8 Ponto de Acesso deve implementar instalação plug and play. 1.9 Ponto de Acesso deve implementar análise de espectro RF. 1.10 Ponto de Acesso deve implementar um modo hibrido de operação que seja capaz de suportar varredura de segurança e atender os clientes no mesmo rádio. 1.11 Transmissão máxima de potência de cada rádio deve ser de pelo menos 26dBm em 2.4 GHz e 5GHz. 1.12. Deve implementar associação de policies para clientes, sem precisar de segmentação VIA SSIDs dedicados. 2. Portas de Rede: 2.1 Possuir pelo menos 2 (duas) portas Gigabit Ethernet 10/100/1000 Mbps, auto-sensing, com conector RJ-45 Fêmea para dados, não sendo aceito portas de gerência; 2.2 Permitir sua energização, pela interface de rede descrita no item anterior, através de um único injetor padrão IEEE 802.3af PoE; 2.3 O ponto de acesso deve permitir sua operação em capacidade máxima mesmo quando energizado através do injetor PoE; 2.4 Suportar sua energização através de fonte externa ou interna que opere com tensão de entrada para a fonte, em 110-200Vac; 3. LED’s e Sinalização: 3.1 Possuir LEDs indicativos do estado de operação; 3.2 Possuir LEDs indicativos da atividade dos rádios; 3.3 Possuir LEDs indicativos da atividade da interface Gigabit Ethernet; 4. Antenas: 4.1 Possuir 6 (seis) antenas externas ao AP, em conformidade com o padrão IEEE 802.11a/b/g/n/ac; 4.2 Possuir ganho de, pelo menos, 3dBi para 2.4 GHz; 4.3 Possuir ganho de, pelo menos, 3dBi para 5.0 GHz; 4.4 Que implante padrão de irradiação omnidirecional; 4.5 Que implante operação simultânea em 3x3:3 MIMO; 5. Modo de Operação: 5.1 Implantar modo de operação onde o ponto de acesso possa estar remotamente conectado ao controlador wireless tanto de forma direta em uma rede de camada 2 ou em qualquer ponto de uma rede segmentada em subredes de camada 3; 5.2 O ponto de acesso deve permitir sua operação através da conexão a um controlador principal e a um controlador secundário; 5.3 Selecionar automaticamente o canal de transmissão; 5.4 Ajustar dinamicamente o nível de potência e canal de rádio; 5.5 Possuir suporte a pelo menos 8 SSIDs para 2.4Ghz e 8 SSIDs para 5.0Ghz; 5.6 Permitir habilitar e desabilitar a divulgação do SSID; 5.7 Deve implementar Fast Roaming ou funcionalidade similar de forma a garantir o Roaming sem perda de				

		conexão; 5.8 Não deve haver licença restringindo o número de usuários por AP. 5.9 Implantar a pilha de protocolos TCP/IP; 5.10 Implantar VLANs conforme padrão IEEE 802.1Q; 5.11 Implantar cliente DHCP, para configuração automática de rede; 5.12 Configurar-se automaticamente ao ser conectado na rede; 5.13 Implementar Packet aggregation A-MPDU, A-MSDU para 802.11ac e 802.11n. 6. Gerenciamento: 6.1 Possuir porta de console para configuração; 6.2 Permitir via controlador wireless, a atualização remota do sistema operacional; 6.3 Permitir via controlador wireless, a atualização remota dos arquivos de configuração utilizados no equipamento; 6.4 Implantar funcionamento em modo gerenciado pelo controlador wireless; 7. Segurança e QoS: 7.1 Possuir entrada para dispositivo antifurto do tipo Kensingtonlock ou similar; 7.2 Implanta varredura de Rádio Frequência nas tecnologias 802.11a, 802.11b/g, 802.11n e 802.11ac para identificação de AP não autorizados (rogues); 7.3 Implementar varredura de Rádio Frequência nas tecnologias 802.11a, 802.11b/g, 802.11n, 802.11ac para identificação de interferências nos canais na rede WLAN; 7.4 Implementar IEEE 802.1x de acesso do próprio AP a rede cabeada; 7.5 Implementar autenticação com geração dinâmica de chaves criptográficas por sessão e por usuário; 7.6 Implementar em conjunto com o Controlador WLAN, WEP, chaves estáticas e dinâmicas; 7.7 Implementar em conjunto com o Controlador WLAN, WPA com algoritmo de criptografia TKIP e MIC; 7.8 Implementar em conjunto com o Controlador WLAN, WPA2 com algoritmo de criptografia AES; 7.9 Implementar padrão IEEE 802.11e WMM da Wi-Fi Alliance para priorização de tráfego, suportando aplicações em tempo real, tais como VoIP e vídeo; 7.10 O sistema de monitoração e controle de RF deve possuir mecanismos de detecção e prevenção de intrusos no ambiente wireless; 7.11 Implantar modo de operação onde o WIPS possa estar remotamente conectado ao controlador wireless tanto de forma direta em uma rede de camada 2 ou em qualquer ponto de uma rede segmentada em subredes de camada 3; 7.12 O WIPS deve permitir sua operação através da conexão a um controlador principal ou controlador secundário, realizando detecção de: 7.12.1 Rogue AP; 7.12.2 Honeypot; 7.12.3 Packet Injection; 7.12.4 Redes Ad Hoc; 7.12.5 Main-in-the-middle; 7.12.6 Negação de Serviço (DoS); 7.12.7 MAC Spoofing; 7.12.8 Tentativa de quebra de chaves; 7.12.9 Reconhecimento de rede; 8. Certificações: 8.1 Possuir certificação da Wi-Fi Alliance. 8.2. Possuir certificação/homologação da ANATEL. 9. Garantia: 9.1 O Ponto de Acesso deverá possuir garantia do fabricante pelo período mínimo de 60 (sessenta) meses. 9.2. Nos casos de troca equipamentos defeituosos, os mesmos devem ser enviados no próximo dia útil subsequente a abertura do chamado e comprovação do defeito, sem quaisquer custos adicionais. 9.3. Os chamados técnicos deverão ser gerenciados pelo fornecedor em horário comercial na modalidade 8x5 (oito horas por dia, cinco dias por semana), através de telefone gratuito. Também deve ser disponibilizado endereço de e-mail para				

		abertura dos chamados técnicos. 9.4 A empresa deverá possuir pelo menos 1 (um) Engenheiro apto a prestar serviços de suporte técnico no equipamento proposto. O Engenheiro deverá possuir registro junto ao CREA e certificação no produto comprovada pelo fabricante. 9.5 O Fabricante deverá disponibilizar gratuitamente, suporte e atualizações dos softwares, firmwares e sistema operacional para correção de bugs e implementações de segurança. 9.6. Fornecer os softwares e suas atualizações, firmwares, sistema operacional através de meio eletrônico ou magnético sem ônus adicionais. 10. Compatibilidade: 10.1. Os componentes do Ponto de Acesso deverão ser homologados pelo fabricante. Não será aceita a adição ou subtração de qualquer componente não original de fábrica para adequação do equipamento; Todos os componentes deverão ser compatíveis entre si, com o conjunto do equipamento e com suas funcionalidades, sem a utilização de adaptadores, fresagens, pinturas, usinagens em geral, furações, emprego de adesivos, fitas adesivas ou quaisquer outros procedimentos ou emprego de materiais inadequados ou que visem adaptar forçadamente o equipamento ou suas partes que sejam fisicamente ou logicamente incompatíveis. (Será aceito o regime de OEM desde que comprovado pelo próprio fabricante). 10.2 O Ponto de Acesso especificado neste item deve ser totalmente compatível com o Controlador Wireless Extreme Networks V2110. 10.3 O Ponto de Acesso especificado neste item deve ser totalmente compatível com a Solução de Gerenciamento NetSight Base 500. Referência: Marca Extreme Network, modelo WS-AP3825e ou de melhor qualidade. (TCU, Acórdão 2401/2006, 9.3.2 – Plenário). **(COTA PRINCIPAL)**				
68992	30	Ponto de Acesso Indoor WS-AP3825e Tipo 4: 1. Características Básicas: 1.1 Ponto de Acesso deve atender simultaneamente aos padrões: IEEE 802.11a; IEEE 802.11b; IEEE 802.11g; IEEE 802.11n; IEEE 802.11ac; 1.2 Permitir a conexão simultânea de dispositivos configurados nos padrões: IEEE 802.11b/g/n; IEEE 802.11a/n; IEEE 802.11ac; 1.3 Implantar funcionamento simultâneo dos rádios 2.4Ghz e 5.0 Ghz; 1.4 Implantar todas as seguintes taxas de transmissão e fallback automático: 1.4.1 IEEE 802.11a: 54, 48, 36, 24, 18, 12, 9 e 6 Mbps; 1.4.2 IEEE 802.11b: 11, 55, 2 e 1 Mbps; 1.4.3 IEEE 802.11g: 54, 48, 36, 24, 18, 12, 11, 9, 6, 55, 2 e 1 Mbps; 1.4.4 IEEE 802.11n: 300, 270, 180, 120, 60, 45, 30 e 15 Mbps; 1.4.5 IEEE 802.11n: 450, 300, 270, 180, 120, 60, 45, 30 e 15 Mbps; 1.4.6 IEEE 802.11ac: 1300, 866.7, 780, 390, 260, 130, 97.5, 65 e 32.5 Mbps; 1.5 Possuir e acompanhar componentes que permita sua fixação em teto e parede; 1.6 Ponto de Acesso devem ser eficientemente energizados e usar até 12.95 Watts com todas as funcionalidades habilitadas. 1.7 Ponto de Acesso deve suportar performance em conexão cabeada de 75000pps. 1.8 Ponto de Acesso deve implementar instalação plug and play. 1.9 Ponto de Acesso deve implementar análise de espectro RF. 1.10 Ponto de Acesso deve implementar um modo hibrido de operação que seja capaz de suportar varredura de	un	12		

		segurança e atender os clientes no mesmo rádio. 1.11 Transmissão máxima de potência de cada rádio deve ser de pelo menos 26dBm em 2.4 GHz e 5GHz. 1.12. Deve implementar associação de policies para clientes, sem precisar de segmentação VIA SSIDs dedicados. 2. Portas de Rede: 2.1 Possuir pelo menos 2 (duas) portas Gigabit Ethernet 10/100/1000 Mbps, auto-sensing, com conector RJ-45 Fêmea para dados, não sendo aceito portas de gerência; 2.2 Permitir sua energização, pela interface de rede descrita no item anterior, através de um único injetor padrão IEEE 802.3af PoE; 2.3 O ponto de acesso deve permitir sua operação em capacidade máxima mesmo quando energizado através do injetor PoE; 2.4 Suportar sua energização através de fonte externa ou interna que opere com tensão de entrada para a fonte, em 110-200Vac; 3. LED's e Sinalização: 3.1 Possuir LEDs indicativos do estado de operação; 3.2 Possuir LEDs indicativos da atividade dos rádios; 3.3 Possuir LEDs indicativos da atividade da interface Gigabit Ethernet; 4. Antenas: 4.1 Possuir 6 (seis) antenas externas ao AP, em conformidade com o padrão IEEE 802.11a/b/g/n/ac; 4.2 Possuir ganho de, pelo menos, 3dBi para 2.4 GHz; 4.3 Possuir ganho de, pelo menos, 3dBi para 5.0 GHz; 4.4 Que implante padrão de irradiação omnidirecional; 4.5 Que implante operação simultânea em 3x3:3 MIMO; 5. Modo de Operação: 5.1 Implantar modo de operação onde o ponto de acesso possa estar remotamente conectado ao controlador wireless tanto de forma direta em uma rede de camada 2 ou em qualquer ponto de uma rede segmentada em subredes de camada 3; 5.2 O ponto de acesso deve permitir sua operação através da conexão a um controlador principal e a um controlador secundário; 5.3 Selecionar automaticamente o canal de transmissão; 5.4 Ajustar dinamicamente o nível de potência e canal de rádio; 5.5 Possuir suporte a pelo menos 8 SSIDs para 2.4Ghz e 8 SSIDs para 5.0Ghz; 5.6 Permitir habilitar e desabilitar a divulgação do SSID; 5.7 Deve implementar Fast Roaming ou funcionalidade similar de forma a garantir o Roaming sem perda de conexão; 5.8 Não deve haver licença restringindo o número de usuários por AP. 5.9 Implantar a pilha de protocolos TCP/IP; 5.10 Implantar VLANs conforme padrão IEEE 802.1Q; 5.11 Implantar cliente DHCP, para configuração automática de rede; 5.12 Configurar-se automaticamente ao ser conectado na rede; 5.13 Implementar Packet aggregation A-MPDU, A-MSDU para 802.11ac e 802.11n. 6. Gerenciamento: 6.1 Possuir porta de console para configuração; 6.2 Permitir via controlador wireless, a atualização remota do sistema operacional; 6.3 Permitir via controlador wireless, a atualização remota dos arquivos de configuração utilizados no equipamento; 6.4 Implantar funcionamento em modo gerenciado pelo controlador wireless; 7. Segurança e QoS: 7.1 Possuir entrada para dispositivo antifurto do tipo Kensingtonlock ou similar; 7.2 Implanta varredura de Rádio Frequência nas tecnologias 802.11a, 802.11b/g, 802.11n e 802.11ac para identificação de AP não autorizados (rogues); 7.3 Implementar varredura de Rádio Frequência nas tecnologias 802.11a, 802.11b/g, 802.11n, 802.11ac				

		para identificação de interferências nos canais na rede WLAN; 7.4 Implementar IEEE 802.1x de acesso do próprio AP a rede cabeada; 7.5 Implementar autenticação com geração dinâmica de chaves criptográficas por sessão e por usuário; 7.6 Implementar em conjunto com o Controlador WLAN, WEP, chaves estáticas e dinâmicas; 7.7 Implementar em conjunto com o Controlador WLAN, WPA com algoritmo de criptografia TKIP e MIC; 7.8 Implementar em conjunto com o Controlador WLAN, WPA2 com algoritmo de criptografia AES; 7.9 Implementar padrão IEEE 802.11e WMM da Wi-Fi Alliance para priorização de tráfego, suportando aplicações em tempo real, tais como VoIP e vídeo; 7.10 O sistema de monitoração e controle de RF deve possuir mecanismos de detecção e prevenção de intrusos no ambiente wireless; 7.11 Implantar modo de operação onde o WIPS possa estar remotamente conectado ao controlador wireless tanto de forma direta em uma rede de camada 2 ou em qualquer ponto de uma rede segmentada em subredes de camada 3; 7.12 O WIPS deve permitir sua operação através da conexão a um controlador principal ou controlador secundário, realizando detecção de: 7.12.1 Rogue AP; 7.12.2 Honeypot; 7.12.3 Packet Injection; 7.12.4 Redes Ad Hoc; 7.12.5 Main-in-the-middle; 7.12.6 Negação de Serviço (DoS); 7.12.7 MAC Spoofing; 7.12.8 Tentativa de quebra de chaves; 7.12.9 Reconhecimento de rede; 8. Certificações: 8.1 Possuir certificação da Wi-Fi Alliance. 8.2. Possuir certificação/homologação da ANATEL. 9. Garantia: 9.1 O Ponto de Acesso deverá possuir garantia do fabricante pelo período mínimo de 60 (sessenta) meses. 9.2. Nos casos de troca equipamentos defeituosos, os mesmos devem ser enviados no próximo dia útil subsequente a abertura do chamado e comprovação do defeito, sem quaisquer custos adicionais. 9.3. Os chamados técnicos deverão ser gerenciados pelo fornecedor em horário comercial na modalidade 8x5 (oito horas por dia, cinco dias por semana), através de telefone gratuito. Também deve ser disponibilizado endereço de e-mail para abertura dos chamados técnicos. 9.4 A empresa deverá possuir pelo menos 1 (um) Engenheiro apto a prestar serviços de suporte técnico no equipamento proposto. O Engenheiro deverá possuir registro junto ao CREA e certificação no produto comprovada pelo fabricante. 9.5 O Fabricante deverá disponibilizar gratuitamente, suporte e atualizações dos softwares, firmwares e sistema operacional para correção de bugs e implementações de segurança. 9.6. Fornecer os softwares e suas atualizações, firmwares, sistema operacional através de meio eletrônico ou magnético sem ônus adicionais. 10. Compatibilidade: 10.1. Os componentes do Ponto de Acesso deverão ser homologados pelo fabricante. Não será aceita a adição ou subtração de qualquer componente não original de fábrica para adequação do equipamento; Todos os componentes deverão ser compatíveis entre si, com o conjunto do equipamento e com suas funcionalidades, sem a utilização de adaptadores, fresagens, pinturas, usinagens em geral, furações, emprego de adesivos, fitas adesivas ou quaisquer outros procedimentos ou				

		emprego de materiais inadequados ou que visem adaptar forçadamente o equipamento ou suas partes que sejam fisicamente ou logicamente incompatíveis. (Será aceito o regime de OEM desde que comprovado pelo próprio fabricante). 10.2 O Ponto de Acesso especificado neste item deve ser totalmente compatível com o Controlador Wireless Extreme Networks V2110. 10.3 O Ponto de Acesso especificado neste item deve ser totalmente compatível com a Solução de Gerenciamento NetSight Base 500. Referência: Marca Extreme Network, modelo WS-AP3825e ou de melhor qualidade. (TCU, Acórdão 2401/2006, 9.3.2 – Plenário). **(COTA RESERVADA ME/EPP/MEI) – VINCULADO AO ITEM 29**				
68990	31	Ponto de Acesso Indoor WS-AP3825i Tipo 2: 1. Características Básicas: 1.1 Ponto de Acesso deve atender simultaneamente aos padrões: IEEE 802.11a; IEEE 802.11b; IEEE 802.11g; IEEE 802.11n; IEEE 802.11ac; 1.2 Permitir a conexão simultânea de dispositivos configurados nos padrões: IEEE 802.11b/g/n; IEEE 802.11a/n; IEEE 802.11ac; 1.3 Implantar funcionamento simultâneo dos rádios 2.4Ghz e 5.0 Ghz; 1.4 Implantar todas as seguintes taxas de transmissão e fallback automático: 1.4.1 IEEE 802.11a: 54, 48, 36, 24, 18, 12, 9 e 6 Mbps; 1.4.2 IEEE 802.11b: 11, 55, 2 e 1 Mbps; 1.4.3 IEEE 802.11g: 54, 48, 36, 24, 18, 12, 11, 9, 6, 55, 2 e 1 Mbps; 1.4.4 IEEE 802.11n: 300, 270, 180, 120, 60, 45, 30 e 15 Mbps; 1.4.5 IEEE 802.11n: 450, 300, 270, 180, 120, 60, 45, 30 e 15 Mbps; 1.4.6 IEEE 802.11ac: 1300, 866.7, 780, 390, 260, 130, 97.5, 65 e 32.5 Mbps; 1.5 Possuir e acompanhar componentes que permita sua fixação em teto e parede; 1.6 Ponto de Acesso devem ser eficientemente energizados e usar até 12.95 Watts com todas as funcionalidades habilitadas. 1.7 Ponto de Acesso deve suportar performance em conexão cabeada de 75000pps. 1.8 Ponto de Acesso deve implementar instalação plug and play. 1.9 Ponto de Acesso deve implementar análise de espectro RF. 1.10 Ponto de Acesso deve implementar um modo hibrido de operação que seja capaz de suportar varredura de segurança e atender os clientes no mesmo rádio. 1.11 Transmissão máxima de potência de cada rádio deve ser de pelo menos 26dBm em 2.4 GHz e 5GHz. 1.12. Deve implementar associação de policies para clientes, sem precisar de segmentação VIA SSIDs dedicados. 2. Portas de Rede: 2.1. Possuir pelo menos 2 (duas) portas Gigabit Ethernet 10/100/1000 Mbps, auto-sensing, com conector RJ-45 Fêmea para dados, não sendo aceito portas de gerência; 2.2. Implementar agregação de links com suporte a LACP, permitindo agregar as 2 (duas) portas Gigabit Ethernet 10/100/1000 Mbps; 2.3 Permitir sua energização, pela interface de rede descrita no item anterior, através de um único injetor padrão IEEE 802.3af PoE; 2.3. O Ponto de acesso deve permitir sua operação em capacidade máxima mesmo quando energizado através do injetor PoE; 2.4. Suportar sua energização através de fonte externa ou interna que opere com tensão de entrada para a fonte, em 110-200Vac; 3. LED’s e Sinalização: 3.1. Possuir LEDs indicativos do estado de operação; 3.2. Possuir LEDs indicativos da atividade dos rádios; 3.3. Possuir	un	38		

		LEDs indicativos da atividade da interface Gigabit Ethernet; 4. Antenas: 4.1 Possuir antenas internas ao AP, em conformidade com o padrão IEEE 802.11a/b/g/n/ac; 4.2. Possuir ganho de, pelo menos, 3dBi para 2.4 GHz; 4.3 Possuir ganho de, pelo menos, 4dBi para 5.0 GHz; 4.4 Que implante padrão de irradiação omnidirecional; 4.5. Que implante operação simultânea em 3x3:3 MIMO; 5. Modo de Operação: 5.1 Implantar modo de operação onde o ponto de acesso possa estar remotamente conectado ao controlador wireless tanto de forma direta em uma rede de camada 2 ou em qualquer ponto de uma rede segmentada em subredes de camada 3; 5.2 O ponto de acesso deve permitir sua operação através da conexão a um controlador principal e a um controlador secundário; 5.3 Selecionar automaticamente o canal de transmissão; 5.4 Ajustar dinamicamente o nível de potência e canal de rádio; 5.5 Possuir suporte a pelo menos 8 SSIDs para 2.4Ghz e 8 SSIDs para 5.0Ghz; 5.6 Permitir habilitar e desabilitar a divulgação do SSID; 5.7 Deve implementar Fast Roaming ou funcionalidade similar de forma a garantir o Roaming sem perda de conexão; 5.8 Não deve haver licença restringindo o número de usuários por AP. 5.9 Implantar a pilha de protocolos TCP/IP; 5.10 Implantar VLANs conforme padrão IEEE 802.1Q; 5.11 Implantar cliente DHCP, para configuração automática de rede; 5.12 Configurar-se automaticamente ao ser conectado na rede; 5.13 Implementar Packet aggregation A-MPDU, A-MSDU para 802.11ac e 802.11n. 6. Gerenciamento: 6.1 Possuir porta de console para configuração; 6.2 Permitir via controlador wireless, a atualização remota do sistema operacional; 6.3 Permitir via controlador wireless, a atualização remota dos arquivos de configuração utilizados no equipamento; 6.4 Implantar funcionamento em modo gerenciado pelo controlador wireless; 7. Segurança e QoS: 7.1 Possuir entrada para dispositivo antifurto do tipo Kensingtonlock ou similar; 7.2 Implanta varredura de Rádio Frequência nas tecnologias 802.11a, 802.11b/g, 802.11n e 802.11ac para identificação de AP não autorizados (rogues); 7.3 Implementar varredura de Rádio Frequência nas tecnologias 802.11a, 802.11b/g, 802.11n, 802.11ac para identificação de interferências nos canais na rede WLAN; 7.4 Implementar IEEE 802.1x de acesso do próprio AP a rede cabeada; 7.5 Implementar autenticação com geração dinâmica de chaves criptográficas por sessão e por usuário; 7.6 Implementar em conjunto com o Controlador WLAN, WEP, chaves estáticas e dinâmicas; 7.7 Implementar em conjunto com o Controlador WLAN, WPA com algoritmo de criptografia TKIP e MIC; 7.8 Implementar em conjunto com o Controlador WLAN, WPA2 com algoritmo de criptografia AES; 7.9 Implementar padrão IEEE 802.11e WMM da Wi-Fi Alliance para priorização de tráfego, suportando aplicações em tempo real, tais como VoIP e vídeo; 7.10 O sistema de monitoração e controle de RF deve possuir mecanismos de detecção e prevenção de intrusos no ambiente wireless; 7.11 Implantar modo de operação onde o WIPS possa estar remotamente conectado ao controlador wireless tanto de forma direta em uma rede de				

		camada 2 ou em qualquer ponto de uma rede segmentada em subredes de camada 3; 7.12 O WIPS deve permitir sua operação através da conexão a um controlador principal ou controlador secundário, realizando detecção de: 7.12.1 Rogue AP; 7.12.2 Honeypot; 7.12.3 Packet Injection; 7.12.4 Redes Ad Hoc; 7.12.5 Main-in-the-middle; 7.12.6 Negação de Serviço (DoS); 7.12.7 MAC Spoofing; 7.12.8 Tentativa de quebra de chaves; 7.12.9 Reconhecimento de rede; 8. Certificações: 8.1 Possuir certificação da Wi-Fi Alliance. 8.2. Possuir certificação/homologação da ANATEL. 9. Garantia: 9.1 O Ponto de Acesso deverá possuir garantia do fabricante pelo período mínimo de 60 (sessenta) meses. 9.2. Nos casos de troca equipamentos defeituosos, os mesmos devem ser enviados no próximo dia útil subsequente a abertura do chamado e comprovação do defeito, sem quaisquer custos adicionais. 9.3. Os chamados técnicos deverão ser gerenciados pelo fornecedor em horário comercial na modalidade 8x5 (oito horas por dia, cinco dias por semana), através de telefone gratuito. Também deve ser disponibilizado endereço de e-mail para abertura dos chamados técnicos. 9.4 A empresa deverá possuir pelo menos 1 (um) Engenheiro apto a prestar serviços de suporte técnico no equipamento proposto. O Engenheiro deverá possuir registro junto ao CREA e certificação no produto comprovada pelo fabricante. 9.5 O Fabricante deverá disponibilizar gratuitamente, suporte e atualizações dos softwares, firmwares e sistema operacional para correção de bugs e implementações de segurança. 9.6. Fornecer os softwares e suas atualizações, firmwares, sistema operacional através de meio eletrônico ou magnético sem ônus adicionais. 10. Compatibilidade: 10.1. Os componentes do Ponto de Acesso deverão ser homologados pelo fabricante. Não será aceita a adição ou subtração de qualquer componente não original de fábrica para adequação do equipamento; Todos os componentes deverão ser compatíveis entre si, com o conjunto do equipamento e com suas funcionalidades, sem a utilização de adaptadores, fresagens, pinturas, usinagens em geral, furações, emprego de adesivos, fitas adesivas ou quaisquer outros procedimentos ou emprego de materiais inadequados ou que visem adaptar forçadamente o equipamento ou suas partes que sejam fisicamente ou logicamente incompatíveis. (Será aceito o regime de OEM desde que comprovado pelo próprio fabricante). 10.2 O Ponto de Acesso especificado neste item deve ser totalmente compatível com o Controlador Wireless Extreme Networks V2110. 10.3 O Ponto de Acesso especificado neste item deve ser totalmente compatível com a Solução de Gerenciamento NetSight Base 500. Referência: Marca Extreme Network, modelo WS-AP3825i ou de melhor qualidade. (TCU, Acórdão 2401/2006, 9.3.2 – Plenário). **(COTA PRINCIPAL)**				
68990	32	Ponto de Acesso Indoor WS-AP3825i Tipo 2: 1. Características Básicas: 1.1 Ponto de Acesso deve atender simultaneamente aos padrões: IEEE 802.11a; IEEE 802.11b; IEEE 802.11g; IEEE 802.11n; IEEE 802.11ac; 1.2 Permitir a conexão simultânea de dispositivos configurados nos padrões: IEEE	un	12		

		802.11b/g/n; IEEE 802.11a/n; IEEE 802.11ac; 1.3 Implantar funcionamento simultâneo dos rádios 2.4Ghz e 5.0 Ghz; 1.4 Implantar todas as seguintes taxas de transmissão e fallback automático: 1.4.1 IEEE 802.11a: 54, 48, 36, 24, 18, 12, 9 e 6 Mbps; 1.4.2 IEEE 802.11b: 11, 55, 2 e 1 Mbps; 1.4.3 IEEE 802.11g: 54, 48, 36, 24, 18, 12, 11, 9, 6, 55, 2 e 1 Mbps; 1.4.4 IEEE 802.11n: 300, 270, 180, 120, 60, 45, 30 e 15 Mbps; 1.4.5 IEEE 802.11n: 450, 300, 270, 180, 120, 60, 45, 30 e 15 Mbps; 1.4.6 IEEE 802.11ac: 1300, 866.7, 780, 390, 260, 130, 97.5, 65 e 32.5 Mbps; 1.5 Possuir e acompanhar componentes que permita sua fixação em teto e parede; 1.6 Ponto de Acesso devem ser eficientemente energizados e usar até 12.95 Watts com todas as funcionalidades habilitadas. 1.7 Ponto de Acesso deve suportar performance em conexão cabeada de 75000pps. 1.8 Ponto de Acesso deve implementar instalação plug and play. 1.9 Ponto de Acesso deve implementar análise de espectro RF. 1.10 Ponto de Acesso deve implementar um modo hibrido de operação que seja capaz de suportar varredura de segurança e atender os clientes no mesmo rádio. 1.11 Transmissão máxima de potência de cada rádio deve ser de pelo menos 26dBm em 2.4 GHz e 5GHz. 1.12. Deve implementar associação de policies para clientes, sem precisar de segmentação VIA SSIDs dedicados. 2. Portas de Rede: 2.1. Possuir pelo menos 2 (duas) portas Gigabit Ethernet 10/100/1000 Mbps, auto-sensing, com conector RJ-45 Fêmea para dados, não sendo aceito portas de gerência; 2.2. Implementar agregação de links com suporte a LACP, permitindo agregar as 2 (duas) portas Gigabit Ethernet 10/100/1000 Mbps; 2.3 Permitir sua energização, pela interface de rede descrita no item anterior, através de um único injetor padrão IEEE 802.3af PoE; 2.3. O Ponto de acesso deve permitir sua operação em capacidade máxima mesmo quando energizado através do injetor PoE; 2.4. Suportar sua energização através de fonte externa ou interna que opere com tensão de entrada para a fonte, em 110-200Vac; 3. LED’s e Sinalização: 3.1. Possuir LEDs indicativos do estado de operação; 3.2. Possuir LEDs indicativos da atividade dos rádios; 3.3. Possuir LEDs indicativos da atividade da interface Gigabit Ethernet; 4. Antenas: 4.1 Possuir antenas internas ao AP, em conformidade com o padrão IEEE 802.11a/b/g/n/ac; 4.2. Possuir ganho de, pelo menos, 3dBi para 2.4 GHz; 4.3 Possuir ganho de, pelo menos, 4dBi para 5.0 GHz; 4.4 Que implante padrão de irradiação omnidirecional; 4.5. Que implante operação simultânea em 3x3:3 MIMO; 5. Modo de Operação: 5.1 Implantar modo de operação onde o ponto de acesso possa estar remotamente conectado ao controlador wireless tanto de forma direta em uma rede de camada 2 ou em qualquer ponto de uma rede segmentada em subredes de camada 3; 5.2 O ponto de acesso deve permitir sua operação através da conexão a um controlador principal e a um controlador secundário; 5.3 Selecionar automaticamente o canal de transmissão; 5.4 Ajustar dinamicamente o nível de potência e canal de rádio; 5.5 Possuir suporte a pelo menos 8 SSIDs para 2.4Ghz e 8 SSIDs para 5.0Ghz; 5.6 Permitir habilitar e desabilitar a				

		divulgação do SSID; 5.7 Deve implementar Fast Roaming ou funcionalidade similar de forma a garantir o Roaming sem perda de conexão; 5.8 Não deve haver licença restringindo o número de usuários por AP. 5.9 Implantar a pilha de protocolos TCP/IP; 5.10 Implantar VLANs conforme padrão IEEE 802.1Q; 5.11 Implantar cliente DHCP, para configuração automática de rede; 5.12 Configurar-se automaticamente ao ser conectado na rede; 5.13 Implementar Packet aggregation A-MPDU, A-MSDU para 802.11ac e 802.11n. 6. Gerenciamento: 6.1 Possuir porta de console para configuração; 6.2 Permitir via controlador wireless, a atualização remota do sistema operacional; 6.3 Permitir via controlador wireless, a atualização remota dos arquivos de configuração utilizados no equipamento; 6.4 Implantar funcionamento em modo gerenciado pelo controlador wireless; 7. Segurança e QoS: 7.1 Possuir entrada para dispositivo antifurto do tipo Kensingtonlock ou similar; 7.2 Implanta varredura de Rádio Frequência nas tecnologias 802.11a, 802.11b/g, 802.11n e 802.11ac para identificação de AP não autorizados (rogues); 7.3 Implementar varredura de Rádio Frequência nas tecnologias 802.11a, 802.11b/g, 802.11n, 802.11ac para identificação de interferências nos canais na rede WLAN; 7.4 Implementar IEEE 802.1x de acesso do próprio AP a rede cabeada; 7.5 Implementar autenticação com geração dinâmica de chaves criptográficas por sessão e por usuário; 7.6 Implementar em conjunto com o Controlador WLAN, WEP, chaves estáticas e dinâmicas; 7.7 Implementar em conjunto com o Controlador WLAN, WPA com algoritmo de criptografia TKIP e MIC; 7.8 Implementar em conjunto com o Controlador WLAN, WPA2 com algoritmo de criptografia AES; 7.9 Implementar padrão IEEE 802.11e WMM da Wi-Fi Alliance para priorização de tráfego, suportando aplicações em tempo real, tais como VoIP e vídeo; 7.10 O sistema de monitoração e controle de RF deve possuir mecanismos de detecção e prevenção de intrusos no ambiente wireless; 7.11 Implantar modo de operação onde o WIPS possa estar remotamente conectado ao controlador wireless tanto de forma direta em uma rede de camada 2 ou em qualquer ponto de uma rede segmentada em subredes de camada 3; 7.12 O WIPS deve permitir sua operação através da conexão a um controlador principal ou controlador secundário, realizando detecção de: 7.12.1 Rogue AP; 7.12.2 Honeypot; 7.12.3 Packet Injection; 7.12.4 Redes Ad Hoc; 7.12.5 Main-in-the-middle; 7.12.6 Negação de Serviço (DoS); 7.12.7 MAC Spoofing; 7.12.8 Tentativa de quebra de chaves; 7.12.9 Reconhecimento de rede; 8. Certificações: 8.1 Possuir certificação da Wi-Fi Alliance. 8.2. Possuir certificação/homologação da ANATEL. 9. Garantia: 9.1 O Ponto de Acesso deverá possuir garantia do fabricante pelo período mínimo de 60 (sessenta) meses. 9.2. Nos casos de troca equipamentos defeituosos, os mesmos devem ser enviados no próximo dia útil subsequente a abertura do chamado e comprovação do defeito, sem quaisquer custos adicionais. 9.3. Os chamados técnicos deverão ser gerenciados pelo fornecedor em horário comercial na modalidade 8x5				

		(oito horas por dia, cinco dias por semana), através de telefone gratuito. Também deve ser disponibilizado endereço de e-mail para abertura dos chamados técnicos. 9.4 A empresa deverá possuir pelo menos 1 (um) Engenheiro apto a prestar serviços de suporte técnico no equipamento proposto. O Engenheiro deverá possuir registro junto ao CREA e certificação no produto comprovada pelo fabricante. 9.5 O Fabricante deverá disponibilizar gratuitamente, suporte e atualizações dos softwares, firmwares e sistema operacional para correção de bugs e implementações de segurança. 9.6. Fornecer os softwares e suas atualizações, firmwares, sistema operacional através de meio eletrônico ou magnético sem ônus adicionais. 10. Compatibilidade: 10.1. Os componentes do Ponto de Acesso deverão ser homologados pelo fabricante. Não será aceita a adição ou subtração de qualquer componente não original de fábrica para adequação do equipamento; Todos os componentes deverão ser compatíveis entre si, com o conjunto do equipamento e com suas funcionalidades, sem a utilização de adaptadores, fresagens, pinturas, usinagens em geral, furações, emprego de adesivos, fitas adesivas ou quaisquer outros procedimentos ou emprego de materiais inadequados ou que visem adaptar forçadamente o equipamento ou suas partes que sejam fisicamente ou logicamente incompatíveis. (Será aceito o regime de OEM desde que comprovado pelo próprio fabricante). 10.2 O Ponto de Acesso especificado neste item deve ser totalmente compatível com o Controlador Wireless Extreme Networks V2110. 10.3 O Ponto de Acesso especificado neste item deve ser totalmente compatível com a Solução de Gerenciamento NetSight Base 500. Referência: Marca Extreme Network, modelo WS-AP3825i ou de melhor qualidade. (TCU, Acórdão 2401/2006, 9.3.2 – Plenário). **(COTA RESERVADA ME/EPP/MEI) – VINCULADO AO ITEM 31**				
68993	33	Ponto de Acesso Outdoor WS-AP3865e Tipo 1: 1. Características Básicas: 1.1 Ponto de Acesso deve atender simultaneamente aos padrões: IEEE 802.11a; IEEE 802.11b; IEEE 802.11g; IEEE 802.11n e IEEE 802.11ac; 1.2 Permitir a conexão simultânea de dispositivos configurados nos padrões: IEEE 802.11b/g/n; IEEE 802.11a/n e IEEE 802.11ac; 1.3 Implantar funcionamento simultâneo dos rádios 2.4GHz e 5.0GHz; 1.4 Implantar todas as seguintes taxas de transmissão e fallback automático: 1.4.1 IEEE 802.11a: 54, 48, 36, 24, 18, 12, 9 e 6 Mbps; 1.4.2 IEEE 802.11b: 11, 5.5, 2 e 1 Mbps; 1.4.3 IEEE 802.11g: 54, 48, 36, 24, 18, 12, 11, 9, 6, 5.5, 2 e 1 Mbps; 1.4.4 IEEE 802.11n: 450, 300, 270, 180, 120, 60, 45, 30 e 15 Mbps; 1.4.5 IEEE 802.11ac: 1300, 866.7, 780, 390, 260, 130, 97.5, 65 e 32.5 Mbps; 1.5 Possuir e acompanhar componentes que permita sua fixação em teto e parede; 1.6 Ponto de Acesso deve suportar performance em conexão cabeada de 75000pps; 1.7 Ponto de Acesso deve implementar instalação plug and play; 1.8 Ponto de Acesso deve implementar análise de espectro RF; 1.9 Ponto de Acesso deve implementar um modo hibrido de operação que seja capaz de suportar varredura de	un	4		

		segurança e atender os clientes no mesmo rádio; 1.10 Deve implementar um modo de operação que seja capaz de fazer a varredura de segurança, trabalhando de forma dedicada, sem a necessidade de módulos de hardware adicionais para este fim. 1.11. Deve implementar associação de policies para clientes, sem precisar de segmentação via SSIDs dedicados; 2. Portas de Rede: 2.1 Possuir pelo menos 2 (duas) portas Gigabit Ethernet 10/100/1000 Mbps, auto-sensing, com conector RJ-45 Fêmea para dados, não sendo aceito portas de gerência; 2.2 Implementar agregação de links com suporte a LACP, permitindo agregar as 2 (duas) portas Gigabit Ethernet 10/100/1000 Mbps; 2.3 Permitir sua energização, pela interface de rede descrita no item anterior, através de um único injetor padrão IEEE 802.3af PoE; 2.4 O Ponto de Acesso deve permitir sua operação em capacidade máxima mesmo quando energizado através do injetor PoE; 3. Leds e Sinalização: 3.1 Possuir LEDs indicativos do estado de operação; 3.2 Possuir LEDs indicativos da atividade dos rádios; 3.3 Possuir LEDs indicativos da atividade da interface Gigabit Ethernet; 4. Antenas: 4.1 Possuir 6 (seis) antenas externas ao AP, em conformidade com o padrão IEEE 802.11a/b/g/n/ac; 4.2. Possuir ganho de, pelo menos, 5dBi para 2.4 GHz; 4.3. Possuir ganho de, pelo menos, 6dBi para 5.0 GHz; 4.4 Que implante padrão de irradiação omnidirecional; 4.5. Que implante operação simultânea em 3x3:3 MIMO; 5. Modo de Operação: 5.1 Implantar modo de operação onde o Ponto de Acesso possa estar remotamente conectado ao controlador wireless tanto de forma direta em uma rede de camada 2 ou em qualquer ponto de uma rede segmentada em subredes de camada 3; 5.2 O Ponto de Acesso deve permitir sua operação através da conexão a um controlador principal e a um controlador secundário; 5.3 Selecionar automaticamente o canal de transmissão; 5.4 Ajustar dinamicamente o nível de potência e canal de rádio; 5.5 Possuir suporte a pelo menos 8 SSIDs para 2.4GHz e 8 SSIDs para 5.0GHz; 5.6 Permitir habilitar e desabilitar a divulgação do SSID; 5.7 Deve implementar Fast Roaming ou funcionalidade similar de forma a garantir o Roaming sem perda de conexão; 5.8 Não deve haver licença restringindo o número de usuários por AP; 5.9 Implantar a pilha de protocolos TCP/IP; 5.10 Implantar VLANs conforme padrão IEEE 802.1Q; 5.11 Implantar cliente DHCP, para configuração automática de rede; 5.12 Configurar-se automaticamente ao ser conectado na rede; 5.13 Implementar Packet aggregation A-MPDU, A-MSDU para 802.11ac e 802.11n; 6. Gerenciamento: 6.1 Possuir porta de console para configuração; 6.2 Permitir via controlador wireless, a atualização remota do sistema operacional; 6.3 Permitir via controlador wireless, a atualização remota dos arquivos de configuração utilizados no equipamento; 6.4 Implantar funcionamento em modo gerenciado pelo controlador wireless; 7. Segurança e QoS: 7.2 Implantar varredura de Rádio Frequência nas tecnologias 802.11a, 802.11b/g, 802.11n e 802.11ac para identificação de AP não autorizados (rogues); 7.3 Implementar varredura de Rádio Frequência nas tecnologias 802.11a, 802.11b/g, 802.11n,				

		802.11ac para identificação de interferências nos canais na rede WLAN; 7.4 Implementar IEEE 802.1x de acesso do próprio AP a rede cabeada; 7.5 Implementar autenticação com geração dinâmica de chaves criptográficas por sessão e por usuário; 7.6 Implementar em conjunto com o Controlador WLAN, WEP, chaves estáticas e dinâmicas; 7.7 Implementar em conjunto com o Controlador WLAN, WPA com algoritmo de criptografia TKIP e MIC; 7.8 Implementar em conjunto com o Controlador WLAN, WPA2 com algoritmo de criptografia AES; 7.9 Implementar padrão IEEE 802.11e WMM da Wi-Fi Alliance para priorização de tráfego, suportando aplicações em tempo real, tais como VoIP e vídeo; 7.10 O sistema de monitoração e controle de RF deve possuir mecanismos de detecção e prevenção de intrusos no ambiente wireless; 7.11 Possuir grau de proteção IP67; 7.12 Implantar modo de operação onde o WIPS possa estar remotamente conectado ao controlador wireless tanto de forma direta em uma rede de camada 2 ou em qualquer ponto de uma rede segmentada em subredes de camada 3; 7.13 O WIPS deve permitir sua operação através da conexão a um controlador principal ou controlador secundário, realizando detecção de: 7.13.1 Rogue AP; 7.13.2 Honeypot; 7.13.3 Packet Injection; 7.13.4 Redes Ad hoc; 7.13.5 Main-in-the-middle; 7.13.6 Negação de Serviço (DoS); 7.13.7 MAC Spoofing; 7.13.8 Tentativa de quebra de chaves; 7.13.9 Reconhecimento de rede; 8. Certificações: 8.1 Possuir homologação da ANATEL, de acordo com a Resolução número 242. 8.2. Possuir certificação da Wi-Fi Alliance 9. Garantia: 9.1 O Ponto de Acesso deverá possuir garantia do fabricante pelo período mínimo de 60 (sessenta) meses. 9.2. Nos casos de troca equipamentos defeituosos, os mesmos devem ser enviados no próximo dia útil subsequente a abertura do chamado e comprovação do defeito, sem quaisquer custos adicionais. 9.3. Os chamados técnicos deverão ser gerenciados pelo fornecedor em horário comercial na modalidade 8x5 (oito horas por dia, cinco dias por semana), através de telefone gratuito. Também deve ser disponibilizado endereço de e-mail para abertura dos chamados técnicos. 9.4 A empresa deverá possuir pelo menos 1 (um) Engenheiro apto a prestar serviços de suporte técnico no equipamento proposto. O Engenheiro deverá possuir registro junto ao CREA e certificação no produto comprovada pelo fabricante. 9.5 O Fabricante deverá disponibilizar gratuitamente, suporte e atualizações dos softwares, firmwares e sistema operacional para correção de bugs e implementações de segurança. 9.6. Fornecer os softwares e suas atualizações, firmwares, sistema operacional através de meio eletrônico ou magnético sem ônus adicionais. 10. Compatibilidade: 10.1. Os componentes do Ponto de Acesso deverão ser homologados pelo fabricante. Não será aceita a adição ou subtração de qualquer componente não original de fábrica para adequação do equipamento; Todos os componentes deverão ser compatíveis entre si, com o conjunto do equipamento e com suas funcionalidades, sem a utilização de adaptadores, fresagens, pinturas, usinagens em geral, furações, emprego de adesivos, fitas				

		adesivas ou quaisquer outros procedimentos ou emprego de materiais inadequados ou que visem adaptar forçadamente o equipamento ou suas partes que sejam fisicamente ou logicamente incompatíveis. (Será aceito o regime de OEM desde que comprovado pelo próprio fabricante). 10.2 O Ponto de Acesso especificado neste item deve ser totalmente compatível com o Controlador Wireless Extreme Networks V2110. 10.3 O Ponto de Acesso especificado neste item deve ser totalmente compatível com a Solução de Gerenciamento NetSight Base 500. Referência: Marca Extreme Network, modelo WS-AP3865e ou de melhor qualidade. (TCU, Acórdão 2401/2006, 9.3.2 – Plenário). **(COTA PRINCIPAL)**				
68993	34	Ponto de Acesso Outdoor WS-AP3865e Tipo 1: 1. Características Básicas: 1.1 Ponto de Acesso deve atender simultaneamente aos padrões: IEEE 802.11a; IEEE 802.11b; IEEE 802.11g; IEEE 802.11n e IEEE 802.11ac; 1.2 Permitir a conexão simultânea de dispositivos configurados nos padrões: IEEE 802.11b/g/n; IEEE 802.11a/n e IEEE 802.11ac; 1.3 Implantar funcionamento simultâneo dos rádios 2.4GHz e 5.0GHz; 1.4 Implantar todas as seguintes taxas de transmissão e fallback automático: 1.4.1 IEEE 802.11a: 54, 48, 36, 24, 18, 12, 9 e 6 Mbps; 1.4.2 IEEE 802.11b: 11, 5.5, 2 e 1 Mbps; 1.4.3 IEEE 802.11g: 54, 48, 36, 24, 18, 12, 11, 9, 6, 5.5, 2 e 1 Mbps; 1.4.4 IEEE 802.11n: 450, 300, 270, 180, 120, 60, 45, 30 e 15 Mbps; 1.4.5 IEEE 802.11ac: 1300, 866.7, 780, 390, 260, 130, 97.5, 65 e 32.5 Mbps; 1.5 Possuir e acompanhar componentes que permita sua fixação em teto e parede; 1.6 Ponto de Acesso deve suportar performance em conexão cabeada de 75000pps; 1.7 Ponto de Acesso deve implementar instalação plug and play; 1.8 Ponto de Acesso deve implementar análise de espectro RF; 1.9 Ponto de Acesso deve implementar um modo hibrido de operação que seja capaz de suportar varredura de segurança e atender os clientes no mesmo rádio; 1.10 Deve implementar um modo de operação que seja capaz de fazer a varredura de segurança, trabalhando de forma dedicada, sem a necessidade de módulos de hardware adicionais para este fim. 1.11. Deve implementar associação de policies para clientes, sem precisar de segmentação via SSIDs dedicados; 2. Portas de Rede: 2.1 Possuir pelo menos 2 (duas) portas Gigabit Ethernet 10/100/1000 Mbps, auto-sensing, com conector RJ-45 Fêmea para dados, não sendo aceito portas de gerência; 2.2 Implementar agregação de links com suporte a LACP, permitindo agregar as 2 (duas) portas Gigabit Ethernet 10/100/1000 Mbps; 2.3 Permitir sua energização, pela interface de rede descrita no item anterior, através de um único injetor padrão IEEE 802.3af PoE; 2.4 O Ponto de Acesso deve permitir sua operação em capacidade máxima mesmo quando energizado através do injetor PoE; 3. Leds e Sinalização: 3.1 Possuir LEDs indicativos do estado de operação; 3.2 Possuir LEDs indicativos da atividade dos rádios; 3.3 Possuir LEDs indicativos da atividade da interface Gigabit Ethernet; 4. Antenas: 4.1 Possuir 6 (seis) antenas externas ao AP, em conformidade com o padrão IEEE 802.11a/b/g/n/ac; 4.2. Possuir ganho de, pelo menos, 5dBi para 2.4 GHz; 4.3. Possuir ganho de, pelo	un	1		

		menos, 6dBi para 5.0 GHz; 4.4 Que implante padrão de irradiação omnidirecional; 4.5. Que implante operação simultânea em 3x3:3 MIMO; 5. Modo de Operação: 5.1 Implantar modo de operação onde o Ponto de Acesso possa estar remotamente conectado ao controlador wireless tanto de forma direta em uma rede de camada 2 ou em qualquer ponto de uma rede segmentada em subredes de camada 3; 5.2 O Ponto de Acesso deve permitir sua operação através da conexão a um controlador principal e a um controlador secundário; 5.3 Selecionar automaticamente o canal de transmissão; 5.4 Ajustar dinamicamente o nível de potência e canal de rádio; 5.5 Possuir suporte a pelo menos 8 SSIDs para 2.4GHz e 8 SSIDs para 5.0GHz; 5.6 Permitir habilitar e desabilitar a divulgação do SSID; 5.7 Deve implementar Fast Roaming ou funcionalidade similar de forma a garantir o Roaming sem perda de conexão; 5.8 Não deve haver licença restringindo o número de usuários por AP; 5.9 Implantar a pilha de protocolos TCP/IP; 5.10 Implantar VLANs conforme padrão IEEE 802.1Q; 5.11 Implantar cliente DHCP, para configuração automática de rede; 5.12 Configurar-se automaticamente ao ser conectado na rede; 5.13 Implementar Packet aggregation A-MPDU, A-MSDU para 802.11ac e 802.11n; 6. Gerenciamento: 6.1 Possuir porta de console para configuração; 6.2 Permitir via controlador wireless, a atualização remota do sistema operacional; 6.3 Permitir via controlador wireless, a atualização remota dos arquivos de configuração utilizados no equipamento; 6.4 Implantar funcionamento em modo gerenciado pelo controlador wireless; 7. Segurança e QoS: 7.2 Implantar varredura de Rádio Frequência nas tecnologias 802.11a, 802.11b/g, 802.11n e 802.11ac para identificação de AP não autorizados (rogues); 7.3 Implementar varredura de Rádio Frequência nas tecnologias 802.11a, 802.11b/g, 802.11n, 802.11ac para identificação de interferências nos canais na rede WLAN; 7.4 Implementar IEEE 802.1x de acesso do próprio AP a rede cabeada; 7.5 Implementar autenticação com geração dinâmica de chaves criptográficas por sessão e por usuário; 7.6 Implementar em conjunto com o Controlador WLAN, WEP, chaves estáticas e dinâmicas; 7.7 Implementar em conjunto com o Controlador WLAN, WPA com algoritmo de criptografia TKIP e MIC; 7.8 Implementar em conjunto com o Controlador WLAN, WPA2 com algoritmo de criptografia AES; 7.9 Implementar padrão IEEE 802.11e WMM da Wi-Fi Alliance para priorização de tráfego, suportando aplicações em tempo real, tais como VoIP e vídeo; 7.10 O sistema de monitoração e controle de RF deve possuir mecanismos de detecção e prevenção de intrusos no ambiente wireless; 7.11 Possuir grau de proteção IP67; 7.12 Implantar modo de operação onde o WIPS possa estar remotamente conectado ao controlador wireless tanto de forma direta em uma rede de camada 2 ou em qualquer ponto de uma rede segmentada em subredes de camada 3; 7.13 O WIPS deve permitir sua operação através da conexão a um controlador principal ou controlador secundário, realizando detecção de: 7.13.1 Rogue AP; 7.13.2 Honeypot; 7.13.3 Packet Injection; 7.13.4				

		Redes Ad hoc; 7.13.5 Main-in-the-middle; 7.13.6 Negação de Serviço (DoS); 7.13.7 MAC Spoofing; 7.13.8 Tentativa de quebra de chaves; 7.13.9 Reconhecimento de rede; 8. Certificações: 8.1 Possuir homologação da ANATEL, de acordo com a Resolução número 242. 8.2. Possuir certificação da Wi-Fi Alliance 9. Garantia: 9.1 O Ponto de Acesso deverá possuir garantia do fabricante pelo período mínimo de 60 (sessenta) meses. 9.2. Nos casos de troca equipamentos defeituosos, os mesmos devem ser enviados no próximo dia útil subsequente a abertura do chamado e comprovação do defeito, sem quaisquer custos adicionais. 9.3. Os chamados técnicos deverão ser gerenciados pelo fornecedor em horário comercial na modalidade 8x5 (oito horas por dia, cinco dias por semana), através de telefone gratuito. Também deve ser disponibilizado endereço de e-mail para abertura dos chamados técnicos. 9.4 A empresa deverá possuir pelo menos 1 (um) Engenheiro apto a prestar serviços de suporte técnico no equipamento proposto. O Engenheiro deverá possuir registro junto ao CREA e certificação no produto comprovada pelo fabricante. 9.5 O Fabricante deverá disponibilizar gratuitamente, suporte e atualizações dos softwares, firmwares e sistema operacional para correção de bugs e implementações de segurança. 9.6. Fornecer os softwares e suas atualizações, firmwares, sistema operacional através de meio eletrônico ou magnético sem ônus adicionais. 10. Compatibilidade: 10.1. Os componentes do Ponto de Acesso deverão ser homologados pelo fabricante. Não será aceita a adição ou subtração de qualquer componente não original de fábrica para adequação do equipamento; Todos os componentes deverão ser compatíveis entre si, com o conjunto do equipamento e com suas funcionalidades, sem a utilização de adaptadores, fresagens, pinturas, usinagens em geral, furações, emprego de adesivos, fitas adesivas ou quaisquer outros procedimentos ou emprego de materiais inadequados ou que visem adaptar forçadamente o equipamento ou suas partes que sejam fisicamente ou logicamente incompatíveis. (Será aceito o regime de OEM desde que comprovado pelo próprio fabricante). 10.2 O Ponto de Acesso especificado neste item deve ser totalmente compatível com o Controlador Wireless Extreme Networks V2110. 10.3 O Ponto de Acesso especificado neste item deve ser totalmente compatível com a Solução de Gerenciamento NetSight Base 500. Referência: Marca Extreme Network, modelo WS-AP3865e ou de melhor qualidade. (TCU, Acórdão 2401/2006, 9.3.2 – Plenário). **(COTA RESERVADA ME/EPP/MEI) – VINCULADO AO ITEM 33**				
68948	35	Switch de Acesso 24 portas PoE Summit X430-24p: Tipo 2 1. Gabinete/Chassis: 1.1 A solução deve ser composta de um único equipamento, montável em rack 19 polegadas devendo este vir acompanhado dos devidos acessórios para tal. 1.2. Possuir leds indicativos de funcionamento da fonte de alimentação, ventiladores e status das portas. 1.3. Possuir altura máxima de 1U (1,75”). 2. Fonte de Alimentação: 2.1 Possuir fonte de alimentação interna que trabalhe em 100V-240V, 50/60 Hz, com detecção automática	un	1		

		de tensão e frequência. 3. Performance/Desempenho: 3.1 Possuir, no mínimo, 56 Gbps de Switch Fabric. 3.2. Possuir a capacidade de encaminhamentos de pacotes, de no mínimo 41 Mpps utilizando pacotes de 64 bytes. 3.3. Deve armazenar, no mínimo, 16.000 (dezesseis mil) endereços MAC. 3.4. Implementar jumbo frames em todas as portas ofertadas, com suporte a pacotes de até 9216 Bytes. 4. Portas/Interfaces: 4.1 Todas as interfaces ofertadas devem ser non-blocking. 4.2. Possuir 4 (quatro) interfaces Gigabit Ethernet baseadas mini-GBIC, devendo um mesmo mini-GBIC-Slot suportar interfaces 1000BASE-T SFP, 1000Base-SX, 1000Base-LX e 1000BASE-ZX não sendo permitida a utilização de conversores externos. 4.3 Todas as interfaces Gigabit Ethernet, solicitadas nesta especificação, devem funcionar perfeitamente. 4.4. Possuir porta de console com conector RJ-45 ou DB9 macho. 4.5. Possuir 24 portas 10/100/1000BASE-T ativas simultaneamente, com conector RJ-45. 4.6 O equipamento deve possuir além das portas acima citadas uma porta adicional 10/100 com conector RJ-45 para gerência out-of-band do equipamento. 4.7 Detecção automática MDI/MDIX em todas as portas UTP RJ-45. 4.8 Implementar Power over Ethernet (PoE) segundo o padrão IEEE 802.3af em todas as portas 1000Base-T, com no mínimo 370W de potência disponível para dispositivos PoE através de fonte interna. 4.9 Implementar Power over Ethernet Plus (PoE-Plus) segundo o padrão IEEE 802.3at em todas as portas 10/100/1000Base-T, com no mínimo 370W de potência disponível para dispositivos PoE através de fonte interna. 5. Sistema Operacional: 5.1 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. 6. Funcionalidades de Camada 2: 6.1 Implementar EAPS (RFC 3619) ou protocolo similar de resiliência em camada 2, específico para topologias em anel, que permita tempo de convergência inferior a 200 ms. 6.2. Implementar 4094 VLANs por porta, ativas simultaneamente. 6.3 Implementar Private VLANs. 6.4. Implementar agregação de links conforme padrão IEEE 802.3ad com suporte a LACP. 6.5. Implementar agregação de links conforme padrão IEEE 802.3ad com, no mínimo, 124 grupos, sendo 8 links agregados por grupo. 6.6. Implementar Spanning-Tree (IEEE 802.1d), Rapid Spanning Tree (IEEE 802.1w), Multiple Instance STP (802.1s) e PVST+. 6.7. 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. 6.8. Implementar funcionalidade vinculada ao Spanning-tree que evite a eleição de outros switches da rede como Root. 6.9. Implementar funcionalidade vinculada ao Spanning-tree que permita desabilitar uma porta de acesso assim que a mesma receba uma BPDU. 7. Gerenciamento/Monitoramento: 7.1				

		Implementar os seguintes grupos de RMON através da RFC1757: History, Statistics, Alarms e Events. 7.2. Implementar gerenciamento via web com suporte a HTTP e HTTPS/SSL. Esta funcionalidade deve ser implícita ao equipamento. 7.3. 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. 8. Funcionalidades Gerais: 8.1 Deve implementar Dual Stack, ou seja, IPV6 e IPv4. 8.2. Implementar IGMP v1 e v2 Snooping 8.3 Implementar sFlow V5 ou Netflow V5, em hardware. Não serão aceitas soluções similares. 8.4 Implementar Port Mirroring e RSPAN (Remote Mirroring). 8.5. Implementar IPv6 em hardware. 8.6. Implementar os seguintes protocolos em IPv6: Ping, Traceroute, Telnet, SSH-2. 8.7. Implementar IEEE 802.1ab Link Layer Discovery Protocol (LLDP). 8.8. Implementar LLDP-MED (Media Endpoint Discovery), segundo ANSI/TIA-1057, Draft 08. 8.9. 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. 8.10. Suportar transferência de arquivos através dos protocolos TFTP e SCP. 8.11. Implementar a atualização de imagens de software e configuração através de um servidor TFTP. 8.12. Implementar DHCP/Bootp relay. 8.13. Implementar servidor DHCP interno que permita a configuração de um intervalo de endereços IP a serem atribuídos os clientes DHCP. 8.14. Implementar funcionalidade que permita sua autoconfiguração através dos protocolos DHCP e TFTP, permitindo o provisionamento em massa com o mínimo de intervenção humana. 8.15. Suportar múltiplos servidores Syslog. 8.16. 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. 8.17. Implementar ajuste de clock do equipamento utilizando NTP com autenticação MD5 ou SNTP. 8.18 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. 8.19 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. 8.20 A funcionalidade de Rate Shaping deve permitir a configuração de CIR (Commited Rate) e peak rate. 8.21. Implementar 8 filas de prioridade em hardware por porta. 8.22. Implementar a leitura, classificação e remarcação de QoS (802.1p e DSCP). 8.23. Implementar remarcação de prioridade de				

		pacotes Layer 3, remarcando o campo DiffServ para grupos de tráfego classificados segundo portas TCP e UDP, endereço/sub-rede IP, VLAN e MAC origem e destino. 8.24. 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, 802.1p. 9. Funcionalidades de Politicas & Segurança: 9.1 Implementar 1000 regras de ACL. 9.2. Implementar ACLs de entrada (ingress ACLs) em hardware, baseadas em critérios das camadas 2 (MAC origem e destino) e campo 802.1p, 3 (IP origem e destino) e 4 (portas TCP e UDP), em todas as interfaces e VLANs, com suporte a endereços IPv6. Deverá ser possível aplicar ACLs para tráfego interno de uma determinada VLAN. 9.3. 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. 9.4 Implementar Policy Based Switching, ou seja, possibilitar que o tráfego classificado por uma ACL seja redirecionado para uma porta física específica. 9.5. 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. 9.6. Implementar limitação de número de endereços MAC aprendidos por uma porta, para uma determinada VLAN. 9.7. 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. 9.8. 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. 9.9 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. 9.10. Implementar múltiplos suplicantes por porta, onde cada dispositivo deve ser autenticado de forma independente, podendo ser encaminhados à VLANs distintas. As múltiplas autenticações devem ser realizadas através de IEEE 802.1x. 9.11 Implementar TACACS+ segundo a RFC 1492. Não serão aceitas soluções similares. 9.12. Implementar autenticação RADIUS com suporte a: 9.12.1 RADIUS Authentication; 9.12.2 RADIUS Accounting; 9.12.3 RADIUS EAP support for 802.1X . 9.13 A implementação de RADIUS e TACACS+ deve estar disponível para autenticação de usuários via Telnet e Console serial. 9.14. Implementar RADIUS e TACACS+ per-command authentication. 9.15. Implementar autenticação baseada em web, com suporte a SSL, através de RADIUS ou através da base local do switch. 9.16. Implementar autenticação baseada em endereço MAC, através de RADIUS ou através da base local do switch. 9.17. Implementar funcionalidade que permita que somente servidores DHCP autorizados atribuam configuração IP aos clientes DHCP (Trusted DHCP Server). 10.				

		Certificações: 10.1 Possuir homologação da ANATEL, de acordo com a Resolução número 242. 11. Garantia: 11.1 O Switch de Acesso deverá possuir garantia do fabricante pelo período mínimo de 60 (sessenta) meses. 11.2. Nos casos de troca equipamentos defeituosos, os mesmos devem ser enviados no próximo dia útil subsequente a abertura do chamado e comprovação do defeito, sem quaisquer custos adicionais. 11.3. Os chamados técnicos deverão ser gerenciados pelo fornecedor em horário comercial na modalidade 8x5 (oito horas por dia, cinco dias por semana), através de telefone gratuito. Também deve ser disponibilizado endereço de e-mail para abertura dos chamados técnicos. 11.4 A empresa deverá possuir pelo menos 1 (um) Engenheiro apto a prestar serviços de suporte técnico no equipamento proposto. O Engenheiro deverá possuir registro junto ao CREA e certificação no produto comprovada pelo fabricante. 11.5 O Fabricante deverá disponibilizar gratuitamente suporte e atualização dos softwares, firmwares e sistema operacional para correção de bugs e implementações de segurança; 11.6 Fornecer os softwares e suas atualizações, firmwares, sistema operacional através de meio eletrônico ou magnético sem ônus adicionais. 12. Compatibilidade: 12.1. Os componentes do Switch de Acesso deverão ser homologados pelo fabricante. Não será aceita a adição ou subtração de qualquer componente não original de fábrica para adequação do equipamento; 12.2 Todos os componentes do Switch de Acesso deverão ser compatíveis entre si, com o conjunto do equipamento e com suas funcionalidades, sem a utilização de adaptadores, fresagens, pinturas, usinagens em geral, furações, emprego de adesivos, fitas adesivas ou quaisquer outros procedimentos ou emprego de materiais inadequados ou que visem adaptar forçadamente o equipamento ou suas partes que sejam fisicamente ou logicamente incompatíveis. (Será aceito o regime de OEM desde que comprovado pelo próprio fabricante). 12.3 O Switch de Acesso especificado neste item deve ser totalmente compatível com a Solução de Gerenciamento NetSight Base 500. Referência: Marca Extreme Network, modelo Summit X430-24p ou de melhor qualidade. (TCU, Acórdão 2401/2006, 9.3.2 – Plenário).				
68959	36	Switch de Acesso 24 portas PoE Summit X440-24p: Tipo 5 1. Gabinete/Chassis: 1.1 A solução deve ser composta de um único equipamento, montável em rack 19” devendo este vir acompanhado dos devidos acessórios para tal. 1.2. Possuir leds indicativos de funcionamento da fonte de alimentação, ventiladores e status das portas. 1.3. Possuir altura máxima de 1U (1,75”). 2. Fonte de Alimentação: 2.1 Possuir fonte de alimentação interna que trabalhe em 100V-240V, 50/60 Hz, com detecção automática de tensão e frequência. 2.2. Suportar fonte de alimentação redundante interna ou externa. 3. Performance/Desempenho: 3.1 Possuir, no mínimo, 88 Gbps de Switch Fabric. 3.2. Possuir a capacidade de encaminhamentos de pacotes, de no mínimo 65 Mpps utilizando pacotes de 64 bytes. 3.3. Deve armazenar, no mínimo, 16.000 (dezesseis mil) endereços MAC. 3.4. Implementar jumbo frames	un	1		

		em todas as portas ofertadas, com suporte a pacotes de até 9216 Bytes. 4. Portas/Interfaces: 4.1 Todas as interfaces ofertadas devem ser non-blocking. 4.2. Possuir, no mínimo, 4 (quatro) interfaces Gigabit Ethernet baseadas mini-GBIC, devendo um mesmo mini-GBIC-Slot suportar interfaces 1000BASE-T SFP, 1000Base-SX, 1000Base-LX e 1000BASE-ZX não sendo permitida a utilização de conversores externos. 4.3. Possuir 20 portas 10/100/1000BASE-T ativas simultaneamente, com conector RJ-45. 4.4. Possuir porta de console com conector RJ-45 ou DB9 macho. 4.5 O equipamento deve possuir além das portas acima citadas uma porta adicional 10/100 com conector RJ-45 para gerência out-of-band do equipamento. 4.6 Detecção automática MDI/MDIX em todas as portas UTP RJ-45. 4.7 Implementar Power over Ethernet (PoE) segundo o padrão IEEE 802.3af em todas as portas 1000Base-T, com no mínimo 380W de potência disponível para dispositivos PoE através de fonte interna. 4.8 Implementar Power over Ethernet Plus (PoE-Plus) segundo o padrão IEEE 802.3at em todas as portas 10/100/1000Base-T, com no mínimo 380W de potência disponível para dispositivos PoE através de fonte interna. 5. Empilhamento: 5.1 Implementar empilhamento de até oito equipamentos e gerência através de um único endereço IP. 5.2 O equipamento deve possuir portas para empilhamento com velocidade de pelo menos 20Gbps cada (ou 10Gbps Full Duplex), totalizando 40 Gbps (ou 20 Gbps full-duplex). 5.3 Todas as interfaces Gigabit Ethernet e portas específicas para empilhamento, solicitadas nesta especificação, devem funcionar simultaneamente. 5.4 O empilhamento deve possuir arquitetura de anel para prover resiliência. 5.5 O empilhamento deve permitir a criação de grupos de links agregados entre diferentes membros da pilha, segundo 802.3ad. 5.6 O empilhamento deve suportar espelhamento de tráfego entre diferentes unidades da pilha. 5.7. Deve ser possível mesclar em uma mesma pilha equipamentos que não implementem PoE. 5.8 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. 5.9. Possuir indicação visual no painel frontal do equipamento que permita identificar a posição lógica do equipamento da pilha 6. Sistema Operacional: 6.1 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. 6.2 O equipamento ofertado deve possuir um sistema operacional modular. 7. Funcionalidades de Camada 3: 7.1 Deve implementar Dual Stack, ou seja, IPV6 e IPv4. 7.2. Implementar roteamento estático com suporte a, no mínimo, 32 rotas. 7.3. Implementar, no mínimo, 256 interfaces IP (v4 ou v6). 7.4. Implementar IGMPv1 (RFC 1112), IGMP v2 (RFC 2236), IGMP v3 (RFC 3376). 7.5. Implementar os protocolos de roteamento IP: RFC 1058 – RIP v1 e RFC 2453 – RIP v2. 7.6. Suportar o protocolo de roteamento OSPF v2, incluindo autenticação MD5. 7.7. Implementar PIM Snooping. 7.8. Suportar protocolo de				

		multicast PIM-SM. 7.9 Suportar VRRPv3 (RFC 5798) ou similar. 7.10. Implementar MLD Snooping v1 e v2. 8. Funcionalidades de Camada 2: 8.1 Implementar EAPS (RFC 3619) ou protocolo similar de resiliência em camada 2, específico para topologias em anel, que permita tempo de convergência inferior a 200 ms. 8.2. Implementar 4094 VLANs por porta, ativas simultaneamente. 8.3 Implementar Private VLANs. 8.4. Implementar agregação de links conforme padrão IEEE 802.3ad com suporte a LACP. 8.5. Implementar agregação de links conforme padrão IEEE 802.3ad com, no mínimo, 128 grupos, sendo 8 links agregados por grupo. 8.6 Implementar Spanning-Tree (IEEE 802.1d), Rapid Spanning Tree (IEEE 802.1w), Multiple Instance STP (802.1s) e PVST+. 8.7. 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. 8.8. Implementar funcionalidade vinculada ao Spanning-tree que evite a eleição de outros switches da rede como Root. 8.9. Implementar funcionalidade vinculada ao Spanning-tree que permita desabilitar uma porta de acesso assim que a mesma receba uma BPDU. 9. Gerenciamento/Monitoramento: 9.1 Implementar os seguintes grupos de RMON através da RFC1757: History, Statistics, Alarms e Events. 9.2. Implementar gerenciamento via web com suporte a HTTP e HTTPS/SSL. Esta funcionalidade deve ser implícita ao equipamento. 9.3. 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. 10. Funcionalidades Gerais: 10.1 Implementar sFlow V5 ou Netflow V5, em hardware. Não serão aceitas soluções similares. 10.2 Implementar Port Mirroring e RSPAN (Remote Mirroring). 10.3. Implementar IPv6 em hardware nos módulos de interface. 10.4. Implementar os seguintes protocolos em IPv6: Ping, Traceroute, Telnet, SSH-2. 10.5. Implementar IEEE 802.1ab Link Layer Discovery Protocol (LLDP). 10.6. Implementar LLDP-MED (Media Endpoint Discovery), segundo ANSI/TIA-1057, Draft 08. 10.7. 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. 10.8. Suportar transferência de arquivos através dos protocolos TFTP e SCP. 10.9. Implementar a atualização de imagens de software e configuração através de um servidor TFTP. 10.10. Implementar DHCP/Bootp relay. 10.11. Implementar servidor DHCP interno que permita a configuração de um intervalo de endereços IP a serem atribuídos os clientes DHCP. 10.12. Implementar funcionalidade que permita sua autoconfiguração através dos protocolos DHCP e TFTP, permitindo o provisionamento em massa com o mínimo de intervenção humana. 10.13. Suportar múltiplos servidores Syslog. 10.14. 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. 10.15. Implementar ajuste de clock do equipamento utilizando NTP com autenticação MD5 ou SNTP. 10.16 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. 10.17 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. 10.18 A funcionalidade de Rate Shaping deve permitir a configuração de CIR (Commited Rate) e peak rate. 10.19. Implementar 8 filas de prioridade em hardware por porta. 10.20. Implementar a leitura, classificação e remarcação de QoS (802.1p e DSCP). 10.21. 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. 10.22. 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, 802.1p. 11. Funcionalidades de Politicas & Segurança: 11.1 Implementar 1000 regras de ACL. 11.2 Implementar Policy Based Routing. 11.3. Implementar ACLs de entrada (ingress ACLs) em hardware, baseadas em critérios das camadas 2 (MAC origem e destino) e campo 802.1p, 3 (IP origem e destino) e 4 (portas TCP e UDP), em todas as interfaces e VLANs, com suporte a endereços IPv6. Deverá ser possível aplicar ACLs para tráfego interno de uma determinada VLAN. 11.4. 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. 11.5 Implementar Policy Based Switching, ou seja, possibilitar que o tráfego classificado por uma ACL seja redirecionado para uma porta física específica. 11.6 Implementar Gratuitous ARP Protection. 11.7. 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. 11.8. Implementar limitação de número de endereços MAC aprendidos por uma porta, para uma determinada VLAN. 11.9. 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. 11.10. 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. 11.11 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. 11.12. Implementar múltiplos suplicantes por porta, onde cada dispositivo deve ser autenticado de forma independente, podendo ser encaminhados à VLANs distintas. As múltiplas autenticações devem ser realizadas através de IEEE 802.1x. 11.13 Implementar TACACS+ segundo a RFC 1492. Não serão aceitas soluções similares. 11.14. Implementar autenticação RADIUS com suporte a: 11.14.1 RADIUS Authentication; 11.14.2 RADIUS Accounting; 11.14.3 RADIUS EAP support for 802.1X; 11.15 A implementação de RADIUS e TACACS+ deve estar disponível para autenticação de usuários via Telnet e Console serial. 11.16. Implementar RADIUS e TACACS+ per-command authentication. 11.17. Implementar autenticação baseada em web, com suporte a SSL, através de RADIUS ou através da base local do switch. 11.18. Implementar autenticação baseada em endereço MAC, através de RADIUS ou através da base local do switch. 11.19. Implementar funcionalidade que permita que somente servidores DHCP autorizados atribuam configuração IP aos clientes DHCP (Trusted DHCP Server). 12. Certificações: 12.1 Possuir homologação da ANATEL, de acordo com a Resolução número 242. 13. Garantia: 13.1 O Switch de Acesso deverá possuir garantia do fabricante pelo período mínimo de 60 (sessenta) meses. 13.2. Nos casos de troca equipamentos defeituosos, os mesmos devem ser enviados no próximo dia útil subsequente a abertura do chamado e comprovação do defeito, sem quaisquer custos adicionais. 13.3. Os chamados técnicos deverão ser gerenciados pelo fornecedor em horário comercial na modalidade 8x5 (oito horas por dia, cinco dias por semana), através de telefone gratuito. Também deve ser disponibilizado endereço de e-mail para abertura dos chamados técnicos. 13.4 A empresa deverá possuir pelo menos 1 (um) Engenheiro apto a prestar serviços de suporte técnico no equipamento proposto. O Engenheiro deverá possuir registro junto ao CREA e certificação no produto comprovada pelo fabricante. 13.5 O Fabricante deverá disponibilizar gratuitamente suporte e atualização dos softwares, firmwares e sistema operacional para correção de bugs e implementações de segurança; 13.6 Fornecer os softwares e suas atualizações, firmwares, sistema operacional através de meio eletrônico ou magnético sem ônus adicionais. 14. Compatibilidade: 14.1. Os componentes do Switch de Acesso deverão ser homologados pelo fabricante. Não será aceita a adição ou subtração de qualquer componente não original de fábrica para adequação do equipamento; 14.2 Todos os componentes do Switch de Acesso deverão ser compatíveis entre si, com o conjunto do equipamento e com suas funcionalidades, sem a utilização de adaptadores, fresagens, pinturas, usinagens em geral, furações,				

		emprego de adesivos, fitas adesivas ou quaisquer outros procedimentos ou emprego de materiais inadequados ou que visem adaptar forçadamente o equipamento ou suas partes que sejam fisicamente ou logicamente incompatíveis. (Será aceito o regime de OEM desde que comprovado pelo próprio fabricante). 14.3 O Switch de Acesso especificado neste item deve ser totalmente compatível com a Solução de Gerenciamento NetSight Base 500. Referência: Marca Extreme Network, modelo Summit X440-24p ou de melhor qualidade. (TCU, Acórdão 2401/2006, 9.3.2 – Plenário).				
68945	37	Switch de Acesso 24 portas Summit X430-24t: Tipo 1 1. Gabinete/Chassis: 1.1. A solução deve ser composta de um único equipamento, montável em rack 19 polegadas devendo este vir acompanhado dos devidos acessórios para tal. 1.2. Possuir leds indicativos de funcionamento da fonte de alimentação, ventiladores e status das portas. 1.3. Possuir altura máxima de 1U (1,75”). 2. Fonte de Alimentação: 2.1 Possuir fonte de alimentação interna que trabalhe em 100V-240V, 50/60 Hz, com detecção automática de tensão e frequência. 3. Performance/Desempenho: 3.1 Possuir, no mínimo, 56 Gbps de Switch Fabric. 3.2. Possuir a capacidade de encaminhamentos de pacotes, de no mínimo 41 Mpps utilizando pacotes de 64 bytes. 3.3. Deve armazenar, no mínimo, 16.000 (dezesseis mil) endereços MAC. 3.4. Implementar jumbo frames em todas as portas ofertadas, com suporte a pacotes de até 9216 Bytes. 4. Portas/Interfaces: 4.1 Todas as interfaces ofertadas devem ser non-blocking. 4.2. Possuir 4 (quatro) interfaces Gigabit Ethernet baseadas mini-GBIC, devendo um mesmo mini-GBIC-Slot suportar interfaces 1000BASE-T SFP, 1000Base-SX, 1000Base-LX e 1000BASE-ZX não sendo permitida a utilização de conversores externos. 4.3 Todas as interfaces Gigabit Ethernet, solicitadas nesta especificação, devem funcionar perfeitamente. 4.4. Possuir porta de console com conector RJ-45 ou DB9 macho. 4.5. Possuir 24 portas 10/100/1000BASE-T ativas simultaneamente, com conector RJ-45. 4.6 O equipamento deve possuir além das portas acima citadas uma porta adicional 10/100 com conector RJ-45 para gerência out-of-band do equipamento. 4.7 Detecção automática MDI/MDIX em todas as portas UTP RJ-45. 5. Sistema Operacional: 5.1 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. 6. Funcionalidades de Camada 2: 6.1 Implementar EAPS (RFC 3619) ou protocolo similar de resiliência em camada 2, específico para topologias em anel, que permita tempo de convergência inferior a 200 ms. 6.2. Implementar 4094 VLANs por porta, ativas simultaneamente. 6.3 Implementar Private VLANs. 6.4. Implementar agregação de links conforme padrão IEEE 802.3ad com suporte a LACP. 6.5. Implementar agregação de links conforme padrão IEEE 802.3ad com, no mínimo, 124 grupos, sendo 8 links agregados por grupo. 6.6. Implementar Spanning-Tree (IEEE 802.1d), Rapid Spanning Tree (IEEE 802.1w), Multiple	un	1		

		Instance STP (802.1s) e PVST+. 6.7. 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. 6.8. Implementar funcionalidade vinculada ao Spanning-tree que evite a eleição de outros switches da rede como Root. 6.9. Implementar funcionalidade vinculada ao Spanning-tree que permita desabilitar uma porta de acesso assim que a mesma receba uma BPDU. 7. Gerenciamento/Monitoramento: 7.1 Implementar os seguintes grupos de RMON através da RFC1757: History, Statistics, Alarms e Events. 7.2. Implementar gerenciamento via web com suporte a HTTP e HTTPS/SSL. Esta funcionalidade deve ser implícita ao equipamento. 7.3. 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. 8. Funcionalidades Gerais: 8.1 Deve implementar Dual Stack, ou seja, IPV6 e IPv4. 8.2. Implementar IGMP v1 e v2 Snooping 8.3 Implementar sFlow V5 ou Netflow V5, em hardware. Não serão aceitas soluções similares. 8.4 Implementar Port Mirroring e RSPAN (Remote Mirroring). 8.5. Implementar IPv6 em hardware. 8.6. Implementar os seguintes protocolos em IPv6: Ping, Traceroute, Telnet, SSH-2. 8.7. Implementar IEEE 802.1ab Link Layer Discovery Protocol (LLDP). 8.8. Implementar LLDP-MED (Media Endpoint Discovery), segundo ANSI/TIA-1057, Draft 08. 8.9. 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. 8.10. Suportar transferência de arquivos através dos protocolos TFTP e SCP. 8.11. Implementar a atualização de imagens de software e configuração através de um servidor TFTP. 8.12 implementar DHCP/Bootp relay. 8.13. Implementar servidor DHCP interno que permita a configuração de um intervalo de endereços IP a serem atribuídos os clientes DHCP. 8.14. Implementar funcionalidade que permita sua autoconfiguração através dos protocolos DHCP e TFTP, permitindo o provisionamento em massa com o mínimo de intervenção humana. 8.15. Suportar múltiplos servidores Syslog. 8.16. 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. 8.17. Implementar ajuste de clock do equipamento utilizando NTP com autenticação MD5 ou SNTP. 8.18 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. 8.19 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. 8.20 A funcionalidade de Rate Shaping deve permitir a configuração de CIR (Commited Rate) e peak rate. 8.21. Implementar 8 filas de prioridade em hardware por porta. 8.22. Implementar a leitura, classificação e remarcação de QoS (802.1p e DSCP). 8.23. 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. 8.24. 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, 802.1p. 9. Funcionalidades de Politicas & Segurança: 9.1 Implementar 1000 regras de ACL. 9.2. Implementar ACLs de entrada (ingress ACLs) em hardware, baseadas em critérios das camadas 2 (MAC origem e destino) e campo 802.1p, 3 (IP origem e destino) e 4 (portas TCP e UDP), em todas as interfaces e VLANs, com suporte a endereços IPv6. Deverá ser possível aplicar ACLs para tráfego interno de uma determinada VLAN. 9.3. 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. 9.4 Implementar Policy Based Switching, ou seja, possibilitar que o tráfego classificado por uma ACL seja redirecionado para uma porta física específica. 9.5. 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. 9.6. Implementar limitação de número de endereços MAC aprendidos por uma porta, para uma determinada VLAN. 9.7. 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. 9.8. 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. 9.9 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. 9.10. Implementar múltiplos suplicantes por porta, onde cada dispositivo deve ser autenticado de forma independente, podendo ser encaminhados à VLANs distintas. As múltiplas autenticações devem ser realizadas através de IEEE 802.1x. 9.11 Implementar TACACS+ segundo a RFC 1492. Não serão aceitas soluções similares. 9.12. Implementar autenticação RADIUS com suporte a: 9.12.1 RADIUS				

		Authentication; 9.12.2 RADIUS Accounting; 9.12.3 RADIUS EAP support for 802.1X . 9.13 A implementação de RADIUS e TACACS+ deve estar disponível para autenticação de usuários via Telnet e Console serial. 9.14. Implementar RADIUS e TACACS+ per-command authentication. 9.15. Implementar autenticação baseada em web, com suporte a SSL, através de RADIUS ou através da base local do switch. 9.16. Implementar autenticação baseada em endereço MAC, através de RADIUS ou através da base local do switch. 9.17. Implementar funcionalidade que permita que somente servidores DHCP autorizados atribuam configuração IP aos clientes DHCP (Trusted DHCP Server). 10. Certificações: 10.1 Possuir homologação da ANATEL, de acordo com a Resolução número 242. 11. Garantia: 11.1 O Switch de Acesso deverá possuir garantia do fabricante pelo período mínimo de 60 (sessenta) meses. 11.2. Nos casos de troca equipamentos defeituosos, os mesmos devem ser enviados no próximo dia útil subsequente a abertura do chamado e comprovação do defeito, sem quaisquer custos adicionais. 11.3. Os chamados técnicos deverão ser gerenciados pelo fornecedor em horário comercial na modalidade 8x5 (oito horas por dia, cinco dias por semana), através de telefone gratuito. Também deve ser disponibilizado endereço de e-mail para abertura dos chamados técnicos. 11.4 A empresa deverá possuir pelo menos 1 (um) Engenheiro apto a prestar serviços de suporte técnico no equipamento proposto. O Engenheiro deverá possuir registro junto ao CREA e certificação no produto comprovada pelo fabricante. 11.5 O Fabricante deverá disponibilizar gratuitamente suporte e atualização dos softwares, firmwares e sistema operacional para correção de bugs e implementações de segurança; 11.6 Fornecer os softwares e suas atualizações, firmwares, sistema operacional através de meio eletrônico ou magnético sem ônus adicionais. 12. Compatibilidade: 12.1. Os componentes do Switch de Acesso deverão ser homologados pelo fabricante. Não será aceita a adição ou subtração de qualquer componente não original de fábrica para adequação do equipamento; 12.2 Todos os componentes do Switch de Acesso deverão ser compatíveis entre si, com o conjunto do equipamento e com suas funcionalidades, sem a utilização de adaptadores, fresagens, pinturas, usinagens em geral, furações, emprego de adesivos, fitas adesivas ou quaisquer outros procedimentos ou emprego de materiais inadequados ou que visem adaptar forçadamente o equipamento ou suas partes que sejam fisicamente ou logicamente incompatíveis. (Será aceito o regime de OEM desde que comprovado pelo próprio fabricante). 12.3 O Switch de Acesso especificado neste item deve ser totalmente compatível com a Solução de Gerenciamento NetSight Base 500. Referência: Marca Extreme Network, modelo Summit X430-24t ou de melhor qualidade. (TCU, Acórdão 2401/2006, 9.3.2 – Plenário).				
68961	38	Switch de Acesso 24 portas Summit X440-24t-10G: Tipo 7 1. Gabinete/Chassis: 1.1 A solução deve ser composta de um único equipamento, montável em rack 19” devendo este vir acompanhado dos devidos	un	1		

		acessórios para tal. 1.2. Possuir leds indicativos de funcionamento da fonte de alimentação, ventiladores e status das portas. 1.3. Possuir altura máxima de 1U (1,75”). 2. Fonte de Alimentação: 2.1 Possuir fonte de alimentação interna que trabalhe em 100V-240V, 50/60 Hz, com detecção automática de tensão e frequência. 2.2. Suportar fonte de alimentação redundante interna ou externa. 3. Performance/Desempenho: 3.1 Possuir, no mínimo, 88 Gbps de Switch Fabric. 3.2. Possuir a capacidade de encaminhamentos de pacotes, de no mínimo 65 Mpps utilizando pacotes de 64 bytes. 3.3. Deve armazenar, no mínimo, 16.000 (dezesseis mil) endereços MAC. 3.4. Implementar jumbo frames em todas as portas ofertadas, com suporte a pacotes de até 9216 Bytes. 4. Portas/Interfaces: 4.1 Todas as interfaces ofertadas devem ser non-blocking. 4.2. Possuir, no mínimo, 4 (quatro) interfaces Gigabit Ethernet baseadas mini-GBIC, devendo um mesmo mini-GBIC-Slot suportar interfaces 1000BASE-T SFP, 1000Base-SX, 1000Base-LX e 1000BASE-ZX não sendo permitida a utilização de conversores externos. 4.3. Possuir 20 portas 10/100/1000BASE-T ativas simultaneamente, com conector RJ-45. 4.4. Possuir porta de console com conector RJ-45 ou DB9 macho. 4.5 O equipamento deve possuir além das portas acima citadas uma porta adicional 10/100 com conector RJ-45 para gerência out-of-band do equipamento. 4.6 Detecção automática MDI/MDIX em todas as portas UTP RJ-45. 4.7. Possuir 2 portas 10GBASE-X ativas simultaneamente, baseadas em XENPAK ou XFP ou X2 ou SFP+, devendo um mesmo slot suportar interfaces 10 Gigabit Ethernet 10GBASE-SR, 10GBASE-LR e 10GBASE-ER. Não é permitida a utilização de conversores externos. 5. Empilhamento: 5.1 Implementar empilhamento de até oito equipamentos e gerência através de um único endereço IP. 5.2 Todas as interfaces Gigabit Ethernet e 10 Gigabit Ethernet, solicitadas nesta especificação, devem funcionar simultaneamente. 5.3 O empilhamento deve possuir arquitetura de anel para prover resiliência. 5.4 O empilhamento deve permitir a criação de grupos de links agregados entre diferentes membros da pilha, segundo 802.3ad. 5.5 O empilhamento deve suportar espelhamento de tráfego entre diferentes unidades da pilha. 5.6. Deve ser possível mesclar em uma mesma pilha equipamentos que implementem PoE. 5.7 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. 5.8. Possuir indicação visual no painel frontal do equipamento que permita identificar a posição lógica do equipamento da pilha 6. Sistema Operacional: 6.1 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. 6.2 O equipamento ofertado deve possuir um sistema operacional modular. 7. Funcionalidades de Camada 3: 7.1 Deve implementar Dual Stack, ou seja, IPV6 e IPv4. 7.2. Implementar roteamento estático com suporte a, no mínimo, 32 rotas. 7.3. Implementar, no mínimo, 256				

		interfaces IP (v4 ou v6). 7.4. Implementar IGMPv1 (RFC 1112), IGMP v2 (RFC 2236), IGMP v3 (RFC 3376). 7.5. Implementar os protocolos de roteamento IP: RFC 1058 – RIP v1 e RFC 2453 – RIP v2. 7.6. Suportar o protocolo de roteamento OSPF v2, incluindo autenticação MD5. 7.7. Implementar PIM Snooping. 7.8. Suportar protocolo de multicast PIM-SM. 7.9 Suportar VRRPv3 (RFC 5798) ou similar. 7.10. Implementar MLD Snooping v1 e v2. 8. Funcionalidades de Camada 2: 8.1 Implementar EAPS (RFC 3619) ou protocolo similar de resiliência em camada 2, específico para topologias em anel, que permita tempo de convergência inferior a 200 ms. 8.2. Implementar 4094 VLANs por porta, ativas simultaneamente. 8.3 Implementar Private VLANs. 8.4. Implementar agregação de links conforme padrão IEEE 802.3ad com suporte a LACP. 8.5. Implementar agregação de links conforme padrão IEEE 802.3ad com, no mínimo, 128 grupos, sendo 8 links agregados por grupo. 8.6 Implementar Spanning-Tree (IEEE 802.1d), Rapid Spanning Tree (IEEE 802.1w), Multiple Instance STP (802.1s) e PVST+. 8.7. 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. 8.8. Implementar funcionalidade vinculada ao Spanning-tree que evite a eleição de outros switches da rede como Root. 8.9. Implementar funcionalidade vinculada ao Spanning-tree que permita desabilitar uma porta de acesso assim que a mesma receba uma BPDU. 9. Gerenciamento/Monitoramento: 9.1 Implementar os seguintes grupos de RMON através da RFC1757: History, Statistics, Alarms e Events. 9.2. Implementar gerenciamento via web com suporte a HTTP e HTTPS/SSL. Esta funcionalidade deve ser implícita ao equipamento. 9.3. 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. 10. Funcionalidades Gerais: 10.1 Implementar sFlow V5 ou Netflow V5, em hardware. Não serão aceitas soluções similares. 10.2 Implementar Port Mirroring e RSPAN (Remote Mirroring). 10.3. Implementar IPv6 em hardware nos módulos de interface. 10.4. Implementar os seguintes protocolos em IPv6: Ping, Traceroute, Telnet, SSH-2. 10.5. Implementar IEEE 802.1ab Link Layer Discovery Protocol (LLDP). 10.6. Implementar LLDP-MED (Media Endpoint Discovery), segundo ANSI/TIA-1057, Draft 08. 10.7. 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. 10.8. Suportar transferência de arquivos através dos protocolos TFTP e SCP. 10.9. Implementar a atualização de imagens de software e configuração através de um servidor TFTP. 10.10. Implementar DHCP/Bootp relay. 10.11. Implementar servidor DHCP interno que permita a configuração de um intervalo de				

		endereços IP a serem atribuídos os clientes DHCP. 10.12. Implementar funcionalidade que permita sua autoconfiguração através dos protocolos DHCP e TFTP, permitindo o provisionamento em massa com o mínimo de intervenção humana. 10.13. Suportar múltiplos servidores Syslog. 10.14. 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. 10.15. Implementar ajuste de clock do equipamento utilizando NTP com autenticação MD5 ou SNTP. 10.16 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. 10.17 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. 10.18 A funcionalidade de Rate Shaping deve permitir a configuração de CIR (Commited Rate) e peak rate. 10.19. Implementar 8 filas de prioridade em hardware por porta. 10.20. Implementar a leitura, classificação e remarcação de QoS (802.1p e DSCP). 10.21. 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. 10.22. 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, 802.1p. 11. Funcionalidades de Politicas & Segurança: 11.1 Implementar 1000 regras de ACL. 11.2 Implementar Policy Based Routing. 11.3. Implementar ACLs de entrada (ingress ACLs) em hardware, baseadas em critérios das camadas 2 (MAC origem e destino) e campo 802.1p, 3 (IP origem e destino) e 4 (portas TCP e UDP), em todas as interfaces e VLANs, com suporte a endereços IPv6. Deverá ser possível aplicar ACLs para tráfego interno de uma determinada VLAN. 11.4. 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. 11.5 Implementar Policy Based Switching, ou seja, possibilitar que o tráfego classificado por uma ACL seja redirecionado para uma porta física específica. 11.6 Implementar Gratuitous ARP Protection. 11.7. 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. 11.8. Implementar limitação de número de endereços MAC aprendidos por uma porta, para uma determinada VLAN. 11.9.				

		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. 11.10. 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. 11.11 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. 11.12. Implementar múltiplos suplicantes por porta, onde cada dispositivo deve ser autenticado de forma independente, podendo ser encaminhados à VLANs distintas. As múltiplas autenticações devem ser realizadas através de IEEE 802.1x. 11.13 Implementar TACACS+ segundo a RFC 1492. Não serão aceitas soluções similares. 11.14. Implementar autenticação RADIUS com suporte a: 11.14.1 RADIUS Authentication; 11.14.2 RADIUS Accounting; 11.14.3 RADIUS EAP support for 802.1X; 11.15 A implementação de RADIUS e TACACS+ deve estar disponível para autenticação de usuários via Telnet e Console serial. 11.16. Implementar RADIUS e TACACS+ per-command authentication. 11.17. Implementar autenticação baseada em web, com suporte a SSL, através de RADIUS ou através da base local do switch. 11.18. Implementar autenticação baseada em endereço MAC, através de RADIUS ou através da base local do switch. 11.19. Implementar funcionalidade que permita que somente servidores DHCP autorizados atribuam configuração IP aos clientes DHCP (Trusted DHCP Server). 12. Certificações: 12.1 Possuir homologação da ANATEL, de acordo com a Resolução número 242. 13. Garantia: 13.1 O Switch de Acesso deverá possuir garantia do fabricante pelo período mínimo de 60 (sessenta) meses. 13.2. Nos casos de troca equipamentos defeituosos, os mesmos devem ser enviados no próximo dia útil subsequente a abertura do chamado e comprovação do defeito, sem quaisquer custos adicionais. 13.3. Os chamados técnicos deverão ser gerenciados pelo fornecedor em horário comercial na modalidade 8x5 (oito horas por dia, cinco dias por semana), através de telefone gratuito. Também deve ser disponibilizado endereço de e-mail para abertura dos chamados técnicos. 13.4 A empresa deverá possuir pelo menos 1 (um) Engenheiro apto a prestar serviços de suporte técnico no equipamento proposto. O Engenheiro deverá possuir registro junto ao CREA e certificação no produto comprovada pelo fabricante. 13.5 O Fabricante deverá disponibilizar gratuitamente suporte e atualização dos softwares, firmwares e sistema operacional para correção de bugs e implementações de segurança; 13.6 Fornecer os softwares e suas atualizações, firmwares, sistema operacional através de meio eletrônico ou magnético sem ônus adicionais. 14. Compatibilidade: 14.1. Os componentes do Switch de Acesso deverão ser homologados pelo fabricante. Não será aceita a adição ou subtração de qualquer				

		componente não original de fábrica para adequação do equipamento; 14.2 Todos os componentes do Switch de Acesso deverão ser compatíveis entre si, com o conjunto do equipamento e com suas funcionalidades, sem a utilização de adaptadores, fresagens, pinturas, usinagens em geral, furações, emprego de adesivos, fitas adesivas ou quaisquer outros procedimentos ou emprego de materiais inadequados ou que visem adaptar forçadamente o equipamento ou suas partes que sejam fisicamente ou logicamente incompatíveis. (Será aceito o regime de OEM desde que comprovado pelo próprio fabricante). 14.3 O Switch de Acesso especificado neste item deve ser totalmente compatível com a Solução de Gerenciamento NetSight Base 500. Referência: Marca Extreme Network, modelo Summit X440-24t-10G ou de melhor qualidade. (TCU, Acórdão 2401/2006, 9.3.2 – Plenário).				
68952	39	Switch de Acesso 24 portas Summit X440-24t: Tipo 4 1. Gabinete/Chassis: 1.1 A solução deve ser composta de um único equipamento, montável em rack 19” devendo este vir acompanhado dos devidos acessórios para tal. 1.2. Possuir leds indicativos de funcionamento da fonte de alimentação, ventiladores e status das portas. 1.3. Possuir altura máxima de 1U (1,75”). 2. Fonte de Alimentação: 2.1 Possuir fonte de alimentação interna que trabalhe em 100V-240V, 50/60 Hz, com detecção automática de tensão e frequência. 2.2. Suportar fonte de alimentação redundante interna ou externa. 3. Performance/Desempenho: 3.1 Possuir, no mínimo, 88 Gbps de Switch Fabric. 3.2. Possuir a capacidade de encaminhamentos de pacotes, de no mínimo 65 Mpps utilizando pacotes de 64 bytes. 3.3. Deve armazenar, no mínimo, 16.000 (dezesseis mil) endereços MAC. 3.4. Implementar jumbo frames em todas as portas ofertadas, com suporte a pacotes de até 9216 Bytes. 4. Portas/Interfaces: 4.1 Todas as interfaces ofertadas devem ser non-blocking. 4.2. Possuir, no mínimo, 4 (quatro) interfaces Gigabit Ethernet baseadas mini-GBIC, devendo um mesmo mini-GBIC-Slot suportar interfaces 1000BASE-T SFP, 1000Base-SX, 1000Base-LX e 1000BASE-ZX não sendo permitida a utilização de conversores externos. 4.3. Possuir 20 portas 10/100/1000BASE-T ativas simultaneamente, com conector RJ-45. 4.4. Possuir porta de console com conector RJ-45 ou DB9 macho. 4.5 O equipamento deve possuir além das portas acima citadas uma porta adicional 10/100 com conector RJ-45 para gerência out-of-band do equipamento. 4.6 Detecção automática MDI/MDIX em todas as portas UTP RJ-45. 4.7 Todas as interfaces Gigabit Ethernet e portas específicas para empilhamento, solicitadas nesta especificação, devem funcionar simultaneamente. 5. Empilhamento: 5.1 Implementar empilhamento de até oito equipamentos e gerência através de um único endereço IP. 5.2 O equipamento deve possuir portas para empilhamento com velocidade de pelo menos 20Gbps cada (ou 10Gbps Full Duplex), totalizando 40 Gbps (ou 20 Gbps full-duplex). 5.3 O empilhamento deve possuir arquitetura de anel para prover resiliência. 5.4 O empilhamento deve permitir a criação de grupos de links agregados entre diferentes	un	1		

		membros da pilha, segundo 802.3ad. 5.5 O empilhamento deve suportar espelhamento de tráfego entre diferentes unidades da pilha. 5.6. Deve ser possível mesclar em uma mesma pilha equipamentos que implementem PoE. 5.7 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. 5.8. Possuir indicação visual no painel frontal do equipamento que permita identificar a posição lógica do equipamento da pilha. 5.9 Todas as interfaces Gigabit Ethernet e portas específicas para empilhamento, solicitadas nesta especificação, devem funcionar simultaneamente. 6. Sistema Operacional: 6.1 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. 6.2 O equipamento ofertado deve possuir um sistema operacional modular. 7. Funcionalidades de Camada 3: 7.1 Deve implementar Dual Stack, ou seja, IPV6 e IPv4. 7.2. Implementar roteamento estático com suporte a, no mínimo, 32 rotas. 7.3. Implementar, no mínimo, 256 interfaces IP (v4 ou v6). 7.4. Implementar IGMPv1 (RFC 1112), IGMP v2 (RFC 2236), IGMP v3 (RFC 3376). 7.5. Implementar os protocolos de roteamento IP: RFC 1058 – RIP v1 e RFC 2453 – RIP v2. 7.6. Suportar o protocolo de roteamento OSPF v2, incluindo autenticação MD5. 7.7. Implementar PIM Snooping. 7.8. Suportar protocolo de multicast PIM-SM. 7.9 Suportar VRRPv3 (RFC 5798) ou similar. 7.10. Implementar MLD Snooping v1 e v2. 8. Funcionalidades de Camada 2: 8.1 Implementar EAPS (RFC 3619) ou protocolo similar de resiliência em camada 2, específico para topologias em anel, que permita tempo de convergência inferior a 200 ms. 8.2. Implementar 4094 VLANs por porta, ativas simultaneamente. 8.3 Implementar Private VLANs. 8.4. Implementar agregação de links conforme padrão IEEE 802.3ad com suporte a LACP. 8.5. Implementar agregação de links conforme padrão IEEE 802.3ad com, no mínimo, 128 grupos, sendo 8 links agregados por grupo. 8.6 Implementar Spanning-Tree (IEEE 802.1d), Rapid Spanning Tree (IEEE 802.1w), Multiple Instance STP (802.1s) e PVST+. 8.7. 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. 8.8. Implementar funcionalidade vinculada ao Spanning-tree que evite a eleição de outros switches da rede como Root. 8.9. Implementar funcionalidade vinculada ao Spanning-tree que permita desabilitar uma porta de acesso assim que a mesma receba uma BPDU. 9. Gerenciamento/Monitoramento: 9.1 Implementar os seguintes grupos de RMON através da RFC1757: History, Statistics, Alarms e Events. 9.2. Implementar gerenciamento via web com suporte a HTTP e HTTPS/SSL. Esta funcionalidade deve ser implícita ao equipamento. 9.3.				

		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. 10. Funcionalidades Gerais: 10.1 Implementar sFlow V5 ou Netflow V5, em hardware. Não serão aceitas soluções similares. 10.2 Implementar Port Mirroring e RSPAN (Remote Mirroring). 10.3. Implementar IPv6 em hardware nos módulos de interface. 10.4. Implementar os seguintes protocolos em IPv6: Ping, Traceroute, Telnet, SSH-2. 10.5. Implementar IEEE 802.1ab Link Layer Discovery Protocol (LLDP). 10.6. Implementar LLDP-MED (Media Endpoint Discovery), segundo ANSI/TIA-1057, Draft 08. 10.7. 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. 10.8. Suportar transferência de arquivos através dos protocolos TFTP e SCP. 10.9. Implementar a atualização de imagens de software e configuração através de um servidor TFTP. 10.10. Implementar DHCP/Bootp relay. 10.11. Implementar servidor DHCP interno que permita a configuração de um intervalo de endereços IP a serem atribuídos os clientes DHCP. 10.12. Implementar funcionalidade que permita sua autoconfiguração através dos protocolos DHCP e TFTP, permitindo o provisionamento em massa com o mínimo de intervenção humana. 10.13. Suportar múltiplos servidores Syslog. 10.14. 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. 10.15. Implementar ajuste de clock do equipamento utilizando NTP com autenticação MD5 ou SNTP. 10.16 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. 10.17 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. 10.18 A funcionalidade de Rate Shaping deve permitir a configuração de CIR (Commited Rate) e peak rate. 10.19. Implementar 8 filas de prioridade em hardware por porta. 10.20. Implementar a leitura, classificação e remarcação de QoS (802.1p e DSCP). 10.21. 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. 10.22. 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, 802.1p. 11. Funcionalidades de Politicas & Segurança: 11.1 Implementar 1000 regras de ACL. 11.2 Implementar Policy Based Routing. 11.3. Implementar ACLs de entrada (ingress ACLs) em hardware, baseadas em critérios das camadas 2 (MAC origem e destino) e campo 802.1p, 3 (IP origem e destino) e 4 (portas TCP e UDP), em todas as interfaces e VLANs, com suporte a endereços IPv6. Deverá ser possível aplicar ACLs para tráfego interno de uma determinada VLAN. 11.4. 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. 11.5 Implementar Policy Based Switching, ou seja, possibilitar que o tráfego classificado por uma ACL seja redirecionado para uma porta física específica. 11.6 Implementar Gratuitous ARP Protection. 11.7. 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. 11.8. Implementar limitação de número de endereços MAC aprendidos por uma porta, para uma determinada VLAN. 11.9. 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. 11.10. 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. 11.11 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. 11.12. Implementar múltiplos suplicantes por porta, onde cada dispositivo deve ser autenticado de forma independente, podendo ser encaminhados à VLANs distintas. As múltiplas autenticações devem ser realizadas através de IEEE 802.1x. 11.13 Implementar TACACS+ segundo a RFC 1492. Não serão aceitas soluções similares. 11.14. Implementar autenticação RADIUS com suporte a: 11.14.1 RADIUS Authentication; 11.14.2 RADIUS Accounting; 11.14.3 RADIUS EAP support for 802.1X; 11.15 A implementação de RADIUS e TACACS+ deve estar disponível para autenticação de usuários via Telnet e Console serial. 11.16. Implementar RADIUS e TACACS+ per-command authentication. 11.17. Implementar autenticação baseada em web, com suporte a SSL, através de RADIUS ou através da base local do switch. 11.18. Implementar autenticação baseada em endereço MAC, através de RADIUS ou através da base local do switch. 11.19. Implementar funcionalidade que permita que somente servidores DHCP autorizados atribuam configuração IP aos clientes DHCP (Trusted DHCP Server). 12. Certificações: 12.1 Possuir homologação da ANATEL, de acordo com a Resolução número 242. 13. Garantia: 13.1 O Switch de Acesso deverá possuir garantia do fabricante pelo período mínimo de 60 (sessenta) meses.				

		13.2. Nos casos de troca equipamentos defeituosos, os mesmos devem ser enviados no próximo dia útil subsequente a abertura do chamado e comprovação do defeito, sem quaisquer custos adicionais. 13.3. Os chamados técnicos deverão ser gerenciados pelo fornecedor em horário comercial na modalidade 8x5 (oito horas por dia, cinco dias por semana), através de telefone gratuito. Também deve ser disponibilizado endereço de e-mail para abertura dos chamados técnicos. 13.4 A empresa deverá possuir pelo menos 1 (um) Engenheiro apto a prestar serviços de suporte técnico no equipamento proposto. O Engenheiro deverá possuir registro junto ao CREA e certificação no produto comprovada pelo fabricante. 13.5 O Fabricante deverá disponibilizar gratuitamente suporte e atualização dos softwares, firmwares e sistema operacional para correção de bugs e implementações de segurança; 13.6 Fornecer os softwares e suas atualizações, firmwares, sistema operacional através de meio eletrônico ou magnético sem ônus adicionais. 14. Compatibilidade: 14.1. Os componentes do Switch de Acesso deverão ser homologados pelo fabricante. Não será aceita a adição ou subtração de qualquer componente não original de fábrica para adequação do equipamento; 14.2 Todos os componentes do Switch de Acesso deverão ser compatíveis entre si, com o conjunto do equipamento e com suas funcionalidades, sem a utilização de adaptadores, fresagens, pinturas, usinagens em geral, furações, emprego de adesivos, fitas adesivas ou quaisquer outros procedimentos ou emprego de materiais inadequados ou que visem adaptar forçadamente o equipamento ou suas partes que sejam fisicamente ou logicamente incompatíveis. (Será aceito o regime de OEM desde que comprovado pelo próprio fabricante). 14.3 O Switch de Acesso especificado neste item deve ser totalmente compatível com a Solução de Gerenciamento NetSight Base 500. Referência: Marca Extreme Network, modelo Summit X440-24t ou de melhor qualidade. (TCU, Acórdão 2401/2006, 9.3.2 – Plenário).				
68950	40	Switch de Acesso 48 portas Summit X430-48t: Tipo 3 1. Gabinete/Chassis: 1.1 A solução deve ser composta de um único equipamento, montável em rack 19 polegadas devendo este vir acompanhado dos devidos acessórios para tal. 1.2. Possuir leds indicativos de funcionamento da fonte de alimentação, ventiladores e status das portas. 1.3. Possuir altura máxima de 1U (1,75”). 2. Fonte de Alimentação: 2.1 Possuir fonte de alimentação interna que trabalhe em 100V-240V, 50/60 Hz, com detecção automática de tensão e frequência. 3. Performance/Desempenho: 3.1 Possuir, no mínimo, 104 Gbps de Switch Fabric. 3.2. Possuir a capacidade de encaminhamentos de pacotes, de no mínimo 77 Mpps utilizando pacotes de 64 bytes. 3.3. Deve armazenar, no mínimo, 16.000 (dezesseis mil) endereços MAC. 3.4. Implementar jumbo frames em todas as portas ofertadas, com suporte a pacotes de até 9216 Bytes. 4. Portas/Interfaces: 4.1 Todas as interfaces ofertadas devem ser non-blocking. 4.2. Possuir 4 (quatro) interfaces Gigabit Ethernet baseadas mini-GBIC, devendo um mesmo mini-GBIC-Slot suportar	un	1		

		interfaces 1000BASE-T SFP, 1000Base-SX, 1000Base-LX e 1000BASE-ZX não sendo permitida a utilização de conversores externos. 4.3 Todas as interfaces Gigabit Ethernet, solicitadas nesta especificação, devem funcionar perfeitamente. 4.4. Possuir porta de console com conector RJ-45 ou DB9 macho. 4.5. Possuir 48 portas 10/100/1000BASE-T ativas simultaneamente, com conector RJ-45. 4.6 O equipamento deve possuir além das portas acima citadas uma porta adicional 10/100 com conector RJ-45 para gerência out-of-band do equipamento. 4.7 Detecção automática MDI/MDIX em todas as portas UTP RJ-45. 5. Sistema Operacional: 5.1 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. 6. Funcionalidades de Camada 2: 6.1 Implementar EAPS (RFC 3619) ou protocolo similar de resiliência em camada 2, específico para topologias em anel, que permita tempo de convergência inferior a 200 ms. 6.2. Implementar 4094 VLANs por porta, ativas simultaneamente. 6.3 Implementar Private VLANs. 6.4. Implementar agregação de links conforme padrão IEEE 802.3ad com suporte a LACP. 6.5. Implementar agregação de links conforme padrão IEEE 802.3ad com, no mínimo, 124 grupos, sendo 8 links agregados por grupo. 6.6 Implementar Spanning-Tree (IEEE 802.1d), Rapid Spanning Tree (IEEE 802.1w), Multiple Instance STP (802.1s) e PVST+. 6.7. 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. 6.8 implementar funcionalidade vinculada ao Spanning-tree que evite a eleição de outros switches da rede como Root. 6.9. Implementar funcionalidade vinculada ao Spanning-tree que permita desabilitar uma porta de acesso assim que a mesma receba uma BPDU. 7. Gerenciamento/Monitoramento: 7.1 Implementar os seguintes grupos de RMON através da RFC1757: History, Statistics, Alarms e Events. 7.2. Implementar gerenciamento via web com suporte a HTTP e HTTPS/SSL. Esta funcionalidade deve ser implícita ao equipamento. 7.3. 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. 8. Funcionalidades Gerais: 8.1 Deve implementar Dual Stack, ou seja, IPV6 e IPv4. 8.2. Implementar IGMP v1 e v2 Snooping 8.3 Implementar sFlow V5 ou Netflow V5, em hardware. Não serão aceitas soluções similares. 8.4 Implementar Port Mirroring e RSPAN (Remote Mirroring). 8.5. Implementar IPv6 em hardware. 8.6. Implementar os seguintes protocolos em IPv6: Ping, Traceroute, Telnet, SSH-2. 8.7. Implementar IEEE 802.1ab Link Layer Discovery Protocol (LLDP). 8.8. Implementar LLDP-MED (Media Endpoint Discovery), segundo ANSI/TIA-1057, Draft 08. 8.9.				

		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. 8.10. Suportar transferência de arquivos através dos protocolos TFTP e SCP. 8.11. Implementar a atualização de imagens de software e configuração através de um servidor TFTP. 8.12. Implementar DHCP/Bootp relay. 8.13. Implementar servidor DHCP interno que permita a configuração de um intervalo de endereços IP a serem atribuídos os clientes DHCP. 8.14. Implementar funcionalidade que permita sua autoconfiguração através dos protocolos DHCP e TFTP, permitindo o provisionamento em massa com o mínimo de intervenção humana. 8.15. Suportar múltiplos servidores Syslog. 8.16. 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. 8.17. Implementar ajuste de clock do equipamento utilizando NTP com autenticação MD5 ou SNTP. 8.18 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. 8.19 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. 8.20 A funcionalidade de Rate Shaping deve permitir a configuração de CIR (Commited Rate) e peak rate. 8.21. Implementar 8 filas de prioridade em hardware por porta. 8.22. Implementar a leitura, classificação e remarcação de QoS (802.1p e DSCP). 8.23. 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. 8.24. 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, 802.1p. 9. Funcionalidades de Politicas & Segurança: 9.1 Implementar 1000 regras de ACL. 9.2. Implementar ACLs de entrada (ingress ACLs) em hardware, baseadas em critérios das camadas 2 (MAC origem e destino) e campo 802.1p, 3 (IP origem e destino) e 4 (portas TCP e UDP), em todas as interfaces e VLANs, com suporte a endereços IPv6. Deverá ser possível aplicar ACLs para tráfego interno de uma determinada VLAN. 9.3. 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. 9.4 Implementar Policy Based Switching, ou seja, possibilitar				

		que o tráfego classificado por uma ACL seja redirecionado para uma porta física específica. 9.5. 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. 9.6. Implementar limitação de número de endereços MAC aprendidos por uma porta, para uma determinada VLAN. 9.7. 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. 9.8. 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. 9.9 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. 9.10. Implementar múltiplos suplicantes por porta, onde cada dispositivo deve ser autenticado de forma independente, podendo ser encaminhados à VLANs distintas. As múltiplas autenticações devem ser realizadas através de IEEE 802.1x. 9.11 Implementar TACACS+ segundo a RFC 1492. Não serão aceitas soluções similares. 9.12. Implementar autenticação RADIUS com suporte a: 9.12.1 RADIUS Authentication; 9.12.2 RADIUS Accounting; 9.12.3 RADIUS EAP support for 802.1X . 9.13 A implementação de RADIUS e TACACS+ deve estar disponível para autenticação de usuários via Telnet e Console serial. 9.14. Implementar RADIUS e TACACS+ per-command authentication. 9.15. Implementar autenticação baseada em web, com suporte a SSL, através de RADIUS ou através da base local do switch. 9.16. Implementar autenticação baseada em endereço MAC, através de RADIUS ou através da base local do switch. 9.17. Implementar funcionalidade que permita que somente servidores DHCP autorizados atribuam configuração IP aos clientes DHCP (Trusted DHCP Server). 10. Certificações: 10.1 Possuir homologação da ANATEL, de acordo com a Resolução número 242. 11. Garantia: 11.1 O Switch de Acesso deverá possuir garantia do fabricante pelo período mínimo de 60 (sessenta) meses. 11.2. Nos casos de troca equipamentos defeituosos, os mesmos devem ser enviados no próximo dia útil subsequente a abertura do chamado e comprovação do defeito, sem quaisquer custos adicionais. 11.3. Os chamados técnicos deverão ser gerenciados pelo fornecedor em horário comercial na modalidade 8x5 (oito horas por dia, cinco dias por semana), através de telefone gratuito. Também deve ser disponibilizado endereço de e-mail para abertura dos chamados técnicos. 11.4 A empresa deverá possuir pelo menos 1 (um) Engenheiro apto a prestar serviços de suporte técnico no equipamento proposto. O Engenheiro deverá possuir registro junto ao CREA e certificação no produto comprovada pelo fabricante. 11.5 O Fabricante deverá disponibilizar gratuitamente suporte e atualização dos				

		softwares, firmwares e sistema operacional para correção de bugs e implementações de segurança; 11.6 Fornecer os softwares e suas atualizações, firmwares, sistema operacional através de meio eletrônico ou magnético sem ônus adicionais. 12. Compatibilidade: 12.1. Os componentes do Switch de Acesso deverão ser homologados pelo fabricante. Não será aceita a adição ou subtração de qualquer componente não original de fábrica para adequação do equipamento; 12.2 Todos os componentes do Switch de Acesso deverão ser compatíveis entre si, com o conjunto do equipamento e com suas funcionalidades, sem a utilização de adaptadores, fresagens, pinturas, usinagens em geral, furações, emprego de adesivos, fitas adesivas ou quaisquer outros procedimentos ou emprego de materiais inadequados ou que visem adaptar forçadamente o equipamento ou suas partes que sejam fisicamente ou logicamente incompatíveis. (Será aceito o regime de OEM desde que comprovado pelo próprio fabricante). 12.3 O Switch de Acesso especificado neste item deve ser totalmente compatível com a Solução de Gerenciamento NetSight Base 500. Referência: Marca Extreme Network, modelo Summit X430-48t ou de melhor qualidade. (TCU, Acórdão 2401/2006, 9.3.2 – Plenário).				
68962	41	Switch de Acesso 48 portas Summit X440-48t-10G: Tipo 8 1. Gabinete/Chassis: 1.1 A solução deve ser composta de um único equipamento, montável em rack 19” devendo este vir acompanhado dos devidos acessórios para tal. 1.2. Possuir leds indicativos de funcionamento da fonte de alimentação, ventiladores e status das portas. 1.3. Possuir altura máxima de 1U (1,75”). 2. Fonte de Alimentação: 2.1 Possuir fonte de alimentação interna que trabalhe em 100V-240V, 50/60 Hz, com detecção automática de tensão e frequência. 2.2. Suportar fonte de alimentação redundante interna ou externa. 3. Performance/Desempenho: 3.1 Possuir, no mínimo, 136 Gbps de Switch Fabric. 3.2. Possuir a capacidade de encaminhamentos de pacotes, de no mínimo 101 Mpps utilizando pacotes de 64 bytes. 3.3. Deve armazenar, no mínimo, 16.000 (dezesseis mil) endereços MAC. 3.4. Implementar jumbo frames em todas as portas ofertadas, com suporte a pacotes de até 9216 Bytes. 4. Portas/Interfaces: 4.1 Todas as interfaces ofertadas devem ser non-blocking. 4.2. Possuir, no mínimo, 4 (quatro) interfaces Gigabit Ethernet baseadas mini-GBIC, devendo um mesmo mini-GBIC-Slot suportar interfaces 1000BASE-T SFP, 1000Base-SX, 1000Base-LX e 1000BASE-ZX não sendo permitida a utilização de conversores externos. 4.3. Possuir 44 portas 10/100/1000BASE-T ativas simultaneamente, com conector RJ-45. 4.4. Possuir porta de console com conector RJ-45 ou DB9 macho. 4.5 O equipamento deve possuir além das portas acima citadas uma porta adicional 10/100 com conector RJ-45 para gerência out-of-band do equipamento. 4.6 Detecção automática MDI/MDIX em todas as portas UTP RJ-45. 4.7. Possuir 2 portas 10GBASE-X ativas simultaneamente, baseadas em XENPAK ou XFP ou X2 ou SFP+, devendo um mesmo slot suportar interfaces 10 Gigabit Ethernet 10GBASE-SR,	un	1		

		10GBASE-LR e 10GBASE-ER. Não é permitida a utilização de conversores externos. 5. Empilhamento: 5.1 Implementar empilhamento de até oito equipamentos e gerência através de um único endereço IP. 5.2 Todas as interfaces Gigabit Ethernet e 10 Gigabit Ethernet, solicitadas nesta especificação, devem funcionar simultaneamente. 5.3 O empilhamento deve possuir arquitetura de anel para prover resiliência. 5.4 O empilhamento deve permitir a criação de grupos de links agregados entre diferentes membros da pilha, segundo 802.3ad. 5.5 O empilhamento deve suportar espelhamento de tráfego entre diferentes unidades da pilha. 5.6. Deve ser possível mesclar em uma mesma pilha equipamentos que implementem PoE. 5.7 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. 5.8. Possuir indicação visual no painel frontal do equipamento que permita identificar a posição lógica do equipamento da pilha. 6. Sistema Operacional: 6.1 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. 6.2 O equipamento ofertado deve possuir um sistema operacional modular. 7. Funcionalidades de Camada 3: 7.1 Deve implementar Dual Stack, ou seja, IPV6 e IPv4. 7.2. Implementar roteamento estático com suporte a, no mínimo, 32 rotas. 7.3. Implementar, no mínimo, 256 interfaces IP (v4 ou v6). 7.4. Implementar IGMPv1 (RFC 1112), IGMP v2 (RFC 2236), IGMP v3 (RFC 3376). 7.5. Implementar os protocolos de roteamento IP: RFC 1058 – RIP v1 e RFC 2453 – RIP v2. 7.6. Suportar o protocolo de roteamento OSPF v2, incluindo autenticação MD5. 7.7. Implementar PIM Snooping. 7.8. Suportar protocolo de multicast PIM-SM. 7.9 Suportar VRRPv3 (RFC 5798) ou similar. 7.10. Implementar MLD Snooping v1 e v2. 8. Funcionalidades de Camada 2: 8.1 Implementar EAPS (RFC 3619) ou protocolo similar de resiliência em camada 2, específico para topologias em anel, que permita tempo de convergência inferior a 200 ms. 8.2. Implementar 4094 VLANs por porta, ativas simultaneamente. 8.3 Implementar Private VLANs. 8.4. Implementar agregação de links conforme padrão IEEE 802.3ad com suporte a LACP. 8.5. Implementar agregação de links conforme padrão IEEE 802.3ad com, no mínimo, 128 grupos, sendo 8 links agregados por grupo. 8.6 Implementar Spanning-Tree (IEEE 802.1d), Rapid Spanning Tree (IEEE 802.1w), Multiple Instance STP (802.1s) e PVST+. 8.7. 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. 8.8. Implementar funcionalidade vinculada ao Spanning-tree que evite a eleição de outros switches da rede como Root. 8.9. Implementar funcionalidade vinculada ao Spanning-tree que				

		permita desabilitar uma porta de acesso assim que a mesma receba uma BPDU. 9. Gerenciamento/Monitoramento: 9.1 Implementar os seguintes grupos de RMON através da RFC1757: History, Statistics, Alarms e Events. 9.2. Implementar gerenciamento via web com suporte a HTTP e HTTPS/SSL. Esta funcionalidade deve ser implícita ao equipamento. 9.3. 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. 10. Funcionalidades Gerais: 10.1 Implementar sFlow V5 ou Netflow V5, em hardware. Não serão aceitas soluções similares. 10.2 Implementar Port Mirroring e RSPAN (Remote Mirroring). 10.3. Implementar IPv6 em hardware nos módulos de interface. 10.4. Implementar os seguintes protocolos em IPv6: Ping, Traceroute, Telnet, SSH-2. 10.5. Implementar IEEE 802.1ab Link Layer Discovery Protocol (LLDP). 10.6. Implementar LLDP-MED (Media Endpoint Discovery), segundo ANSI/TIA-1057, Draft 08. 10.7. 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. 10.8. Suportar transferência de arquivos através dos protocolos TFTP e SCP. 10.9. Implementar a atualização de imagens de software e configuração através de um servidor TFTP. 10.10. Implementar DHCP/Bootp relay. 10.11. Implementar servidor DHCP interno que permita a configuração de um intervalo de endereços IP a serem atribuídos os clientes DHCP. 10.12. Implementar funcionalidade que permita sua autoconfiguração através dos protocolos DHCP e TFTP, permitindo o provisionamento em massa com o mínimo de intervenção humana. 10.13. Suportar múltiplos servidores Syslog. 10.14. 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. 10.15. Implementar ajuste de clock do equipamento utilizando NTP com autenticação MD5 ou SNTP. 10.16 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. 10.17 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. 10.18 A funcionalidade de Rate Shaping deve permitir a configuração de CIR (Commited Rate) e peak rate. 10.19. Implementar 8 filas de prioridade em hardware por porta. 10.20. Implementar a leitura,				

		classificação e remarcação de QoS (802.1p e DSCP). 10.21. 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. 10.22. 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, 802.1p. 11. Funcionalidades de Politicas & Segurança: 11.1 Implementar 1000 regras de ACL. 11.2 Implementar Policy Based Routing. 11.3. Implementar ACLs de entrada (ingress ACLs) em hardware, baseadas em critérios das camadas 2 (MAC origem e destino) e campo 802.1p, 3 (IP origem e destino) e 4 (portas TCP e UDP), em todas as interfaces e VLANs, com suporte a endereços IPv6. Deverá ser possível aplicar ACLs para tráfego interno de uma determinada VLAN. 11.4. 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. 11.5 Implementar Policy Based Switching, ou seja, possibilitar que o tráfego classificado por uma ACL seja redirecionado para uma porta física específica. 11.6 Implementar Gratuitous ARP Protection. 11.7. 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. 11.8. Implementar limitação de número de endereços MAC aprendidos por uma porta, para uma determinada VLAN. 11.9. 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. 11.10. 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. 11.11 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. 11.12. Implementar múltiplos suplicantes por porta, onde cada dispositivo deve ser autenticado de forma independente, podendo ser encaminhados à VLANs distintas. As múltiplas autenticações devem ser realizadas através de IEEE 802.1x. 11.13 Implementar TACACS+ segundo a RFC 1492. Não serão aceitas soluções similares. 11.14. Implementar autenticação RADIUS com suporte a: 11.14.1 RADIUS Authentication; 11.14.2 RADIUS Accounting; 11.14.3 RADIUS EAP support for 802.1X; 11.15 A implementação de RADIUS e TACACS+ deve estar disponível para autenticação de usuários via Telnet e Console serial. 11.16. Implementar RADIUS e TACACS+ per-command authentication. 11.17. Implementar autenticação baseada em web, com suporte a SSL, através de RADIUS ou através da base local do switch. 11.18. Implementar autenticação baseada em endereço MAC, através de RADIUS ou através da				

		base local do switch. 11.19. Implementar funcionalidade que permita que somente servidores DHCP autorizados atribuam configuração IP aos clientes DHCP (Trusted DHCP Server). 12. Certificações: 12.1 Possuir homologação da ANATEL, de acordo com a Resolução número 242. 13. Garantia: 13.1 O Switch de Acesso deverá possuir garantia do fabricante pelo período mínimo de 60 (sessenta) meses. 13.2. Nos casos de troca equipamentos defeituosos, os mesmos devem ser enviados no próximo dia útil subsequente a abertura do chamado e comprovação do defeito, sem quaisquer custos adicionais. 13.3. Os chamados técnicos deverão ser gerenciados pelo fornecedor em horário comercial na modalidade 8x5 (oito horas por dia, cinco dias por semana), através de telefone gratuito. Também deve ser disponibilizado endereço de e-mail para abertura dos chamados técnicos. 13.4 A empresa deverá possuir pelo menos 1 (um) Engenheiro apto a prestar serviços de suporte técnico no equipamento proposto. O Engenheiro deverá possuir registro junto ao CREA e certificação no produto comprovada pelo fabricante. 13.5 O Fabricante deverá disponibilizar gratuitamente suporte e atualização dos softwares, firmwares e sistema operacional para correção de bugs e implementações de segurança; 13.6 Fornecer os softwares e suas atualizações, firmwares, sistema operacional através de meio eletrônico ou magnético sem ônus adicionais. 14. Compatibilidade: 14.1. Os componentes do Switch de Acesso deverão ser homologados pelo fabricante. Não será aceita a adição ou subtração de qualquer componente não original de fábrica para adequação do equipamento; 14.2 Todos os componentes do Switch de Acesso deverão ser compatíveis entre si, com o conjunto do equipamento e com suas funcionalidades, sem a utilização de adaptadores, fresagens, pinturas, usinagens em geral, furações, emprego de adesivos, fitas adesivas ou quaisquer outros procedimentos ou emprego de materiais inadequados ou que visem adaptar forçadamente o equipamento ou suas partes que sejam fisicamente ou logicamente incompatíveis. (Será aceito o regime de OEM desde que comprovado pelo próprio fabricante). 14.3 O Switch de Acesso especificado neste item deve ser totalmente compatível com a Solução de Gerenciamento NetSight Base 500. Referência: Marca Extreme Network, modelo Summit X440-48t-10G ou de melhor qualidade. (TCU, Acórdão 2401/2006, 9.3.2 – Plenário).				
68960	42	Switch de Acesso 48 portas Summit X440-48t: Tipo 6 1. Gabinete/Chassis: 1.1 A solução deve ser composta de um único equipamento, montável em rack 19” devendo este vir acompanhado dos devidos acessórios para tal. 1.2. Possuir leds indicativos de funcionamento da fonte de alimentação, ventiladores e status das portas. 1.3. Possuir altura máxima de 1U (1,75”). 2. Fonte de Alimentação: 2.1 Possuir fonte de alimentação interna que trabalhe em 100V-240V, 50/60 Hz, com detecção automática de tensão e frequência. 2.2. Suportar fonte de alimentação redundante interna ou externa. 3. Performance/Desempenho: 3.1 Possuir, no mínimo, 136 Gbps de Switch Fabric. 3.2. Possuir a	un	1		

		capacidade de encaminhamentos de pacotes, de no mínimo 101 Mpps utilizando pacotes de 64 bytes. 3.3. Deve armazenar, no mínimo, 16.000 (dezesseis mil) endereços MAC. 3.4. Implementar jumbo frames em todas as portas ofertadas, com suporte a pacotes de até 9216 Bytes. 4. Portas/Interfaces: 4.1 Todas as interfaces ofertadas devem ser non-blocking. 4.2. Possuir, no mínimo, 4 (quatro) interfaces Gigabit Ethernet baseadas mini-GBIC, devendo um mesmo mini-GBIC-Slot suportar interfaces 1000BASE-T SFP, 1000Base-SX, 1000Base-LX e 1000BASE-ZX não sendo permitida a utilização de conversores externos. 4.3. Possuir 44 portas 10/100/1000BASE-T ativas simultaneamente, com conector RJ-45. 4.4. Possuir porta de console com conector RJ-45 ou DB9 macho. 4.5 O equipamento deve possuir além das portas acima citadas uma porta adicional 10/100 com conector RJ-45 para gerência out-of-band do equipamento. 4.6 Detecção automática MDI/MDIX em todas as portas UTP RJ-45. 5. Empilhamento: 5.1 Implementar empilhamento de até oito equipamentos e gerência através de um único endereço IP. 5.2 O equipamento deve possuir portas para empilhamento com velocidade de pelo menos 20Gbps cada (ou 10Gbps Full Duplex), totalizando 40 Gbps (ou 20 Gbps full-duplex). 5.3 O empilhamento deve possuir arquitetura de anel para prover resiliência. 5.4 O empilhamento deve permitir a criação de grupos de links agregados entre diferentes membros da pilha, segundo 802.3ad. 5.5 O empilhamento deve suportar espelhamento de tráfego entre diferentes unidades da pilha. 5.6. Deve ser possível mesclar em uma mesma pilha equipamentos que implementem PoE. 5.7 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. 5.8. Possuir indicação visual no painel frontal do equipamento que permita identificar a posição lógica do equipamento da pilha. 5.9 Todas as interfaces Gigabit Ethernet e portas específicas para empilhamento, solicitadas nesta especificação, devem funcionar simultaneamente. 6. Sistema Operacional: 6.1 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. 6.2 O equipamento ofertado deve possuir um sistema operacional modular. 7. Funcionalidades de Camada 3: 7.1 Deve implementar Dual Stack, ou seja, IPV6 e IPv4. 7.2. Implementar roteamento estático com suporte a, no mínimo, 32 rotas. 7.3. Implementar, no mínimo, 256 interfaces IP (v4 ou v6). 7.4. Implementar IGMPv1 (RFC 1112), IGMP v2 (RFC 2236), IGMP v3 (RFC 3376). 7.5. Implementar os protocolos de roteamento IP: RFC 1058 – RIP v1 e RFC 2453 – RIP v2. 7.6. Suportar o protocolo de roteamento OSPF v2, incluindo autenticação MD5. 7.7. Implementar PIM Snooping. 7.8. Suportar protocolo de multicast PIM-SM. 7.9 Suportar VRRPv3 (RFC 5798) ou similar. 7.10. Implementar MLD Snooping v1 e v2. 8. Funcionalidades de Camada 2: 8.1 Implementar EAPS (RFC 3619) ou protocolo similar de resiliência				

		em camada 2, específico para topologias em anel, que permita tempo de convergência inferior a 200 ms. 8.2. Implementar 4094 VLANs por porta, ativas simultaneamente. 8.3 Implementar Private VLANs. 8.4. Implementar agregação de links conforme padrão IEEE 802.3ad com suporte a LACP. 8.5. Implementar agregação de links conforme padrão IEEE 802.3ad com, no mínimo, 128 grupos, sendo 8 links agregados por grupo. 8.6 Implementar Spanning-Tree (IEEE 802.1d), Rapid Spanning Tree (IEEE 802.1w), Multiple Instance STP (802.1s) e PVST+. 8.7. 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. 8.8. Implementar funcionalidade vinculada ao Spanning-tree que evite a eleição de outros switches da rede como Root. 8.9. Implementar funcionalidade vinculada ao Spanning-tree que permita desabilitar uma porta de acesso assim que a mesma receba uma BPDU. 9. Gerenciamento/Monitoramento: 9.1 Implementar os seguintes grupos de RMON através da RFC1757: History, Statistics, Alarms e Events. 9.2. Implementar gerenciamento via web com suporte a HTTP e HTTPS/SSL. Esta funcionalidade deve ser implícita ao equipamento. 9.3. 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. 10. Funcionalidades Gerais: 10.1 Implementar sFlow V5 ou Netflow V5, em hardware. Não serão aceitas soluções similares. 10.2 Implementar Port Mirroring e RSPAN (Remote Mirroring). 10.3. Implementar IPv6 em hardware nos módulos de interface. 10.4. Implementar os seguintes protocolos em IPv6: Ping, Traceroute, Telnet, SSH-2. 10.5. Implementar IEEE 802.1ab Link Layer Discovery Protocol (LLDP). 10.6. Implementar LLDP-MED (Media Endpoint Discovery), segundo ANSI/TIA-1057, Draft 08. 10.7. 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. 10.8. Suportar transferência de arquivos através dos protocolos TFTP e SCP. 10.9. Implementar a atualização de imagens de software e configuração através de um servidor TFTP. 10.10. Implementar DHCP/Bootp relay. 10.11. Implementar servidor DHCP interno que permita a configuração de um intervalo de endereços IP a serem atribuídos os clientes DHCP. 10.12. Implementar funcionalidade que permita sua autoconfiguração através dos protocolos DHCP e TFTP, permitindo o provisionamento em massa com o mínimo de intervenção humana. 10.13. Suportar múltiplos servidores Syslog. 10.14. 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. 10.15. Implementar ajuste de clock do equipamento utilizando NTP com autenticação MD5 ou				

		SNTP. 10.16 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. 10.17 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. 10.18 A funcionalidade de Rate Shaping deve permitir a configuração de CIR (Commited Rate) e peak rate. 10.19. Implementar 8 filas de prioridade em hardware por porta. 10.20. Implementar a leitura, classificação e remarcação de QoS (802.1p e DSCP). 10.21. 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. 10.22. 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, 802.1p. 11. Funcionalidades de Politicas & Segurança: 11.1 Implementar 1000 regras de ACL. 11.2 Implementar Policy Based Routing. 11.3. Implementar ACLs de entrada (ingress ACLs) em hardware, baseadas em critérios das camadas 2 (MAC origem e destino) e campo 802.1p, 3 (IP origem e destino) e 4 (portas TCP e UDP), em todas as interfaces e VLANs, com suporte a endereços IPv6. Deverá ser possível aplicar ACLs para tráfego interno de uma determinada VLAN. 11.4. 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. 11.5 Implementar Policy Based Switching, ou seja, possibilitar que o tráfego classificado por uma ACL seja redirecionado para uma porta física específica. 11.6 Implementar Gratuitous ARP Protection. 11.7. 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. 11.8. Implementar limitação de número de endereços MAC aprendidos por uma porta, para uma determinada VLAN. 11.9. 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. 11.10. 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. 11.11 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. 11.12. Implementar múltiplos suplicantes por porta, onde cada dispositivo deve ser autenticado de forma independente, podendo ser encaminhados à VLANs distintas. As múltiplas autenticações devem ser realizadas através de IEEE 802.1x. 11.13 Implementar TACACS+ segundo a RFC 1492. Não serão aceitas soluções similares. 11.14. Implementar autenticação RADIUS com suporte a: 11.14.1 RADIUS Authentication; 11.14.2 RADIUS Accounting; 11.14.3 RADIUS EAP support for 802.1X; 11.15 A implementação de RADIUS e TACACS+ deve estar disponível para autenticação de usuários via Telnet e Console serial. 11.16. Implementar RADIUS e TACACS+ per-command authentication. 11.17. Implementar autenticação baseada em web, com suporte a SSL, através de RADIUS ou através da base local do switch. 11.18. Implementar autenticação baseada em endereço MAC, através de RADIUS ou através da base local do switch. 11.19. Implementar funcionalidade que permita que somente servidores DHCP autorizados atribuam configuração IP aos clientes DHCP (Trusted DHCP Server). 12. Certificações: 12.1 Possuir homologação da ANATEL, de acordo com a Resolução número 242. 13. Garantia: 13.1 O Switch de Acesso deverá possuir garantia do fabricante pelo período mínimo de 60 (sessenta) meses. 13.2. Nos casos de troca equipamentos defeituosos, os mesmos devem ser enviados no próximo dia útil subsequente a abertura do chamado e comprovação do defeito, sem quaisquer custos adicionais. 13.3. Os chamados técnicos deverão ser gerenciados pelo fornecedor em horário comercial na modalidade 8x5 (oito horas por dia, cinco dias por semana), através de telefone gratuito. Também deve ser disponibilizado endereço de e-mail para abertura dos chamados técnicos. 13.4 A empresa deverá possuir pelo menos 1 (um) Engenheiro apto a prestar serviços de suporte técnico no equipamento proposto. O Engenheiro deverá possuir registro junto ao CREA e certificação no produto comprovada pelo fabricante. 13.5 O Fabricante deverá disponibilizar gratuitamente suporte e atualização dos softwares, firmwares e sistema operacional para correção de bugs e implementações de segurança; 13.6 Fornecer os softwares e suas atualizações, firmwares, sistema operacional através de meio eletrônico ou magnético sem ônus adicionais. 14. Compatibilidade: 14.1. Os componentes do Switch de Acesso deverão ser homologados pelo fabricante. Não será aceita a adição ou subtração de qualquer componente não original de fábrica para adequação do equipamento; 14.2 Todos os componentes do Switch de Acesso deverão ser compatíveis entre si, com o conjunto do equipamento e com suas funcionalidades, sem a utilização de adaptadores, fresagens, pinturas, usinagens em geral, furações, emprego de adesivos, fitas adesivas ou quaisquer outros procedimentos ou emprego de materiais inadequados ou que visem adaptar forçadamente o equipamento ou suas partes que sejam fisicamente ou logicamente incompatíveis. (Será aceito o regime de OEM desde que				

		comprovado pelo próprio fabricante). 14.3 O Switch de Acesso especificado neste item deve ser totalmente compatível com a Solução de Gerenciamento NetSight Base 500. Referência: Marca Extreme Network, modelo Summit X440-48t ou de melhor qualidade. (TCU, Acórdão 2401/2006, 9.3.2 – Plenário).				
68969	43	Switch Distribuição 24 portas X460-G2-24x-10GE4-Base-Unit: Tipo 1 1. Gabinete/Chassis: 1.1 A solução deve ser composta de um único equipamento, montável em rack 19 polegadas devendo este vir acompanhado dos devidos acessórios para tal. 1.2 Possuir ventilação “front-to-back”, ou seja, a saída de ar quente deve acontecer pela traseira do equipamento. 1.3. Possuir bandeja de ventiladores substituível em campo (field replaceable). 1.4. Possuir leds indicativos de funcionamento da fonte de alimentação, ventiladores e status das portas. 2. Fonte de Alimentação: 2.1 Possuir fonte de alimentação interna que trabalhe em 100V-240V, 50/60 Hz, com detecção automática de tensão e frequência, hot-swappable. 2.2. Possuir fonte de alimentação AC redundante interna, hot-swappable. 2.3. Suportar fonte de alimentação DC interna 2.4 Possibilitar que o equipamento funcione com uma fonte AC e uma fonte DC instaladas simultaneamente. 3. Performance/Desempenho: 3.1 Possuir capacidade agregada de switching de, no mínimo, 296 Gbps. 3.2. Possuir a capacidade de encaminhamentos de pacotes, de no mínimo 220 Mpps utilizando pacotes de 64 bytes. 3.3. Deve suportar o armazenamento de até 96.000 (noventa e seis mil) endereços MAC. 3.4. Implementar jumbo frames em todas as portas ofertadas, com suporte a pacotes de até 9216 Bytes. 4. Portas/Interfaces: 4.1 Implementar interfaces Gigabit Ethernet (IEEE 802.3z, 1000BASE-X) e 10 Gigabit Ethernet (IEEE 802.3ae 10GBASE-X). 4.2. Possuir 20 portas 100/1000BASE-X, baseadas em mini-GBIC, devendo um mesmo miniGBIC-Slot suportar interfaces 100BASE-FX, 1000Base-SX, 1000Base-LX (10KM) e ZX (70Km), não sendo permitida a utilização de conversores externos. 4.3. Possuir 8 portas 10/100/1000BASE-T com conector RJ-45. 4.4. Possuir 4 portas 10GBASE-X ativas simultaneamente, baseadas em SFP+, devendo um mesmo slot suportar interfaces 10 Gigabit Ethernet 10GBASE-SR, 10GBASE-LR, 10GBASE-CR (Twinax). Essas interfaces deverão suportar a utilização de mini-GBICs (SFPs) Gigabit Ethernet 1000Base-SX e 1000Base-LX (10KM). Não é permitida a utilização de conversores externos; 4.5 Suportar no mínimo 2 portas 10GBASE-X, adicionais as portas solicitadas anteriormente, baseadas em SFP+, devendo um mesmo slot suportar interfaces 10 Gigabit Ethernet 10GBASE-SR, 10GBASE-LR, 10GBASE-ER e 10GBASE-ZR. Não é permitida a utilização de conversores externos. 4.6. Suportar no mínimo 2 portas 40GBASE-X, adicionais as portas solicitadas anteriormente, baseadas em QSFP+, devendo um mesmo slot suportar interfaces 40 Gigabit Ethernet 40GBASE-SR4 e 40GBASE-LR4, não sendo permitida a utilização de conversores externos. 4.7. Deve suportar o uso simultâneo de todas as portas Gigabit	un	1		

		ethernet solicitadas neste edital, em conjunto com 6 portas 10 Gigabit Ethernet ou 4 portas 10 Gigabit Ethernet e 2 portas 40 Gigabit Ethernet. 4.8. Possuir porta de console com conector RJ-45 ou DB9 macho. 4.9 O equipamento deve possuir além das portas acima citadas uma porta adicional 10/100 com conector RJ-45 para gerência out-of-band do equipamento. 5. Empilhamento: 5.1 Suportar empilhamento de até oito equipamentos e gerência através de um único endereço IP. 5.2. Deve suportar empilhamento através de portas 10 Gigabit Ethernet e 40 Gigabit Ethernet padrão, permitindo o empilhamento de equipamentos que estejam em locais distintos com no mínimo 10 km, conectados através de fibra óptica; 5.3 O empilhamento deve suportar arquitetura de anel para prover resiliência. 5.4 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. 5.5 O empilhamento deve permitir a criação de grupos de links agregados entre diferentes membros da pilha, segundo 802.3ad. Caso seja ofertado um equipamento do tipo chassi modular, deve permitir a criação de grupos de links agregados entre diferentes módulos do chassi, segundo 802.3ad. 5.6 O empilhamento deve suportar espelhamento de tráfego entre diferentes unidades da pilha. 5.7. Deve ser possível mesclar em uma mesma pilha equipamentos que possuam portas de acesso 10/100, equipamentos que implementem PoE e equipamentos que adicionem no mínimo 48 portas 10G. 6. Sistema Operacional: 6.1 O equipamento ofertado deve possuir um sistema operacional modular. 6.2 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. 7. Funcionalidades de Camada 3: 7.1 Deve suportar o armazenamento de até 12.000 (doze mil) rotas IPv4. 7.2. Deve suportar o armazenamento de até 6.000 (seis mil) rotas IPv6. 7.3. Deve implementar Dual Stack, ou seja, IPV6 e IPv4. 7.4. Implementar roteamento estático com suporte a, no mínimo, 1000 rotas. 7.5. Implementar, no mínimo, 2048 interfaces IP (v4 ou v6). 7.6. Implementar IGMPv1 (RFC 1112), IGMP v2 (RFC 2236), IGMP v3 (RFC 3376). 7.7. Implementar os protocolos de roteamento IP: RFC 1058 – RIP v1 e RFC 2453 – RIP v2. 7.8. Suportar o protocolo de roteamento OSPF v2, incluindo autenticação MD5. 7.9 A implementação de OSPF e rotas estáticas deve incluir ECMP (Equal Cost Multi Path). 7.10. Suportar OSPF para IPv6 (OSPFv3) RFC 2740 7.11 Implementar PIM Snooping. 7.12. Suportar protocolo de multicast PIM-SM. 7.13 Suportar PIM-DM. 7.14 Suportar PIM-SSM. 7.15. Suportar MSDP (Multicast Source Discovery Protocol). 7.16. Suportar VRRPv3 (RFC 5798) ou similar. 7.17. Suportar BGP incluindo ECMP (Equal Cost Multi Path). 7.18. Suportar BGP v4. 7.19. Implementar MLD Snooping v1 e v2. 8. Funcionalidades de Camada 2: 8.1 Implementar EAPS (RFC 3619) ou protocolo similar de resiliência em camada 2, específico para topologias em anel, que permita tempo de				

		convergência inferior a 200 ms. 8.2. Implementar 4094 VLANs por porta, ativas simultaneamente, através do protocolo 802.1Q. 8.3 Implementar Private VLANs. 8.4. Implementar agregação de links conforme padrão IEEE 802.3ad com suporte a LACP. 8.5. Implementar agregação de links conforme padrão IEEE 802.3ad com, no mínimo, 128 grupos, sendo 32 links agregados por grupo. 8.6. 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 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. 8.7 Implementar Spanning-Tree (IEEE 802.1d), Rapid Spanning Tree (IEEE 802.1w), Multiple Instance STP (802.1s) e PVST+. 8.8. 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. 8.9. Implementar funcionalidade vinculada ao Spanning-tree que evite a eleição de outros switches da rede como Root. 8.10. Implementar funcionalidade vinculada ao Spanning-tree que permita desabilitar uma porta de acesso assim que a mesma receba uma BPDU. 9. Gerenciamento/Monitoramento: 9.1 Implementar os seguintes grupos de RMON através da RFC1757: History, Statistics, Alarms e Events. 9.2. Implementar gerenciamento via web com suporte a HTTP e HTTPS/SSL. Esta funcionalidade deve ser implícita ao equipamento. 9.3. 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. 10. Funcionalidades Gerais: 10.1 O equipamento deve implementar o set de protocolos DCB (Data Center Bridging) com suporte a PFC (Priority Flow Control), ETS (Enhanced Transmission Selection) e DCBx (Data Center Bridging Exchange). 10.2 O equipamento deverá suportar VPLS e H-VPLS de acordo com os seguintes padrões: 10.2.1 RFC 2961 RSVP Refresh Overhead Reduction Extensions. 10.2.2 RFC 3031 Multiprotocol Label Switching Architecture. 10.2.3 RFC 3032 MPLS Label Stack Encoding. 10.2.5 RFC 3209 RSVP-TE: Extensions to RSVP for LSP Tunnels. 10.2.6 RFC 3630 Traffic Engineering Extensions to OSPFv2. 10.2.7 RFC 3811 Definitions of Textual Conventions (TCs) for Multiprotocol Label Switching (MPLS) Management 10.2.8 RFC 3812 Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) Management Information Base (MIB). 10.2.9 RFC 3813 Multiprotocol Label Switching (MPLS) Label Switching Router (LSR) Management Information Base (MIB) 10.2.10 RFC 3815 Definitions of Managed Objects for the				

		Multiprotocol Label Switching (MPLS), Label Distribution Protocol (LDP). 10.2.11 RFC 4090 Fast Re-route Extensions to RSVP-TE for LSP (Detour Paths). 10.2.12 RFC 4379 Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures (LSP Ping). 10.2.13 draft-ietf-bfd-base-09.txt Bidirectional Forwarding Detection. 10.2.14 RFC 4447 Pseudowire Setup and Maintenance using the Label Distribution Protocol (LDP). 10.2.15 RFC 4448 Encapsulation Methods for Transport of Ethernet over MPLS Networks. 10.2.16 RFC 4762 Virtual Private LAN Services (VPLS) using Label Distribution Protocol (LDP) Signaling. 10.2.17 RFC 5085 Pseudowire Virtual Circuit Connectivity Verification (VCCV). 10.2.18 RFC 5542 Definitions of Textual Conventions for Pseudowire (PW) Management. 10.2.19 RFC 5601 Pseudowire (PW) Management Information Base (MIB). 10.2.20 RFC 5602 Pseudowire (PW) over MPLS PSN (MIB). 10.2.21 RFC 5603 Ethernet Pseudowire (PW) MIB. 10.2.22 draft-ietf-l2vpn-vpls-mib-02.txt Virtual Private LAN Services (VPLS) MIB". 10.3 Implementar WRED. 10.4 Implementar IPFIX ou Netflow, em hardware. Não serão aceitas soluções similares. 10.5 Implementar Port Mirroring e RSPAN (Remote Mirroring). 10.6. Implementar IPv6 em hardware nos módulos de interface. 10.7. Implementar os seguintes protocolos em IPv6: Ping, Traceroute, Telnet, SSH-2. 10.8. Implementar IEEE 802.1ab Link Layer Discovery Protocol (LLDP). 10.9. Implementar LLDP-MED (Media Endpoint Discovery), segundo ANSI/TIA-1057, Draft 08. 10.10. 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. 10.11. Suportar transferência de arquivos através dos protocolos TFTP e SCP. 10.12. Implementar a atualização de imagens de software e configuração através de um servidor TFTP. 10.13. Implementar DHCP/Bootp relay. 10.14. Implementar servidor DHCP interno que permita a configuração de um intervalo de endereços IP a serem atribuídos os clientes DHCP. 10.15. Implementar funcionalidade que permita sua autoconfiguração através dos protocolos DHCP e TFTP, permitindo o provisionamento em massa com o mínimo de intervenção humana. 10.16. Suportar múltiplos servidores Syslog. 10.17. 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. 10.18. Implementar ajuste de clock do equipamento utilizando NTP com autenticação MD5 ou SNTP. 10.19 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.				

		10.20 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. 10.21 A funcionalidade de Rate Shaping deve permitir a configuração de CIR (Commited Rate) e peak rate. 10.22. Implementar 8 filas de prioridade em hardware por porta. 10.23. Implementar a leitura, classificação e remarcação de QoS (802.1p e DSCP). 10.24. 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. 10.25. 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, 802.1p. 10.26 Implementar os algoritmos de gerenciamento de filas WRR (Weighted Round Robin) e SP (Strict Priority). 11. Funcionalidades de Politicas & Segurança: 11.1 Implementar regras de ACL de entrada (inbound ACLs) e de saída (outbound ACLs) em hardware. 11.2. Implementar ACLs de entrada (ingress ACLs) em hardware, baseadas em critérios das camadas 2 (MAC origem e destino) e campo 802.1p, 3 (IP origem e destino) e 4 (portas TCP e UDP), em todas as interfaces e VLANs, com suporte a endereços IPv6. Deverá ser possível aplicar ACLs para tráfego interno de uma determinada VLAN. 11.3. 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. 11.4 Implementar Policy Based Routing. 11.5 Implementar Policy Based Switching, ou seja, possibilitar que o tráfego classificado por uma ACL seja redirecionado para uma porta física específica. 11.6 Implementar Gratuitous ARP Protection. 11.7. 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. 11.8. Implementar limitação de número de endereços MAC aprendidos por uma porta, para uma determinada VLAN. 11.9. 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. 11.10. 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. 11.11 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. 11.12. Implementar múltiplos suplicantes por porta, onde cada dispositivo deve ser autenticado de forma independente, podendo ser encaminhados à VLANs distintas. As múltiplas autenticações devem ser realizadas através de IEEE 802.1x. 11.13 Implementar TACACS+				

		segundo a RFC 1492. Não serão aceitas soluções similares. 11.14. Implementar autenticação RADIUS com suporte a: 11.14.1 RADIUS Authentication. 11.14.2 RADIUS Accounting. 11.14.3 RADIUS EAP support for 802.1X. 11.15 A implementação de RADIUS e TACACS+ deve estar disponível para autenticação de usuários via Telnet e Console serial. 11.16. Implementar RADIUS e TACACS+ per-command authentication. 11.17. Implementar autenticação baseada em web, com suporte a SSL, através de RADIUS ou através da base local do switch. 11.18. Implementar autenticação baseada em endereço MAC, através de RADIUS ou através da base local do switch. 11.19. Implementar funcionalidade que permita que somente servidores DHCP autorizados atribuam configuração IP aos clientes DHCP (Trusted DHCP Server). 12. Certificações: 12.1 Possuir homologação da ANATEL, de acordo com a Resolução número 242. 13. Garantia: 13.1 O Switch Distribuição deverá possuir garantia do fabricante pelo período mínimo de 60 (sessenta) meses. 13.2. Nos casos de troca equipamentos defeituosos, os mesmos devem ser enviados no próximo dia útil subsequente a abertura do chamado e comprovação do defeito, sem quaisquer custos adicionais. 13.3. Os chamados técnicos deverão ser gerenciados pelo fornecedor em horário comercial na modalidade 8x5 (oito horas por dia, cinco dias por semana), através de telefone gratuito. Também deve ser disponibilizado endereço de e-mail para abertura dos chamados técnicos. 13.4 A empresa deverá possuir pelo menos 1 (um) Engenheiro apto a prestar serviços de suporte técnico no equipamento proposto. O Engenheiro deverá possuir registro junto ao CREA e certificação no produto comprovada pelo fabricante. 13.5 O Fabricante deverá disponibilizar gratuitamente suporte e atualização dos softwares, firmwares e sistema operacional para correção de bugs e implementações de segurança; 13.6 Fornecer os softwares e suas atualizações, firmwares, sistema operacional através de meio eletrônico ou magnético sem ônus adicionais. 14. Compatibilidade: 14.1. Os componentes do Switch Distribuição deverão ser homologados pelo fabricante. Não será aceita a adição ou subtração de qualquer componente não original de fábrica para adequação do equipamento; 14.2 Todos os componentes do Switch Distribuição deverão ser compatíveis entre si, com o conjunto do equipamento e com suas funcionalidades, sem a utilização de adaptadores, fresagens, pinturas, usinagens em geral, furações, emprego de adesivos, fitas adesivas ou quaisquer outros procedimentos ou emprego de materiais inadequados ou que visem adaptar forçadamente o equipamento ou suas partes que sejam fisicamente ou logicamente incompatíveis. (Será aceito o regime de OEM desde que comprovado pelo próprio fabricante). 14.3 O Switch Distribuição especificado neste item deve ser totalmente compatível com a Solução de Gerenciamento NetSight Base 500. Referência: Marca Extreme Network, modelo X460-G2-24x-10GE4-Base-Unit ou de melhor qualidade. (TCU, Acórdão 2401/2006, 9.3.2 – Plenário).				

68970	44	Switch Distribuição 48 portas (PoE+) X460-G2-48p-10GE4-Base-Unit: Tipo 2 1. Gabinete/Chassis: 1.1 A solução deve ser composta de um único equipamento, montável em rack 19 polegadas devendo este vir acompanhado dos devidos acessórios para tal. 1.2 Possuir ventilação “front-to-back”, ou seja, a saída de ar quente deve acontecer pela traseira do equipamento. 1.3. Possuir bandeja de ventiladores substituível em campo (field replaceable). 1.4. Possuir leds indicativos de funcionamento da fonte de alimentação, ventiladores e status das portas. 2. Fonte de Alimentação: 2.1 Possuir fonte de alimentação interna que trabalhe em 100V-240V, 50/60 Hz, com detecção automática de tensão e frequência, hot-swappable. 2.2. Suportar fonte de alimentação AC redundante interna, hot-swappable. 2.3. Suportar fonte de alimentação DC interna 2.4 Possibilitar que o equipamento funcione com uma fonte AC e uma fonte DC instaladas simultaneamente. 3. Performance/Desempenho: 3.1 Possuir capacidade agregada de switching de, no mínimo, 336 Gbps. 3.2. Possuir a capacidade de encaminhamentos de pacotes, de no mínimo 250 Mpps utilizando pacotes de 64 bytes. 3.3. Deve suportar o armazenamento de até 96.000 (noventa e seis mil) endereços MAC. 3.4. Implementar jumbo frames em todas as portas ofertadas, com suporte a pacotes de até 9216 Bytes. 4. Portas/Interfaces: 4.1 Implementar interfaces Gigabit Ethernet (IEEE 802.3z, 1000BASE-X) e 10 Gigabit Ethernet (IEEE 802.3ae 10GBASE-X). 4.2. Possuir 48 portas 10/100/1000BASE-T com conector RJ-45. 4.3. Possuir 4 portas 10GBASE-X ativas simultaneamente, baseadas em SFP+, devendo um mesmo slot suportar interfaces 10 Gigabit Ethernet 10GBASE-SR, 10GBASE-LR, 10GBASE-CR (Twinax). Essas interfaces deverão suportar a utilização de mini-GBICs (SFPs) Gigabit Ethernet 1000Base-SX e 1000Base-LX (10KM). Não é permitida a utilização de conversores externos; 4.4 Suportar no mínimo 2 portas 10GBASE-X, adicionais as portas solicitadas anteriormente, baseadas em XENPAK ou XFP ou X2 ou SFP+, devendo um mesmo slot suportar interfaces 10 Gigabit Ethernet 10GBASE-SR, 10GBASE-LR, 10GBASE-ER, 10GBASE-ZR e Tunable DWDM. Não é permitida a utilização de conversores externos. 4.5. Suportar no mínimo 2 portas 40GBASE-X, adicionais as portas solicitadas anteriormente, baseadas em QSFP+, devendo um mesmo slot suportar interfaces 40 Gigabit Ethernet 40GBASE-SR4 e 40GBASE-LR4, não sendo permitida a utilização de conversores externos. 4.6. Deve suportar o uso simultâneo de todas as portas Gigabit ethernet solicitadas neste edital, em conjunto com 6 portas 10 Gigabit Ethernet ou 4 portas 10 Gigabit Ethernet e 2 portas 40 Gigabit Ethernet. 4.7. Possuir porta de console com conector RJ-45 ou DB9 macho. 4.8 O equipamento deve possuir além das portas acima citadas uma porta adicional 10/100 com conector RJ-45 para gerência out-of-band do equipamento. 4.9 Implementar Power over Ethernet Plus (PoE-Plus) segundo o padrão IEEE 802.3at em todas as portas 10/100/1000Base-T, com no mínimo 500W de potência disponível para dispositivos PoE através de fonte interna. 4.10. Deve	un	38		

		suportar o padrão IEEE 802.3az (Energy Efficient Ethernet) 5. Empilhamento: 5.1 Suportar empilhamento de até oito equipamentos e gerência através de um único endereço IP. 5.2. Deve suportar empilhamento através de portas 10 Gigabit Ethernet e 40 Gigabit Ethernet padrão, permitindo o empilhamento de equipamentos que estejam em locais distintos com no mínimo 10 km, conectados através de fibra óptica. 5.3 O empilhamento deve suportar arquitetura de anel para prover resiliência. 5.4 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. 5.5 O empilhamento deve permitir a criação de grupos de links agregados entre diferentes membros da pilha, segundo 802.3ad. Caso seja ofertado um equipamento do tipo chassi modular, deve permitir a criação de grupos de links agregados entre diferentes módulos do chassi, segundo 802.3ad. 5.6 O empilhamento deve suportar espelhamento de tráfego entre diferentes unidades da pilha. Caso seja ofertado um equipamento do tipo chassi modular, deve suportar espelhamento de tráfego entre diferentes módulos do chassi. 5.7. Deve ser possível mesclar em uma mesma pilha equipamentos que possuam portas de acesso 10/100, equipamentos que não implementem PoE e equipamentos que adicionem no mínimo 48 portas 10G. 6. Sistema Operacional: 6.1 O equipamento ofertado deve possuir um sistema operacional modular. 6.2 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. 7. Funcionalidades de Camada 3: 7.1 Deve suportar o armazenamento de até 12.000 (doze mil) rotas IPv4. 7.2. Deve suportar o armazenamento de até 6.000 (seis mil) rotas IPv6. 7.3. Deve implementar Dual Stack, ou seja, IPV6 e IPv4. 7.4. Implementar roteamento estático com suporte a, no mínimo, 1000 rotas. 7.5. Implementar, no mínimo, 2048 interfaces IP (v4 ou v6). 7.6. Implementar IGMPv1 (RFC 1112), IGMP v2 (RFC 2236), IGMP v3 (RFC 3376). 7.7. Implementar os protocolos de roteamento IP: RFC 1058 – RIP v1 e RFC 2453 – RIP v2. 7.8. Suportar o protocolo de roteamento OSPF v2, incluindo autenticação MD5. 7.9 A implementação de OSPF e rotas estáticas deve incluir ECMP (Equal Cost Multi Path). 7.10. Suportar OSPF para IPv6 (OSPFv3) RFC 2740 7.11 Implementar PIM Snooping. 7.12. Suportar protocolo de multicast PIM-SM. 7.13 Suportar PIM-DM. 7.14 Suportar PIM-SSM. 7.15. Suportar MSDP (Multicast Source Discovery Protocol). 7.16. Suportar VRRPv3 (RFC 5798) ou similar. 7.17. Suportar BGP incluindo ECMP (Equal Cost Multi Path). 7.18. Suportar BGP v4. 7.19. Implementar MLD Snooping v1 e v2. 8. Funcionalidades de Camada 2: 8.1 Implementar EAPS (RFC 3619) ou protocolo similar de resiliência em camada 2, específico para topologias em anel, que permita tempo de convergência inferior a 200 ms. 8.2. Implementar 4094 VLANs por porta, ativas simultaneamente, através do protocolo 802.1Q. 8.3 Implementar Private VLANs. 8.4. Implementar				

		agregação de links conforme padrão IEEE 802.3ad com suporte a LACP. 8.5. Implementar agregação de links conforme padrão IEEE 802.3ad com, no mínimo, 128 grupos, sendo 32 links agregados por grupo. 8.6. 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 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. 8.7 Implementar Spanning-Tree (IEEE 802.1d), Rapid Spanning Tree (IEEE 802.1w), Multiple Instance STP (802.1s) e PVST+. 8.8. 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. 8.9. Implementar funcionalidade vinculada ao Spanning-tree que evite a eleição de outros switches da rede como Root. 8.10. Implementar funcionalidade vinculada ao Spanning-tree que permita desabilitar uma porta de acesso assim que a mesma receba uma BPDU. 9. Gerenciamento/Monitoramento: 9.1 Implementar os seguintes grupos de RMON através da RFC1757: History, Statistics, Alarms e Events. 9.2. Implementar gerenciamento via web com suporte a HTTP e HTTPS/SSL. Esta funcionalidade deve ser implícita ao equipamento. 9.3. 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. 10. Funcionalidades Gerais: 10.1 O equipamento deve implementar o set de protocolos DCB (Data Center Bridging) com suporte a PFC (Priority Flow Control), ETS (Enhanced Transmission Selection) e DCBx (Data Center Bridging Exchange). 10.2 O equipamento deverá suportar VPLS e H-VPLS de acordo com os seguintes padrões: 10.2.1 RFC 2961 RSVP Refresh Overhead Reduction Extensions. 10.2.2 RFC 3031 Multiprotocol Label Switching Architecture. 10.2.3 RFC 3032 MPLS Label Stack Encoding. 10.2.5 RFC 3209 RSVP-TE: Extensions to RSVP for LSP Tunnels. 10.2.6 RFC 3630 Traffic Engineering Extensions to OSPFv2. 10.2.7 RFC 3811 Definitions of Textual Conventions (TCs) for Multiprotocol Label Switching (MPLS) Management 10.2.8 RFC 3812 Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) Management Information Base (MIB). 10.2.9 RFC 3813 Multiprotocol Label Switching (MPLS) Label Switching Router (LSR) Management Information Base (MIB) 10.2.10 RFC 3815 Definitions of Managed Objects for the Multiprotocol Label Switching (MPLS), Label Distribution Protocol (LDP). 10.2.11 RFC 4090 Fast Re-route Extensions to RSVP-TE for LSP (Detour Paths). 10.2.12 RFC 4379 Detecting Multi-Protocol				

		Label Switched (MPLS) Data Plane Failures (LSP Ping). 10.2.13 draft-ietf-bfd-base-09.txt Bidirectional Forwarding Detection. 10.2.14 RFC 4447 Pseudowire Setup and Maintenance using the Label Distribution Protocol (LDP). 10.2.15 RFC 4448 Encapsulation Methods for Transport of Ethernet over MPLS Networks. 10.2.16 RFC 4762 Virtual Private LAN Services (VPLS) using Label Distribution Protocol (LDP) Signaling. 10.2.17 RFC 5085 Pseudowire Virtual Circuit Connectivity Verification (VCCV). 10.2.18 RFC 5542 Definitions of Textual Conventions for Pseudowire (PW) Management. 10.2.19 RFC 5601 Pseudowire (PW) Management Information Base (MIB). 10.2.20 RFC 5602 Pseudowire (PW) over MPLS PSN (MIB). 10.2.21 RFC 5603 Ethernet Pseudowire (PW) MIB. 10.2.22 draft-ietf-l2vpn-vpls-mib-02.txt Virtual Private LAN Services (VPLS) MIB". 10.3 Implementar WRED. 10.4 Implementar IPFIX ou Netflow, em hardware. Não serão aceitas soluções similares. 10.5 Implementar Port Mirroring e RSPAN (Remote Mirroring). 10.6. Implementar IPv6 em hardware nos módulos de interface. 10.7. Implementar os seguintes protocolos em IPv6: Ping, Traceroute, Telnet, SSH-2. 10.8. Implementar IEEE 802.1ab Link Layer Discovery Protocol (LLDP). 10.9. Implementar LLDP-MED (Media Endpoint Discovery), segundo ANSI/TIA-1057, Draft 08. 10.10. 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. 10.11. Suportar transferência de arquivos através dos protocolos TFTP e SCP. 10.12. Implementar a atualização de imagens de software e configuração através de um servidor TFTP. 10.13. Implementar DHCP/Bootp relay. 10.14. Implementar servidor DHCP interno que permita a configuração de um intervalo de endereços IP a serem atribuídos os clientes DHCP. 10.15. Implementar funcionalidade que permita sua autoconfiguração através dos protocolos DHCP e TFTP, permitindo o provisionamento em massa com o mínimo de intervenção humana. 10.16. Suportar múltiplos servidores Syslog. 10.17. 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. 10.18. Implementar ajuste de clock do equipamento utilizando NTP com autenticação MD5 ou SNTP. 10.19 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. 10.20 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. 10.21 A funcionalidade de Rate Shaping deve permitir a configuração de CIR (Commited Rate) e peak rate. 10.22. Implementar 8 filas de prioridade em hardware por porta. 10.23. Implementar a leitura, classificação e remarcação de QoS (802.1p e DSCP). 10.24. 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. 10.25. 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, 802.1p. 10.26 Implementar os algoritmos de gerenciamento de filas WRR (Weighted Round Robin) e SP (Strict Priority). 11. Funcionalidades de Politicas & Segurança: 11.1 Implementar regras de ACL de entrada (inbound ACLs) e de saída (outbound ACLs) em hardware. 11.2. Implementar ACLs de entrada (ingress ACLs) em hardware, baseadas em critérios das camadas 2 (MAC origem e destino) e campo 802.1p, 3 (IP origem e destino) e 4 (portas TCP e UDP), em todas as interfaces e VLANs, com suporte a endereços IPv6. Deverá ser possível aplicar ACLs para tráfego interno de uma determinada VLAN. 11.3. 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. 11.4 Implementar Policy Based Routing. 11.5 Implementar Policy Based Switching, ou seja, possibilitar que o tráfego classificado por uma ACL seja redirecionado para uma porta física específica. 11.6 Implementar Gratuitous ARP Protection. 11.7. 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. 11.8. Implementar limitação de número de endereços MAC aprendidos por uma porta, para uma determinada VLAN. 11.9. 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. 11.10. 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. 11.11 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. 11.12. Implementar múltiplos suplicantes por porta, onde cada dispositivo deve ser autenticado de forma independente, podendo ser encaminhados à VLANs distintas. As múltiplas autenticações devem ser realizadas através de IEEE 802.1x. 11.13 Implementar TACACS+ segundo a RFC 1492. Não serão aceitas soluções similares. 11.14. Implementar autenticação RADIUS com suporte a: 11.14.1 RADIUS Authentication. 11.14.2 RADIUS Accounting. 11.14.3 RADIUS EAP				

		support for 802.1X. 11.15 A implementação de RADIUS e TACACS+ deve estar disponível para autenticação de usuários via Telnet e Console serial. 11.16. Implementar RADIUS e TACACS+ per-command authentication. 11.17. Implementar autenticação baseada em web, com suporte a SSL, através de RADIUS ou através da base local do switch. 11.18. Implementar autenticação baseada em endereço MAC, através de RADIUS ou através da base local do switch. 11.19. Implementar funcionalidade que permita que somente servidores DHCP autorizados atribuam configuração IP aos clientes DHCP (Trusted DHCP Server). 12. Certificações: 12.1 Possuir homologação da ANATEL, de acordo com a Resolução número 242. 13. Garantia: 13.1 O Switch Distribuição deverá possuir garantia do fabricante pelo período mínimo de 60 (sessenta) meses. 13.2. Nos casos de troca equipamentos defeituosos, os mesmos devem ser enviados no próximo dia útil subsequente a abertura do chamado e comprovação do defeito, sem quaisquer custos adicionais. 13.3. Os chamados técnicos deverão ser gerenciados pelo fornecedor em horário comercial na modalidade 8x5 (oito horas por dia, cinco dias por semana), através de telefone gratuito. Também deve ser disponibilizado endereço de e-mail para abertura dos chamados técnicos. 13.4 A empresa deverá possuir pelo menos 1 (um) Engenheiro apto a prestar serviços de suporte técnico no equipamento proposto. O Engenheiro deverá possuir registro junto ao CREA e certificação no produto comprovada pelo fabricante. 13.5 O Fabricante deverá disponibilizar gratuitamente suporte e atualização dos softwares, firmwares e sistema operacional para correção de bugs e implementações de segurança; 13.6 Fornecer os softwares e suas atualizações, firmwares, sistema operacional através de meio eletrônico ou magnético sem ônus adicionais. 14. Compatibilidade: 14.1. Os componentes do Switch Distribuição deverão ser homologados pelo fabricante. Não será aceita a adição ou subtração de qualquer componente não original de fábrica para adequação do equipamento; 14.2 Todos os componentes do Switch Distribuição deverão ser compatíveis entre si, com o conjunto do equipamento e com suas funcionalidades, sem a utilização de adaptadores, fresagens, pinturas, usinagens em geral, furações, emprego de adesivos, fitas adesivas ou quaisquer outros procedimentos ou emprego de materiais inadequados ou que visem adaptar forçadamente o equipamento ou suas partes que sejam fisicamente ou logicamente incompatíveis. (Será aceito o regime de OEM desde que comprovado pelo próprio fabricante). 14.3 O Switch Distribuição especificado neste item deve ser totalmente compatível com a Solução de Gerenciamento NetSight Base 500. Referência: Marca Extreme Network, modelo X460-G2-48p-10GE4-Base-Unit ou de melhor qualidade. (TCU, Acórdão 2401/2006, 9.3.2 – Plenário). **(COTA PRINCIPAL)**				
68970	45	Switch Distribuição 48 portas (PoE+) X460-G2-48p-10GE4-Base-Unit: Tipo 2 1. Gabinete/Chassis: 1.1 A solução deve ser composta de um único equipamento, montável em rack 19 polegadas devendo este	un	12		

		vir acompanhado dos devidos acessórios para tal. 1.2 Possuir ventilação “front-to-back”, ou seja, a saída de ar quente deve acontecer pela traseira do equipamento. 1.3. Possuir bandeja de ventiladores substituível em campo (field replaceable). 1.4. Possuir leds indicativos de funcionamento da fonte de alimentação, ventiladores e status das portas. 2. Fonte de Alimentação: 2.1 Possuir fonte de alimentação interna que trabalhe em 100V-240V, 50/60 Hz, com detecção automática de tensão e frequência, hot-swappable. 2.2. Suportar fonte de alimentação AC redundante interna, hot-swappable. 2.3. Suportar fonte de alimentação DC interna 2.4 Possibilitar que o equipamento funcione com uma fonte AC e uma fonte DC instaladas simultaneamente. 3. Performance/Desempenho: 3.1 Possuir capacidade agregada de switching de, no mínimo, 336 Gbps. 3.2. Possuir a capacidade de encaminhamentos de pacotes, de no mínimo 250 Mpps utilizando pacotes de 64 bytes. 3.3. Deve suportar o armazenamento de até 96.000 (noventa e seis mil) endereços MAC. 3.4. Implementar jumbo frames em todas as portas ofertadas, com suporte a pacotes de até 9216 Bytes. 4. Portas/Interfaces: 4.1 Implementar interfaces Gigabit Ethernet (IEEE 802.3z, 1000BASE-X) e 10 Gigabit Ethernet (IEEE 802.3ae 10GBASE-X). 4.2. Possuir 48 portas 10/100/1000BASE-T com conector RJ-45. 4.3. Possuir 4 portas 10GBASE-X ativas simultaneamente, baseadas em SFP+, devendo um mesmo slot suportar interfaces 10 Gigabit Ethernet 10GBASE-SR, 10GBASE-LR, 10GBASE-CR (Twinax). Essas interfaces deverão suportar a utilização de mini-GBICs (SFPs) Gigabit Ethernet 1000Base-SX e 1000Base-LX (10KM). Não é permitida a utilização de conversores externos; 4.4 Suportar no mínimo 2 portas 10GBASE-X, adicionais as portas solicitadas anteriormente, baseadas em XENPAK ou XFP ou X2 ou SFP+, devendo um mesmo slot suportar interfaces 10 Gigabit Ethernet 10GBASE-SR, 10GBASE-LR, 10GBASE-ER, 10GBASE-ZR e Tunable DWDM. Não é permitida a utilização de conversores externos. 4.5. Suportar no mínimo 2 portas 40GBASE-X, adicionais as portas solicitadas anteriormente, baseadas em QSFP+, devendo um mesmo slot suportar interfaces 40 Gigabit Ethernet 40GBASE-SR4 e 40GBASE-LR4, não sendo permitida a utilização de conversores externos. 4.6. Deve suportar o uso simultâneo de todas as portas Gigabit ethernet solicitadas neste edital, em conjunto com 6 portas 10 Gigabit Ethernet ou 4 portas 10 Gigabit Ethernet e 2 portas 40 Gigabit Ethernet. 4.7. Possuir porta de console com conector RJ-45 ou DB9 macho. 4.8 O equipamento deve possuir além das portas acima citadas uma porta adicional 10/100 com conector RJ-45 para gerência out-of-band do equipamento. 4.9 Implementar Power over Ethernet Plus (PoE-Plus) segundo o padrão IEEE 802.3at em todas as portas 10/100/1000Base-T, com no mínimo 500W de potência disponível para dispositivos PoE através de fonte interna. 4.10. Deve suportar o padrão IEEE 802.3az (Energy Efficient Ethernet) 5. Empilhamento: 5.1 Suportar empilhamento de até oito equipamentos e gerência através de um único endereço IP. 5.2. Deve suportar				

		empilhamento através de portas 10 Gigabit Ethernet e 40 Gigabit Ethernet padrão, permitindo o empilhamento de equipamentos que estejam em locais distintos com no mínimo 10 km, conectados através de fibra óptica. 5.3 O empilhamento deve suportar arquitetura de anel para prover resiliência. 5.4 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. 5.5 O empilhamento deve permitir a criação de grupos de links agregados entre diferentes membros da pilha, segundo 802.3ad. Caso seja ofertado um equipamento do tipo chassi modular, deve permitir a criação de grupos de links agregados entre diferentes módulos do chassi, segundo 802.3ad. 5.6 O empilhamento deve suportar espelhamento de tráfego entre diferentes unidades da pilha. Caso seja ofertado um equipamento do tipo chassi modular, deve suportar espelhamento de tráfego entre diferentes módulos do chassi. 5.7. Deve ser possível mesclar em uma mesma pilha equipamentos que possuam portas de acesso 10/100, equipamentos que não implementem PoE e equipamentos que adicionem no mínimo 48 portas 10G. 6. Sistema Operacional: 6.1 O equipamento ofertado deve possuir um sistema operacional modular. 6.2 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. 7. Funcionalidades de Camada 3: 7.1 Deve suportar o armazenamento de até 12.000 (doze mil) rotas IPv4. 7.2. Deve suportar o armazenamento de até 6.000 (seis mil) rotas IPv6. 7.3. Deve implementar Dual Stack, ou seja, IPV6 e IPv4. 7.4. Implementar roteamento estático com suporte a, no mínimo, 1000 rotas. 7.5. Implementar, no mínimo, 2048 interfaces IP (v4 ou v6). 7.6. Implementar IGMPv1 (RFC 1112), IGMP v2 (RFC 2236), IGMP v3 (RFC 3376). 7.7. Implementar os protocolos de roteamento IP: RFC 1058 – RIP v1 e RFC 2453 – RIP v2. 7.8. Suportar o protocolo de roteamento OSPF v2, incluindo autenticação MD5. 7.9 A implementação de OSPF e rotas estáticas deve incluir ECMP (Equal Cost Multi Path). 7.10. Suportar OSPF para IPv6 (OSPFv3) RFC 2740 7.11 Implementar PIM Snooping. 7.12. Suportar protocolo de multicast PIM-SM. 7.13 Suportar PIM-DM. 7.14 Suportar PIM-SSM. 7.15. Suportar MSDP (Multicast Source Discovery Protocol). 7.16. Suportar VRRPv3 (RFC 5798) ou similar. 7.17. Suportar BGP incluindo ECMP (Equal Cost Multi Path). 7.18. Suportar BGP v4. 7.19. Implementar MLD Snooping v1 e v2. 8. Funcionalidades de Camada 2: 8.1 Implementar EAPS (RFC 3619) ou protocolo similar de resiliência em camada 2, específico para topologias em anel, que permita tempo de convergência inferior a 200 ms. 8.2. Implementar 4094 VLANs por porta, ativas simultaneamente, através do protocolo 802.1Q. 8.3 Implementar Private VLANs. 8.4. Implementar agregação de links conforme padrão IEEE 802.3ad com suporte a LACP. 8.5. Implementar agregação de links conforme padrão IEEE 802.3ad com, no mínimo, 128 grupos, sendo 32 links agregados por				

		grupo. 8.6. 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 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. 8.7 Implementar Spanning-Tree (IEEE 802.1d), Rapid Spanning Tree (IEEE 802.1w), Multiple Instance STP (802.1s) e PVST+. 8.8. 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. 8.9. Implementar funcionalidade vinculada ao Spanning-tree que evite a eleição de outros switches da rede como Root. 8.10. Implementar funcionalidade vinculada ao Spanning-tree que permita desabilitar uma porta de acesso assim que a mesma receba uma BPDU. 9. Gerenciamento/Monitoramento: 9.1 Implementar os seguintes grupos de RMON através da RFC1757: History, Statistics, Alarms e Events. 9.2. Implementar gerenciamento via web com suporte a HTTP e HTTPS/SSL. Esta funcionalidade deve ser implícita ao equipamento. 9.3. 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. 10. Funcionalidades Gerais: 10.1 O equipamento deve implementar o set de protocolos DCB (Data Center Bridging) com suporte a PFC (Priority Flow Control), ETS (Enhanced Transmission Selection) e DCBx (Data Center Bridging Exchange). 10.2 O equipamento deverá suportar VPLS e H-VPLS de acordo com os seguintes padrões: 10.2.1 RFC 2961 RSVP Refresh Overhead Reduction Extensions. 10.2.2 RFC 3031 Multiprotocol Label Switching Architecture. 10.2.3 RFC 3032 MPLS Label Stack Encoding. 10.2.5 RFC 3209 RSVP-TE: Extensions to RSVP for LSP Tunnels. 10.2.6 RFC 3630 Traffic Engineering Extensions to OSPFv2. 10.2.7 RFC 3811 Definitions of Textual Conventions (TCs) for Multiprotocol Label Switching (MPLS) Management 10.2.8 RFC 3812 Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) Management Information Base (MIB). 10.2.9 RFC 3813 Multiprotocol Label Switching (MPLS) Label Switching Router (LSR) Management Information Base (MIB) 10.2.10 RFC 3815 Definitions of Managed Objects for the Multiprotocol Label Switching (MPLS), Label Distribution Protocol (LDP). 10.2.11 RFC 4090 Fast Re-route Extensions to RSVP-TE for LSP (Detour Paths). 10.2.12 RFC 4379 Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures (LSP Ping). 10.2.13 draft-ietf-bfd-base-09.txt Bidirectional Forwarding Detection. 10.2.14 RFC 4447 Pseudowire Setup and Maintenance using the Label				

		Distribution Protocol (LDP). 10.2.15 RFC 4448 Encapsulation Methods for Transport of Ethernet over MPLS Networks. 10.2.16 RFC 4762 Virtual Private LAN Services (VPLS) using Label Distribution Protocol (LDP) Signaling. 10.2.17 RFC 5085 Pseudowire Virtual Circuit Connectivity Verification (VCCV). 10.2.18 RFC 5542 Definitions of Textual Conventions for Pseudowire (PW) Management. 10.2.19 RFC 5601 Pseudowire (PW) Management Information Base (MIB). 10.2.20 RFC 5602 Pseudowire (PW) over MPLS PSN (MIB). 10.2.21 RFC 5603 Ethernet Pseudowire (PW) MIB. 10.2.22 draft-ietf-l2vpn-vpls-mib-02.txt Virtual Private LAN Services (VPLS) MIB". 10.3 Implementar WRED. 10.4 Implementar IPFIX ou Netflow, em hardware. Não serão aceitas soluções similares. 10.5 Implementar Port Mirroring e RSPAN (Remote Mirroring). 10.6. Implementar IPv6 em hardware nos módulos de interface. 10.7. Implementar os seguintes protocolos em IPv6: Ping, Traceroute, Telnet, SSH-2. 10.8. Implementar IEEE 802.1ab Link Layer Discovery Protocol (LLDP). 10.9. Implementar LLDP-MED (Media Endpoint Discovery), segundo ANSI/TIA-1057, Draft 08. 10.10. 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. 10.11. Suportar transferência de arquivos através dos protocolos TFTP e SCP. 10.12. Implementar a atualização de imagens de software e configuração através de um servidor TFTP. 10.13. Implementar DHCP/Bootp relay. 10.14. Implementar servidor DHCP interno que permita a configuração de um intervalo de endereços IP a serem atribuídos os clientes DHCP. 10.15. Implementar funcionalidade que permita sua autoconfiguração através dos protocolos DHCP e TFTP, permitindo o provisionamento em massa com o mínimo de intervenção humana. 10.16. Suportar múltiplos servidores Syslog. 10.17. 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. 10.18. Implementar ajuste de clock do equipamento utilizando NTP com autenticação MD5 ou SNTP. 10.19 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. 10.20 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. 10.21 A funcionalidade de Rate Shaping deve permitir a configuração de CIR (Commited Rate) e peak rate.				

		10.22. Implementar 8 filas de prioridade em hardware por porta. 10.23. Implementar a leitura, classificação e remarcação de QoS (802.1p e DSCP). 10.24. 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. 10.25. 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, 802.1p. 10.26 Implementar os algoritmos de gerenciamento de filas WRR (Weighted Round Robin) e SP (Strict Priority). 11. Funcionalidades de Politicas & Segurança: 11.1 Implementar regras de ACL de entrada (inbound ACLs) e de saída (outbound ACLs) em hardware. 11.2. Implementar ACLs de entrada (ingress ACLs) em hardware, baseadas em critérios das camadas 2 (MAC origem e destino) e campo 802.1p, 3 (IP origem e destino) e 4 (portas TCP e UDP), em todas as interfaces e VLANs, com suporte a endereços IPv6. Deverá ser possível aplicar ACLs para tráfego interno de uma determinada VLAN. 11.3. 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. 11.4 Implementar Policy Based Routing. 11.5 Implementar Policy Based Switching, ou seja, possibilitar que o tráfego classificado por uma ACL seja redirecionado para uma porta física específica. 11.6 Implementar Gratuitous ARP Protection. 11.7. 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. 11.8. Implementar limitação de número de endereços MAC aprendidos por uma porta, para uma determinada VLAN. 11.9. 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. 11.10. 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. 11.11 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. 11.12. Implementar múltiplos suplicantes por porta, onde cada dispositivo deve ser autenticado de forma independente, podendo ser encaminhados à VLANs distintas. As múltiplas autenticações devem ser realizadas através de IEEE 802.1x. 11.13 Implementar TACACS+ segundo a RFC 1492. Não serão aceitas soluções similares. 11.14. Implementar autenticação RADIUS com suporte a: 11.14.1 RADIUS Authentication. 11.14.2 RADIUS Accounting. 11.14.3 RADIUS EAP support for 802.1X. 11.15 A implementação de RADIUS e TACACS+ deve estar disponível para autenticação de usuários via Telnet e Console serial. 11.16. Implementar RADIUS e TACACS+ per-				

		command authentication. 11.17. Implementar autenticação baseada em web, com suporte a SSL, através de RADIUS ou através da base local do switch. 11.18. Implementar autenticação baseada em endereço MAC, através de RADIUS ou através da base local do switch. 11.19. Implementar funcionalidade que permita que somente servidores DHCP autorizados atribuam configuração IP aos clientes DHCP (Trusted DHCP Server). 12. Certificações: 12.1 Possuir homologação da ANATEL, de acordo com a Resolução número 242. 13. Garantia: 13.1 O Switch Distribuição deverá possuir garantia do fabricante pelo período mínimo de 60 (sessenta) meses. 13.2. Nos casos de troca equipamentos defeituosos, os mesmos devem ser enviados no próximo dia útil subsequente a abertura do chamado e comprovação do defeito, sem quaisquer custos adicionais. 13.3. Os chamados técnicos deverão ser gerenciados pelo fornecedor em horário comercial na modalidade 8x5 (oito horas por dia, cinco dias por semana), através de telefone gratuito. Também deve ser disponibilizado endereço de e-mail para abertura dos chamados técnicos. 13.4 A empresa deverá possuir pelo menos 1 (um) Engenheiro apto a prestar serviços de suporte técnico no equipamento proposto. O Engenheiro deverá possuir registro junto ao CREA e certificação no produto comprovada pelo fabricante. 13.5 O Fabricante deverá disponibilizar gratuitamente suporte e atualização dos softwares, firmwares e sistema operacional para correção de bugs e implementações de segurança; 13.6 Fornecer os softwares e suas atualizações, firmwares, sistema operacional através de meio eletrônico ou magnético sem ônus adicionais. 14. Compatibilidade: 14.1. Os componentes do Switch Distribuição deverão ser homologados pelo fabricante. Não será aceita a adição ou subtração de qualquer componente não original de fábrica para adequação do equipamento; 14.2 Todos os componentes do Switch Distribuição deverão ser compatíveis entre si, com o conjunto do equipamento e com suas funcionalidades, sem a utilização de adaptadores, fresagens, pinturas, usinagens em geral, furações, emprego de adesivos, fitas adesivas ou quaisquer outros procedimentos ou emprego de materiais inadequados ou que visem adaptar forçadamente o equipamento ou suas partes que sejam fisicamente ou logicamente incompatíveis. (Será aceito o regime de OEM desde que comprovado pelo próprio fabricante). 14.3 O Switch Distribuição especificado neste item deve ser totalmente compatível com a Solução de Gerenciamento NetSight Base 500. Referência: Marca Extreme Network, modelo X460-G2-48p-10GE4-Base-Unit ou de melhor qualidade. (TCU, Acórdão 2401/2006, 9.3.2 – Plenário). **(COTA RESERVADA ME/EPP/MEI) – VINCULADO AO ITEM 44**				
68981	46	Switch Top of Rack 10GBase-X, Summit X670-G2-48x-4q-Base-Unit 1. Gabinete/Chassis: 1.1 A solução deve ser composta de um único equipamento, montável em rack 19 polegadas devendo este vir acompanhado dos devidos acessórios para tal. 1.2 Possuir ventilação “front-to-back”, ou seja, a saída de ar quente deve acontecer pela traseira do equipamento. 1.3. Possuir bandeja de ventiladores substituível	un	1		

		em campo (field replaceable). 1.4. Possuir leds indicativos de funcionamento da fonte de alimentação, ventiladores e status das portas. 2. Fonte de Alimentação: 2.1 Possuir fonte de alimentação interna que trabalhe em 100V-240V, 50/60 Hz, com detecção automática de tensão e frequência, hot-swappable. 2.2. Possuir fonte de alimentação AC redundante interna, hot-swappable. 2.3. Suportar fonte de alimentação DC interna 2.4 Possibilitar que o equipamento funcione com uma fonte AC e uma fonte DC instaladas simultaneamente. 3. Performance/Desempenho: 3.1 Possuir capacidade agregada de switching de, no mínimo, 1280 Gbps. 3.2. Possuir a capacidade de encaminhamentos de pacotes, de no mínimo 952 Mpps utilizando pacotes de 64 bytes. 3.3. Deve suportar o armazenamento de até 288.000 (duzentos e oitenta e oito mil) endereços MAC. 3.4. Implementar jumbo frames em todas as portas ofertadas, com suporte a pacotes de até 9216 Bytes. 4. Portas/Interfaces: 4.1 Todas as interfaces ofertadas devem ser non-blocking. 4.2. Possuir 48 portas 1/10GBASE-X ativas simultaneamente, baseadas em SFP+, devendo um mesmo slot suportar interfaces 10 Gigabit Ethernet 10GBASE-SR, 10GBASE-LR, 10GBASE-CR (Twinax). Essas interfaces deverão suportar a utilização de mini-GBICs (SFPs) Gigabit Ethernet 1000Base-SX e 1000Base-LX (10KM). Não é permitida a utilização de conversores externos; 4.3 Possuir 4 portas 40GBASE-X ativas simultaneamente, baseadas em QSFP+, devendo um mesmo slot suportar interfaces 40 Gigabit Ethernet 40GBASE-SR4 e 40GBASE-LR4, não sendo permitida a utilização de conversores externos. 4.4 Todas as interfaces 10 Gigabit Ethernet, Gigabit Ethernet e 40 Gigabit Ethernet acima devem funcionar simultaneamente; 4.5 Possuir porta de console com conector RJ-45 ou DB9 macho. 4.6 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. 5. Empilhamento: 5.1 Suportar empilhamento de até oito equipamentos e gerência através de um único endereço IP. 5.2. Deve suportar empilhamento através de portas 10 Gigabit Ethernet e 40 Gigabit Ethernet padrão, permitindo o empilhamento de equipamentos que estejam em locais distintos com no mínimo 10 km, conectados através de fibra óptica. 5.3 O empilhamento deve suportas arquitetura de anel para prover resiliência. 5.4 O empilhamento deve permitir a criação de grupos de links agregados entre diferentes membros da pilha, segundo 802.3ad. 5.5 O empilhamento deve suportar espelhamento de tráfego entre diferentes unidades da pilha. Caso seja ofertado um equipamento do tipo chassi modular, deve suportar espelhamento de tráfego entre diferentes módulos do chassi. 5.6. Deve ser possível mesclar em uma mesma pilha equipamentos que possuam portas de acesso 10/100/1000 e equipamentos implementem PoE 6. Sistema Operacional: 6.1 O equipamento ofertado deve possuir um sistema operacional modular. 6.2 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. 7. Funcionalidades de Camada 3: 7.1. Implementar Proxy-ARP (RFC 1027). 7.2. Deve implementar Dual Stack, ou seja IPv6 e IPv4, com suporte as seguintes funcionalidades/RFCs: 7.2.1. RFC 1981, Path MTU Discovery for IPv6, August 1996 - Host Requirements; 7.2.2. RFC 5095, Internet Protocol, Version 6 (IPv6) Specification; 7.2.3. RFC 4861, Neighbor Discovery for IP Version 6, (IPv6); 7.2.4. RFC 2462, IPv6 Stateless Address Auto configuration - Host Requirements; 7.2.5. RFC 2463, Internet Control Message Protocol (ICMPv6) for the IPv6 Specification; 7.2.6. RFC 2464, Transmission of IPv6 Packets over Ethernet Networks; 7.2.7. RFC 2465, IPv6 MIB, General Group and Textual Conventions; 7.2.8. RFC 2466, MIB for ICMPv6; 7.2.9. RFC 3513, Internet Protocol Version 6 (IPv6) Addressing Architecture; 7.2.10. RFC 3587, Global Unicast Address Format; 7.3. Deve implementar BGPv4 de acordo com as seguintes RFCs: RFC 1771, Border Gateway Protocol 4; RFC 1965, Autonomous System Confederations for BGP; RFC 2796, BGP Route Reflection (supersedes RFC 1966); RFC 1997, BGP Communities Attribute; RFC 1745, BGP4/IDRP for IP—OSPF Interaction; RFC 2385, TCP MD5 Authentication for BGPv4; RFC 2439, BGP Route Flap Damping; RFC 3392, Capabilities Advertisement with BGP-4; RFC 2918, Route Refresh Capability for BGP-4; RFC 4360, BGP Extended Communities Attribute; RFC 4760, Multiprotocol Extensions for BGP4; RFC 4274, Graceful Restart Mechanism for BGP; RFC 4893, BGP Support for four-octet AS number space; 7.4 A implementação de BGP deve incluir ECMP (Equal Cost Multi Path). 7.5 A implementação de BGP deve permitir, no mínimo, 128 peers e 25.000 rotas. 7.6. Implementar roteamento estático com suporte a, no mínimo, 1000 rotas; 7.7 Implementar, no mínimo, 2048 interfaces IP (v4 ou v6). 7.8. Implementar IGMPv1 (RFC 1112), IGMP v2 (RFC 2236), IGMP v3 (RFC 3376). 7.9. Implementar os protocolos de roteamento IP: RFC 1058 – RIP v1 e RFC 2453 – RIP v2. 7.10. Implementar IGMP v1, v2 e v3 Snooping. 7.11. Implementar IGMPv2 SSM. 7.12. Implementar o protocolo de roteamento OSPFv2 (RFC 2328), incluindo autenticação MD5. 7.13 A implementação de OSPF deve estar de acordo com as seguintes RFCs: RFC 1587 The OSPF NSSA Option; RFC 1765 OSPF Database Overflow; RFC 2370 The OSPF Opaque LSA Option; RFC 3623 Graceful OSPF Restart" 7.14 A implementação de OSPF e rotas estáticas deve incluir ECMP (Equal Cost Multi Path). 7.15. Implementar OSPFv3 conforme RFC 2740. 7.16 A implementação de OSPFv3 e rotas estáticas para IPv6 deve incluir ECMP (Equal Cost Multi Path). 7.17. Implementar IS-IS, de acordo com as seguintes RFCs: RFC 1195 Use of OSI IS-IS for Routing in TCP/IP and Dual Environments (TCP/IP transport only); RFC 2763 Dynamic Hostname Exchange Mechanism for IS-IS; RFC 2966 Domain-wide Prefix Distribution with Two-Level IS-IS; RFC 2973 IS-IS Mesh Groups; Draft-ietf-isis-restart-02 Restart Signaling for IS-IS; Draft-ietf-isis-ipv6-06 Routing IPv6 with IS-IS;				

		Draft-ietf-isis-wg-multi-topology-11 Multi Topology (MT) Routing in IS-IS; 7.18. Implementar PIM Snooping. 7.19. Implementar protocolo de multicast PIM-SM para IPv4 e IPv6. 7.20. Implementar PIM-DM para IPv4 e IPv6. 7.21. Implementar PIM-SSM segundo a RFC 3569. 7.22. Implementar MSDP (Multicast Source Discovery Protocol), de acordo com a RFC 3618. 7.23. Implementar VRRPv3 (RFC 5798). 7.24. Implementar MLD Snooping v1 e v2 8 Funcionalidades de Camada 2: 8.1 O equipamento deve implementar VRF (Virtual Routing Forwarding) fora do contexto de protocolo MPLS, com no mínimo 190 instâncias. 8.2 O equipamento deve implementar Virtual Routing, permitindo a sua virtualização em no mínimo 63 entidades lógicas com tabelas de roteamento independentes. 8.3. Implementar EAPS (RFC 3619) ou protocolo similar de resiliência em camada 2, específico para topologias em anel, que permita tempo de convergência inferior a 200 ms. 8.3 A implementação de EAPS (RFC 3619) deve também utilizar IEEE 802.1ag CFM (Connectivity Fault Management) para detecção de falha de link. 8.5. Implementar 4096 VLANs por porta, ativas simultaneamente, através do protocolo 802.1Q. 8.6 Implementar Private VLANs. 8.7. Implementar VLAN Translation. 8.8 Implementar Super VLAN/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. 8.8. Implementar agregação de links conforme padrão IEEE 802.3ad com suporte a LACP. 8.9. Implementar agregação de links conforme padrão IEEE 802.3ad com, no mínimo, 128 grupos, sendo 32 links agregados por grupo. 8.10. 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 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. 8.11 Implementar Spanning-Tree (IEEE 802.1d), Rapid Spanning Tree (IEEE 802.1w), Multiple Instance STP (802.1s) e PVST+. 8.12. Implementar a configuração de Multiple Spanning Tree Protocol, com suporte a, pelo menos, 64 domínios. 8.13. 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. 8.14. Implementar funcionalidade vinculada ao Spanning-tree que evite a eleição de outros switches da rede como Root. 8.15. Implementar funcionalidade vinculada ao Spanning-tree que permita desabilitar uma porta de acesso assim que a mesma receba uma BPDU. 9. Gerenciamento/Monitoramento: 9.1 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. 9.2. Possibilitar a coleta de estatísticas de tráfego baseada em VLANs IEEE 802.1Q e double-tagged VLANs IEEE 802.1ad. 9.3 Implementar os seguintes grupos de RMON através da RFC1757: History, Statistics, Alarms e Events. 9.4. 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. 9.5. Implementar gerenciamento através de SNMPv1 (RFC 1157), v2c (RFCs 1901 a 1908), v3 (RFCs 3410 a 3415) e SNMP para IPv6. 9.6. Implementar SMON de acordo com a RFC 2613. 9.7. Implementar gerenciamento via web com suporte a HTTP e HTTPS/SSL, permitindo visualização gráfica da utilização (em percentual, bytes e pacotes) das portas. 10. Funcionalidades Gerais: 10.1 Suportar os métodos de encaminhamento de frames &quotstore-and-forward" e &quotcut-through". 10.2 O equipamento deve implementar o set de protocolos DCB (Data Center Bridging) com suporte a PFC (Priority Flow Control), ETS (Enhanced Transmission Selection) e DCBx (Data Center Bridging Exchange). 10.3. O equipamento deverá suportar VPLS e H-VPLS de acordo com os seguintes padrões: RFC 2961 RSVP Refresh Overhead Reduction Extensions; RFC 3031 Multiprotocol Label Switching Architecture; RFC 3032 MPLS Label Stack Encoding; RFC 3036 Label Distribution Protocol (LDP); RFC 3209 RSVP-TE: Extensions to RSVP for LSP Tunnels; RFC 3630 Traffic Engineering Extensions to OSPFv2; RFC 3811 Definitions of Textual Conventions (TCs) for Multiprotocol Label Switching (MPLS) Management; RFC 3812 Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) Management Information Base (MIB); RFC 3813 Multiprotocol Label Switching (MPLS) Label Switching Router (LSR) Management Information Base (MIB); RFC 3815 Definitions of Managed Objects for the Multiprotocol Label Switching (MPLS), Label Distribution Protocol (LDP); RFC 4090 Fast Re-route Extensions to RSVP-TE for LSP (Detour Paths); RFC 4379 Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures (LSP Ping); draft-ietf-bfd-base-09.txt Bidirectional Forwarding Detection; RFC 4447 Pseudowire Setup and Maintenance using the Label Distribution Protocol (LDP); RFC 4448 Encapsulation Methods for Transport of Ethernet over MPLS Networks; RFC 4762 Virtual Private LAN Services (VPLS) using Label Distribution Protocol (LDP) Signaling; RFC 5085 Pseudowire Virtual Circuit Connectivity Verification (VCCV); RFC 5542 Definitions of Textual Conventions for Pseudowire (PW) Management; RFC 5601 Pseudowire (PW) Management Information Base (MIB); RFC 5602 Pseudowire (PW) over MPLS PSN (MIB); RFC 5603 Ethernet Pseudowire (PW) MIB; draft-ietf-l2vpn-vpls-mib-02.txt Virtual Private LAN Services (VPLS) MIB" 10.4. Implementar WRED. 10.5. Implementar MVR (Multicast VLAN Registration). 10.6.				

		Implementar sFlow ou Netflow, em hardware. 10.7 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. 10.8. Implementar IPv6 em hardware. 10.9. Implementar os seguintes protocolos em IPv6: Ping, Traceroute, Telnet, SSH-2, SNMP, SNTP e DNS. 10.10. Implementar IEEE 802.1ab Link Layer Discovery Protocol (LLDP). 10.11. Implementar LLDP-MED (Media Endpoint Discovery), segundo ANSI/TIA-1057, Draft 08. 10.12. 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. 10.13. Possuir DNS Client para IPv4 segundo a RFC 1591 e DNS Client para IPv6. 10.14 Possuir Telnet client and server segundo a RFC 854. 10.15. Implementar a atualização de imagens de software e configuração através de um servidor TFTP. 10.16. Implementar DHCP/Bootp relay configurável por VLAN para IPv4 e IPv6. 10.17. 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. 10.18. Implementar funcionalidade que permita sua autoconfiguração através dos protocolos DHCP e TFTP, permitindo o provisionamento em massa com o mínimo de intervenção humana. 10.19. Implementar DHCP Option 82, de acordo com a RFC 3046, com identificação de porta e VLAN, configurável por VLAN. 10.20. Suportar múltiplos servidores Syslog. 10.21. 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. 10.22. Implementar ajuste de clock do equipamento utilizando NTP com autenticação MD5 ou SNTP. 10.23 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. 10.24 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. 10.25 A funcionalidade de Rate Shaping deve permitir a configuração de CIR (Commited Rate), banda máxima, banda mínima e peak rate. 10.26. Implementar 8 filas de prioridade em hardware por porta. 10.27. Implementar a leitura, classificação e remarcação de QoS (802.1p e DSCP). 10.28. 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. 10.29. 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.Implementar os algoritmos de gerenciamento de filas WRR (Weighted Round Robin) e SP (Strict Priority). 10.30. Deve suportar mecanismo para permitir mobilidade de máquinas virtuais (VMs) de uma porta da solução virtual ofertada para qualquer outra porta, de forma que todas as características e configurações necessárias para operação da VM na nova porta física devem ser realizadas automaticamente (ACLs e características de QoS), sem necessidade de configuração manual dos equipamentos; 10.31 Deve implementar contadores de pacotes e bytes por máquina virtual. No caso de movimentação da máquina virtual, o contador deve ser configurado automáticamente na porta de destino para onde a máquina virtual foi movida. 10.32. Implementar IEEE 802.1v: VLAN classification by Protocol and Port. 10.33. Implementar MAC Based VLAN. 10.34 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. 10.35. Implementar IEEE 802.1ad com a possibilidade de associar CVIDs específicos para diferentes SVIDs (selective QinQ, 802.1ad CEP). A implementação deverá permitir a tradução do CVID. 10.26. Implementar IEEE 802.1ag L2 ping e traceroute, CFM (Connectivity Fault Management). 10.37. Implementar funcionalidade baseada na recomendação do ITU Y.1731 (ou similar) que permita medir o atraso (two-way delay) e a variância (jitter) entre dois pontos quaisquer da rede. 10.38. Implementar o protocolo ITU-T G.8032 ERPS. 10.39. Implementar o protocolo GRE. 10.40 Deve implementar IPv6 de acordo com as seguintes RFCs: Static Unicast routes for IPv6; RFC 1981, Path MTU Discovery for IPv6, August 1996 - Router Requirements; RFC 2462, IPv6 Stateless Address Auto configuration - Router Requirements; RFC 2080, RIPng; RFC 2893, Configured Tunnels; RFC 2710, IPv6 Multicast Listener Discovery v1 (MLDv1) Protocol; RFC 3056, 6-to-4; RFC 3810, IPv6 Multicast Listener Discovery v2 (MLDv2) Protocol; RFC 6106, IPv6 Router Advertisement Options for DNS Configuration; IPv6 Router Advertisement Filtering; 10.41 Implementar NTP server. 10.42 A implementação de NTP server deve suportar a configuração de um endereço virtual do VRRP como endereço IP para o servidor NTP. 10.43. 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). 10.44 Implementar cliente e servidor SSHv2. 10.45 Implementar cliente e servidor SCP e servidor SFTP. 10.46. Implementar linguagem de scripting, permitindo a automatização de tarefas. A linguagem deve implementar estruturas de controle como loops e execução condicional e permitir a				

		definição de variáveis. 10.47. 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. 10.48. Deve suportar integração com o OpenStack utilizando, no mínimo, o plugin Quantum 1.1 e 2.0. 10.49. Implementar os algoritmos de gerenciamento de filas WRR (Weighted Round Robin), WDRR (Weighted Deficit Round Robin) e SP (Strict Priority). 10.50. Deve implementar, ao menos dois dos algoritimos acima, simultâneamente em uma mesma porta. 10.51 Implementar as seguintes RFCs: RFC 2474 DiffServ Precedence; RFC 2598 DiffServ Expedited Forwarding (EF); RFC 2597 DiffServ Assured Forwarding (AF); RFC 2475 DiffServ Core and Edge Router Functions. 11. Funcionalidades de Politicas & Segurança: 11.1 mplementar 4096 regras de ACL de entrada (ingress ACLs). 11.2. Implementar 1024 regras de ACL de saída (egress ACLs). 11.3. Implementar ACLs de entrada (ingress ACLs) em hardware, baseadas em critérios das camadas 2 (MAC origem e destino) e campo 802.1p, 3 (IP origem e destino) e 4 (portas TCP e UDP), em todas as interfaces e VLANs, com suporte a endereços IPv6. Deverá ser possível aplicar ACLs para tráfego interno de uma determinada VLAN. 11.4. 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. 11.5 Implementar Policy Based Routing, inclusive para fluxos internos a uma determinada VLAN para IPv4 e IPv6. 11.6 Implementar Policy Based Switching, ou seja, possibilitar que o tráfego classificado por uma ACL seja redirecionado para uma porta física específica. 11.7 Implementar Gratuitous ARP Protection. 11.8. 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. 11.9. Implementar limitação de número de endereços MAC aprendidos por uma porta, para uma determinada VLAN. 11.10. 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. 11.11. 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. 11.12 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. 11.13. Implementar múltiplos suplicantes por porta, onde cada dispositivo deve ser autenticado de forma independente, podendo ser encaminhados à VLANs distintas. As múltiplas autenticações devem ser realizadas através de IEEE 802.1x. 11.14 Implementar TACACS+ segundo a RFC 1492. 11.15. Implementar autenticação RADIUS com suporte a: RFC 2138 RADIUS				

		Authentication; RFC 2139 RADIUS Accounting; RFC 3597 RADIUS EAP support for 802.1X; 11.16 A implementação de RADIUS e TACACS+ deve estar disponível para autenticação de usuários via Telnet e Console serial. 11.17. Implementar RADIUS e TACACS+ per-command authentication. 11.18. Implementar autenticação baseada em web, com suporte a SSL, através de RADIUS ou através da base local do switch. 11.19. Implementar autenticação baseada em endereço MAC, através de RADIUS ou através da base local do switch. 11.20. Implementar funcionalidade que permita que somente endereços designados por um servidor DHCP tenham acesso à rede. 11.21. Implementar funcionalidade que permita que somente servidores DHCP autorizados atribuam configuração IP aos clientes DHCP (Trusted DHCP Server). 11.22. Implementar funcionalidade que permita a execução de ACLs em um determinado horário do dia (time-based ACLs). 11.23. Implementar políticas por usuário, permitindo que as configurações de ACL, QoS sejam aplicadas na porta utilizada para a conexão à rede, após a autenticação. 11.24. 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. 12. Certificações: 12.1 Possuir homologação da ANATEL, de acordo com a Resolução número 242. 13. Garantia: 13.1 O Switch Top of Rack deverá possuir garantia do fabricante pelo período mínimo de 36 (trinta e seis) meses. 13.2. Nos casos de troca equipamentos defeituosos, os mesmos devem ser enviados no próximo dia útil subsequente a abertura do chamado e comprovação do defeito, sem quaisquer custos adicionais. 13.3. Os chamados técnicos deverão ser gerenciados pelo fornecedor em horário comercial na modalidade 8x5 (oito horas por dia, cinco dias por semana), através de telefone gratuito. Também deve ser disponibilizado endereço de e-mail para abertura dos chamados técnicos. 13.4 A empresa deverá possuir pelo menos 1 (um) Engenheiro apto a prestar serviços de suporte técnico no equipamento proposto. O Engenheiro deverá possuir registro junto ao CREA e certificação no produto comprovada pelo fabricante. 13.5 O Fabricante deverá disponibilizar gratuitamente, suporte e atualizações dos softwares, firmwares e sistema operacional para correção de bugs e implementações de segurança; 13.6 Fornecer os softwares e suas atualizações, firmwares, sistema operacional através de meio eletrônico ou magnético sem ônus adicionais. 14. Compatibilidade: 14.1. Os componentes do Switch Top of Rack deverão ser homologados pelo fabricante. Não será aceita a adição ou subtração de qualquer componente não original de fábrica para adequação do equipamento; 14.2 Todos os componentes do Switch Top of Rack deverão ser compatíveis entre si, com o conjunto do equipamento e com suas funcionalidades, sem a utilização de adaptadores, fresagens, pinturas, usinagens em geral, furações, emprego de adesivos, fitas adesivas ou				

		quaisquer outros procedimentos ou emprego de materiais inadequados ou que visem adaptar forçadamente o equipamento ou suas partes que sejam fisicamente ou logicamente incompatíveis. (Será aceito o regime de OEM desde que comprovado pelo próprio fabricante). 14.3 O Switch Top of Rack especificado neste item deve ser totalmente compatível com a Solução de Gerenciamento NetSight Base 500. Referência: Marca Extreme Network, modelo Summit X670-G2-48x-4q-Base-Unit ou de melhor qualidade. (TCU, Acórdão 2401/2006, 9.3.2 – Plenário).				
68964	47	Transceiver 1000BASE-LX 1. Características Gerais: 1.1 Módulo Transceptor Ótico Gigabit Ethernet para fibra monomodo; 1.2 Formato Hot-Pluggable padrão SFP; 1.3 Suportar distância de no mínimo 10 km; 1.4 Conector LC; 2. Garantia: 2.1 O Transceiver deverá possuir garantia do fabricante pelo período mínimo de 12 (doze) meses. 2.2. Nos casos de troca equipamentos defeituosos, os mesmos devem ser enviados no próximo dia útil subsequente a abertura do chamado e comprovação do defeito, sem quaisquer custos adicionais. 2.3. Os chamados técnicos deverão ser gerenciados pelo fornecedor em horário comercial na modalidade 8x5 (oito horas por dia, cinco dias por semana), através de telefone gratuito. Também deve ser disponibilizado endereço de e-mail para abertura dos chamados técnicos. 2.4 A empresa deverá possuir pelo menos 1 (um) Engenheiro apto a prestar serviços de suporte técnico no equipamento proposto. O Engenheiro deverá possuir registro junto ao CREA e certificação no produto comprovada pelo fabricante. 3. Compatibilidade: 3.1 Deve ser obrigatoriamente do mesmo fabricante, compatível e peça original dos Switches de Acesso. Referência: Marca Extreme Network, modelo 1000BASE-LX SFP 10 Pack, Hi ou de melhor qualidade. (TCU, Acórdão 2401/2006, 9.3.2 – Plenário).	tes	80		
68963	48	Transceiver 1000BASE-SX 1. Características Gerais: 1.1 Módulo Transceptor Ótico Gigabit Ethernet para fibra multimodo; 1.2 Formato Hot-Pluggable padrão SFP; 1.3 Suportar distância de no mínimo 550 metros; 1.4 Conector LC; 2. Garantia: 2.1 O Transceiver deverá possuir garantia do fabricante pelo período mínimo de 12 (doze) meses. 2.2. Nos casos de troca equipamentos defeituosos, os mesmos devem ser enviados no próximo dia útil subsequente a abertura do chamado e comprovação do defeito, sem quaisquer custos adicionais. 2.3. Os chamados técnicos deverão ser gerenciados pelo fornecedor em horário comercial na modalidade 8x5 (oito horas por dia, cinco dias por semana), através de telefone gratuito. Também deve ser disponibilizado endereço de e-mail para abertura dos chamados técnicos. 2.4 A empresa deverá possuir pelo menos 1 (um) Engenheiro apto a prestar serviços de suporte técnico no equipamento proposto. O Engenheiro deverá possuir registro junto ao CREA e certificação no produto comprovada pelo fabricante. 3. Compatibilidade: 3.1 Deve ser obrigatoriamente do mesmo fabricante, compatível e peça original dos Switches de Acesso. Referência: Marca Extreme Network, modelo 1000BASE-SX SFP 10 Pack, Hi ou de melhor qualidade. (TCU, Acórdão 2401/2006, 9.3.2 – Plenário).	un	80		

68966	49	Transceiver 10GBASE-LR 1. Características Gerais: 1.1 Módulo Transceptor Ótico 10 Gigabit Ethernet para fibra monomodo; 1.2 Formato Hot-Pluggable padrão SFP+; 1.3 Suportar distância de no mínimo 10 km; 1.4 Conector LC; 2. Garantia: 2.1 O Transceiver deverá possuir garantia do fabricante pelo período mínimo de 12 (doze) meses. 2.2. Nos casos de troca equipamentos defeituosos, os mesmos devem ser enviados no próximo dia útil subsequente a abertura do chamado e comprovação do defeito, sem quaisquer custos adicionais. 2.3. Os chamados técnicos deverão ser gerenciados pelo fornecedor em horário comercial na modalidade 8x5 (oito horas por dia, cinco dias por semana), através de telefone gratuito. Também deve ser disponibilizado endereço de e-mail para abertura dos chamados técnicos. 2.4 A empresa deverá possuir pelo menos 1 (um) Engenheiro apto a prestar serviços de suporte técnico no equipamento proposto. O Engenheiro deverá possuir registro junto ao CREA e certificação no produto comprovada pelo fabricante. 3. Compatibilidade: 3.1 Deve ser obrigatoriamente do mesmo fabricante, compatível e peça original dos Switches de Acesso. Referência: Marca Extreme Network, modelo LR SFP+ Module ou de melhor qualidade. (TCU, Acórdão 2401/2006, 9.3.2 – Plenário). **(COTA PRINCIPAL)**	un	45		
68966	50	Transceiver 10GBASE-LR 1. Características Gerais: 1.1 Módulo Transceptor Ótico 10 Gigabit Ethernet para fibra monomodo; 1.2 Formato Hot-Pluggable padrão SFP+; 1.3 Suportar distância de no mínimo 10 km; 1.4 Conector LC; 2. Garantia: 2.1 O Transceiver deverá possuir garantia do fabricante pelo período mínimo de 12 (doze) meses. 2.2. Nos casos de troca equipamentos defeituosos, os mesmos devem ser enviados no próximo dia útil subsequente a abertura do chamado e comprovação do defeito, sem quaisquer custos adicionais. 2.3. Os chamados técnicos deverão ser gerenciados pelo fornecedor em horário comercial na modalidade 8x5 (oito horas por dia, cinco dias por semana), através de telefone gratuito. Também deve ser disponibilizado endereço de e-mail para abertura dos chamados técnicos. 2.4 A empresa deverá possuir pelo menos 1 (um) Engenheiro apto a prestar serviços de suporte técnico no equipamento proposto. O Engenheiro deverá possuir registro junto ao CREA e certificação no produto comprovada pelo fabricante. 3. Compatibilidade: 3.1 Deve ser obrigatoriamente do mesmo fabricante, compatível e peça original dos Switches de Acesso. Referência: Marca Extreme Network, modelo LR SFP+ Module ou de melhor qualidade. (TCU, Acórdão 2401/2006, 9.3.2 – Plenário). **(COTA RESERVADA ME/EPP/MEI) – VINCULADO AO ITEM 49**	un	15		
68965	51	Transceiver 10GBASE-SR 1. Características Gerais: 1.1 Módulo Transceptor Ótico 10 Gigabit Ethernet para fibra multimodo; 1.2 Formato Hot-Pluggable padrão SFP+; 1.3 Suportar distância de no mínimo 300 metros; 1.4 Conector LC; 2. Garantia: 2.1 O Transceiver deverá possuir garantia do fabricante pelo período mínimo de 12 (doze) meses. 2.2. Nos casos de troca equipamentos defeituosos, os mesmos	un	45		

		devem ser enviados no próximo dia útil subsequente a abertura do chamado e comprovação do defeito, sem quaisquer custos adicionais. 2.3. Os chamados técnicos deverão ser gerenciados pelo fornecedor em horário comercial na modalidade 8x5 (oito horas por dia, cinco dias por semana), através de telefone gratuito. Também deve ser disponibilizado endereço de e-mail para abertura dos chamados técnicos. 2.4 A empresa deverá possuir pelo menos 1 (um) Engenheiro apto a prestar serviços de suporte técnico no equipamento proposto. O Engenheiro deverá possuir registro junto ao CREA e certificação no produto comprovada pelo fabricante. 3. Compatibilidade: 3.1 Deve ser obrigatoriamente do mesmo fabricante, compatível e peça original dos Switches de Acesso. Referência: Marca Extreme Network, modelo SR SFP+ Module ou de melhor qualidade. (TCU, Acórdão 2401/2006, 9.3.2 – Plenário). **(COTA PRINCIPAL)**				
68965	52	Transceiver 10GBASE-SR 1. Características Gerais: 1.1 Módulo Transceptor Ótico 10 Gigabit Ethernet para fibra multimodo; 1.2 Formato Hot-Pluggable padrão SFP+; 1.3 Suportar distância de no mínimo 300 metros; 1.4 Conector LC; 2. Garantia: 2.1 O Transceiver deverá possuir garantia do fabricante pelo período mínimo de 12 (doze) meses. 2.2. Nos casos de troca equipamentos defeituosos, os mesmos devem ser enviados no próximo dia útil subsequente a abertura do chamado e comprovação do defeito, sem quaisquer custos adicionais. 2.3. Os chamados técnicos deverão ser gerenciados pelo fornecedor em horário comercial na modalidade 8x5 (oito horas por dia, cinco dias por semana), através de telefone gratuito. Também deve ser disponibilizado endereço de e-mail para abertura dos chamados técnicos. 2.4 A empresa deverá possuir pelo menos 1 (um) Engenheiro apto a prestar serviços de suporte técnico no equipamento proposto. O Engenheiro deverá possuir registro junto ao CREA e certificação no produto comprovada pelo fabricante. 3. Compatibilidade: 3.1 Deve ser obrigatoriamente do mesmo fabricante, compatível e peça original dos Switches de Acesso. Referência: Marca Extreme Network, modelo SR SFP+ Module ou de melhor qualidade. (TCU, Acórdão 2401/2006, 9.3.2 – Plenário). **(COTA RESERVADA ME/EPP/MEI) – VINCULADO AO ITEM 51**	un	15		
68974	53	Transceiver 40GBASE-SR4, QSFP+, QSFP+ SR4 module 1. Características Gerais: 1.1 Módulo Transceptor Ótico 40 Gigabit Ethernet para fibra multimodo; 1.2 Formato Hot-Pluggable padrão QSFP+; 1.3 Suportar distância de no mínimo 100 metros; 1.4 Conector MPO; 2. Garantia: 2.1 O Transceiver deverá possuir garantia do fabricante pelo período mínimo de 12 (doze) meses. 2.2. Nos casos de troca equipamentos defeituosos, os mesmos devem ser enviados no próximo dia útil subsequente a abertura do chamado e comprovação do defeito, sem quaisquer custos adicionais. 2.3. Os chamados técnicos deverão ser gerenciados pelo fornecedor em horário comercial na modalidade 8x5 (oito horas por dia, cinco dias por semana), através de telefone gratuito. Também deve ser	un	10		

		disponibilizado endereço de e-mail para abertura dos chamados técnicos. 2.4 A empresa deverá possuir pelo menos 1 (um) Engenheiro apto a prestar serviços de suporte técnico no equipamento proposto. O Engenheiro deverá possuir registro junto ao CREA e certificação no produto comprovada pelo fabricante. 3. Compatibilidade: 3.1 Deve ser obrigatoriamente do mesmo fabricante, compatível e peça original dos Switches Distribuição. Referência: Marca Extreme Network, modelo QSFP+ SR4 module ou de melhor qualidade. (TCU, Acórdão 2401/2006, 9.3.2 – Plenário).				
68982	54	Transceiver 40GBASE-SR4, QSFP+ SR4 module 1. Características Gerais: 1.1 Módulo Transceptor Ótico 40 Gigabit Ethernet para fibra multimodo; 1.2 Formato Hot-Pluggable padrão QSFP+; 1.3 Suportar distância de no mínimo 100 metros; 1.4 Conector MPO; 2. Garantia: 2.1 O Transceiver deverá possuir garantia do fabricante pelo período mínimo de 12 (doze) meses. 2.2. Nos casos de troca equipamentos defeituosos, os mesmos devem ser enviados no próximo dia útil subsequente a abertura do chamado e comprovação do defeito, sem quaisquer custos adicionais. 2.3. Os chamados técnicos deverão ser gerenciados pelo fornecedor em horário comercial na modalidade 8x5 (oito horas por dia, cinco dias por semana), através de telefone gratuito. Também deve ser disponibilizado endereço de e-mail para abertura dos chamados técnicos. 2.4 A empresa deverá possuir pelo menos 1 (um) Engenheiro apto a prestar serviços de suporte técnico no equipamento proposto. O Engenheiro deverá possuir registro junto ao CREA e certificação no produto comprovada pelo fabricante. 3. Compatibilidade: 3.1 Deve ser obrigatoriamente do mesmo fabricante, compatível e peça original do Switch Top of Rack. Referência: Marca Extreme Network, modelo QSFP+ SR4 module ou de melhor qualidade. (TCU, Acórdão 2401/2006, 9.3.2 – Plenário).	un	1		

OBSERVAÇÕES

1. Todos os equipamentos deverão ter, no mínimo, **01 (um) ano de garantia**;

   1.1 Para os itens 9, 10, 20, 21, 22, 23, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44 e 45 o período mínimo de garantia deverá ser de 60 (sessenta) meses, conforme descrito no anexo I deste edital.

   1.2 Para o item 46 o período mínimo de garantia deverá ser de 36 (trinta e seis) meses, conforme descrito no anexo I deste edital.

2 **VALIDADE DA ATA SRP:** 12 (doze) meses, a contar do início da vigência da Ata de Registro de Preços;

3 **PRAZO PARA ENTREGA:** até 30 (trinta) dias corridos para nacionais e até 60 (sessenta) dias para importados, contados da data do recebimento da Nota de Empenho.

4 **Havendo divergências entre a descrição do objeto constante no edital e a descrição do objeto constante no SITE COMPRASNET, "SIASG" OU NOTA DE EMPENHO, prevalecerá, sempre, a descrição deste edital.**

5 **(**) -** As indicações de marcas foram usadas como parâmetro de qualidade para facilitar a descrição do objeto a ser licitado, que deverá ser equivalente, similar ou de melhor qualidade. **(TCU, Acórdão 2401/2006, 9.3.2 - Plenário).**

ANEXO II

PREGÃO ELETRÔNICO 110/2015

RAZÃO SOCIAL DA PROPONENTE.....

ENDEREÇO: .....

CIDADE/UF: ..... CEP: .....

CNPJ: ..... e-mail: .....

FONE:..... FAX: .....

REPRESENTANTE LEGAL: .....

CPF: ..... RG: .....

DADOS BANCÁRIOS:

BANCO: .....

AGÊNCIA: ..... CONTA: .....

(Enviar este Anexo pelo correio eletrônico pregao@unifal-mg.edu.br, após a fase de aceitação das propostas, durante a sessão pública)

ANEXO III

PREGÃO ELETRÔNICO Nº 110/2015

MARGEM DE PREFERÊNCIA

Será aplicada margem de preferência, nos termos dos Decretos 7.903/2013, 8.186/2014 e 8.194/2014, para os seguintes itens:

Item	UN	Qtd. Licitada	MARGEM NORMAL (%)	MARGEM ADICIONAL (%)
1	un	1	0	18
2	un	1	0	18
3	un	60	15	10
4	un	30	15	10
5	un	5	15	10
6	un	10	15	10
7	un	1	15	10
8	un	1	15	10
9	un	2	15	10
10	un	2	15	10
11	un	5	15	10
12	un	2	15	10
13	un	50	15	10
14	un	6	15	10
15	tes	3	0	18

16	tes	1	0	18
17	un	2	0	18
18	un	2	0	18
19	un	4	0	18
20	un	19	15	10
21	un	6	15	10
22	un	10	15	10
23	un	25	15	10
24	un	1	0	18
25	un	15	15	10
26	un	5	15	10
27	un	15	15	10
28	un	5	15	10
29	un	38	15	10
30	un	12	15	10
31	un	38	15	10
32	un	12	15	10
33	un	4	15	10
34	un	1	15	10
35	un	1	15	10
36	un	1	15	10
37	un	1	15	10
38	un	1	15	10
39	un	1	15	10
40	un	1	15	10
41	un	1	15	10

42	un	1	15	10
43	un	1	15	10
44	un	38	15	10
45	un	12	15	10
46	un	1	15	10
47	tes	80	15	10
48	un	80	15	10
49	un	45	15	10
50	un	15	15	10
51	un	45	15	10
52	un	15	15	10
53	un	10	15	10
54	un	1	15	10

TERMO DE REFERÊNCIA

Processo: 23087.010345/2015-59

1 OBJETO

1.1 O presente Termo de Referência tem como finalidade o registro de preço para possível aquisição futura de ativos de redes e software de gerenciamento de redes.

2 DISPOSIÇÕES INICIAIS

2.1 As especificações contidas neste Termo de Referência constarão no anexo I do edital, e em nenhum momento serão substituídas pelas descrições resumidas, constantes no Aviso divulgado no sitio www.comprasnet.gov.br. Em caso de divergência nas especificações, prevalecerão as dos Anexos do Edital, dos avisos e esclarecimentos lançados no Comprasnet.

2.2 A proposta de preços deverá ser apresentada em moeda nacional, preços unitários e totais, em algarismo e por extenso, com no máximo 02 casas decimais após a vírgula (ex. R$ 0,01), observando-se as especificações necessárias indicadas no Anexo I do edital, presumindo-se estarem inclusos os encargos que incidem ou venham a incidir sobre o objeto licitado, **incluindo todas as despesas que influam no custo, tais como: impostos, taxas, transportes, entrega no local, seguros, encargos fiscais e todos os ônus diretos.**

2.3 As propostas que apresentem no **"campo descrição detalhada do objeto ofertado"** a informação **"de acordo com o edital"** ou similar **serão consideradas como produto ofertado EXATAMENTE igual ao registrado na especificação do Anexo I do Edital.**

2.4 O critério de julgamento será pelo **menor preço unitário por ITEM.**

3 FUNDAMENTO LEGAL

3.1 A contratação de Pessoa Jurídica para fornecimento dos materiais objeto deste Termo de Referência tem amparo legal na Lei nº 10.520/2002, subsidiada pela Lei nº 8.666/93 e suas alterações, na Lei 8.078/1990, na Lei Complementar 123/2006 e 147/2014, nos Decretos 5.450/2005, 6.204/2007 e 7.892/2013 e suas alterações.

4 ESPECIFICAÇÕES

4.1 Os materiais em referência deverão guardar perfeita compatibilização com as especificações, quantidades e condições descritas no Anexo I do Edital, em nenhum momento poderão ser substituídas pelas descrições resumidas, constantes no Aviso divulgado no sítio www.comprasnet.gov.br.

4.2 As soluções a ser fornecida deverá atender aos requisitos elencados a seguir:

4.2.1 A solução a ser ofertada para cada um dos itens deve ser da marca Extreme Networks, devido a quase totalidade dos ativos de redes instalados na CONTRATANTE ser deste fabricante. O processo de padronização destes equipamentos teve início em 2010, tendo a marca sido adotada por ser a vencedora do certame licitatório realizado na época;

4.2.2 Os itens 3, 4, 5, 6, 7, 8, 11, 12, 20, 21, 22, 23, 47, 48, 49, 50 ,51, 52, 53 e 54 devem ser da marca Extreme Networks ou 100% compatíveis, compatibilidade esta que deve ser comprovada mediante documentação oficial do fabricante;

4.2.3 Todos os itens do certame, exceto os itens 1, 2 e 24 devem ser totalmente compatíveis com a Solução de Gerenciamento NetSight Base 500, já adquirida e em operação na CONTRATANTE;

4.2.4 As **Controladoras Wireless** especificados nos itens 9 e 10, os Pontos de Acesso especificado nos itens 25, 26, 27, 28, 29, 30, 31, 32, 33 e 34 e os injetores dos itens 13 e 14 devem ser totalmente compatíveis com os Access Points Extreme Networks 3715i e 3825e em operação na CONTRATANTE;

4.2.5 Os itens 1, 2 e 24 devem ser totalmente compatíveis com os Switches Extreme Networks Summit 450e, 460 e 480, Pontos de Acesso IdentiFi 3715i e 3825 e Controlador Wireless V2110, em operação na CONTRATANTE.

4.3 A PROPONENTE que oferecer o menor preço deverá apresentar, após solicitação do pregoeiro, a documentação técnica do fabricante do equipamento comprovando o atendimento a todos os requisitos contidos nas "Características técnicas mínimas obrigatórias" do objeto a ser contratado, com o atendimento das seguintes condições:

4.3.1 Não será aceita Carta do Fornecedor/Distribuidor como comprovação de atendimento a características técnicas e de compatibilidade especificados neste termo de referência;

4.3.2 Documentação técnica. Nessa documentação, a PROPONENTE deve fornecer uma planilha ponto-a-ponto indicando documento e página em que consta o cumprimento de cada um dos requisitos das especificações técnicas;

4.3.3 Os documentos devem descrever claramente a referência ao modelo apresentado na proposta, e não serão válidas referências genéricas;

4.3.4 Não serão aceitas referências a futuras atualizações ou versões de produtos para comprovar a existência ou aderência a qualquer quesito desta especificação;

4.3.5 Relação de componentes. Nessa documentação, a PROPONENTE deve fornecer uma lista completa contendo a configuração do equipamento ofertado, incluindo módulos, fontes e acessórios, com as respectivas quantidades de cada item;

4.3.6 A PROPONENTE deve fornecer declaração de que os equipamentos propostos e todos os seus componentes são novos, de primeiro uso e estão em linha de fabricação na data de abertura das propostas;

4.3.7 A PROPONENTE deve fornecer declaração do fabricante de que o equipamento proposto possui a garantia e suporte técnico solicitado no item "Garantia e Suporte" de cada item, conforme descrito no “Anexo I”.

5 JUSTIFICATIVA

5.1 O Núcleo de Tecnologia da Informação, através da Gerência de Redes e Infraestrutura, necessita de aquisição de ativos de redes e de software de gerenciamento de redes, para atenderem as necessidades na oferta de serviços de redes de internet, nos diversos prédios em fase final de construção, ampliação em reformas em prédios já construídos, substituição de switches obsoletos e ampliação e melhoria dos serviços de rede Wi-Fi nos Campi e Unidade II da Universidade Federal de Alfenas – UNIFAL-MG.

6 VALOR DE REFERÊNCIA TOTAL ESTIMADO

6.1 O valor de referência foi baseado em pré-cotações realizadas no mercado, com valor total estimado em **R$ 4.489.377,00 (QUATRO MILHÕES, QUATROCENTOS E OITENTA E NOVE MIL, TREZENTOS E SETENTA E SETE REAIS).**

6.2 Foram utilizados três orçamentos como referência para composição dos preços.

7 DA ENTREGA DO OBJETO

7.1 Local e horário para entrega: Almoxarifado Central da Universidade Federal de Alfenas – UNIFAL-MG, Rua Pio XII, 794 – Centro- Alfenas/MG – CEP 37130-000, das 7h às 10h30 e das 13h às 16h30 horas, em dias úteis.

7.1.1 Será recebido somente nas condições exigidas pelo Edital.

7.2 O prazo de entrega do objeto proposto deverá ser de até 30 (trinta) dias corridos para nacionais e até 60 (sessenta) dias para importados, contados da data do recebimento da Nota de Empenho/Contrato.

8 DA DOTAÇÃO ORÇAMENTARIA

8.1 Os recursos para aquisição dos materiais objeto do presente registro de preços, de acordo com os quantitativos efetivamente contratados, possuem dotação orçamentária própria e serão certificados por ocasião de cada contratação.

8.2 Conforme §2º do art. 7º do Decreto 7.892, de 2013, na licitação para registro de preços não é necessário indicar a dotação orçamentária, que somente será exigida para a formalização do contrato ou outro instrumento hábil.

9 DO PAGAMENTO

9.1 O pagamento será efetuado no prazo máximo de 10 (dez) dias úteis, contados da data do recebimento definitivo e pela apresentação do documento fiscal, desde que atendidas às exigências do Edital e o disposto no item 8.8 da Instrução Normativa nº 05, de 21/07/95, do Ministério da Administração Federal e Reforma do Estado, mediante crédito em Conta corrente bancária da LICITANTE VENCEDORA, através do Banco do Brasil S/A.

9.2 O documento Fiscal terá que ser emitido obrigatoriamente com o número de inscrição no CNPJ apresentado para a Habilitação, não se admitindo documento Fiscal emitido com outro CNPJs, mesmo aqueles de filiais ou matriz.

9.3 Antes de cada pagamento à contratada, será realizada consulta ao SICAF para verificar a manutenção das condições de habilitação exigidas no edital.

9.4 Constatando-se, junto ao SICAF, a situação de irregularidade da contratada, será providenciada sua advertência, por escrito, para que, no prazo de 5 (cinco) dias, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da contratante.

9.5 Não havendo regularização ou sendo a defesa considerada improcedente, a contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência da contratada, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

9.6 Persistindo a irregularidade, a contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada à contratada a ampla defesa.

9.7 Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso a contratada não regularize sua situação junto ao SICAF.

9.8 Considerar-se-á como último dia útil para pagamento, o de emissão da respectiva Ordem Bancária pelo SIAFI (Sistema da administração Financeira do Governo Federal);

9.9 No pagamento serão observadas as retenções, de acordo com a legislação e normas vigentes, no âmbito da União, Estado e Município.

9.10 Poderá ser deduzido do documento Fiscal o valor de multa aplicada.

9.11 Nenhum pagamento será efetuado à LICITANTE VENCEDORA enquanto pendente de liquidação ou qualquer obrigação financeira que lhe for imposta, em virtude de penalidade ou inadimplência.

10 OBRIGAÇÕES DA LICITANTE VENCEDORA

10.1 A LICITANTE VENCEDORA se obriga a atender plenamente o compromisso assumido com a UNIFAL-MG:

10.2 A LICITANTE VENCEDORA é obrigada a pagar todos os tributos, contribuições fiscais e parafiscais que incidem ou venham a incidir, direta ou indiretamente, sobre todos os produtos contratados.

11 OBRIGAÇÕES DA CONTRATANTE

11.1 A UNIFAL-MG obriga-se a:

a) solicitar, o eventual fornecimento dos materiais, cujos preços encontram-se registrados na ARP, sendo considerada 1 (uma) unidade de fornecimento a quantidade mínima para efetuar o pedido;
b) efetuar o pagamento ao fornecedor no valor total, através de nota(s) fiscal(is) dos produtos entregues, se aceitos;
c) observar para que, durante a vigência da ARP, sejam mantidas todas as condições de habilitação e qualificação exigida na licitação, bem como a sua compatibilidade com as obrigações assumidas;
d) efetuar o pagamento em até 10 (dez) dias úteis, contados da apresentação da(s) nota(s) fiscal(is), correspondente(s) ao(s) fornecimento(s) executado(s);
e) acompanhar e fiscalizar a perfeita execução da ARP, através de fiscal(is) designado(s) para tal; e
f) recusar materiais que estejam em desacordo com as especificações dos registrados na ARP.

12 MEDIDAS ACAUTELADORAS

12.1 Consoante o artigo 45 da Lei nº 9.784, de 1999, a Administração Pública poderá, sem a prévia manifestação do interessado, motivadamente, adotar providências acauteladoras, inclusive retendo o pagamento, em caso de risco iminente, como forma de prevenir a ocorrência de dano de difícil ou impossível reparação.

13 DAS SANÇÕES ADMINISTRATIVAS

13.1 Comete infração administrativa, nos termos da Lei nº 10.520, de 2002, o licitante/adjudicatário que:

13.1.1 não aceitar/retirar a nota de empenho, ou não assinar a ata de registro de preço e/ou o termo de contrato, quando convocado dentro do prazo de validade da proposta;

13.1.2 apresentar documentação falsa;

13.1.3 deixar de entregar os documentos exigidos no certame;

13.1.4 ensejar o retardamento da execução do objeto;

13.1.5 não mantiver a proposta;

13.1.6 cometer fraude fiscal;

13.1.7 comportar-se de modo inidôneo;

13.2 Considera-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de participação, quanto ao enquadramento como ME/EPP ou o conluio entre os licitantes, em qualquer momento da licitação, mesmo após o encerramento da fase de lances.

13.3 O licitante/adjudicatário que cometer qualquer das infrações discriminadas no subitem anterior e na forma dos artigos 77 a 80 da Lei 8.666/93, ficará sujeito, sem prejuízo da responsabilidade civil e criminal, garantida a prévia defesa, às seguintes sanções previstas nos artigos 81 a 88 da Lei 8.666/93, artigo 7º da Lei 10.520/02, no artigo 28 do Decreto 5.450/05 e do artigo 14 do Decreto 3.555/00:

13.3.1 Advertência

13.3.2 Multa:

13.3.2.1 Multa de mora no percentual correspondente a 0,5% (zero vírgula cinco por cento), calculada sobre o valor remanescente do contrato, por dia de inadimplência, até o limite de 15 (quinze) dias úteis de atraso na entrega do material caracterizando inexecução parcial; e

13.3.2.2 Compensatória no valor de 10% (dez por cento), sobre o valor remanescente do contrato.

13.3.3 Suspensão temporária de participação em licitação com a Administração;

13.3.4 Impedimento de licitar e contratar no âmbito da União;

13.3.5 Declaração de inidoneidade.

13.4 A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa ao licitante/adjudicatário, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente na Lei nº 9.784, de 1999.

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

13.6 As penalidades serão obrigatoriamente registradas no SICAF.

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DE ALFENAS - UNIFAL-MG
SETOR DE COMPRAS
Rua Gabriel Monteiro da Silva, 700 - Alfenas/MG - CEP 37130-000.
Fone: (35) 3299-1072/1070 - Fax: (35) 3299-1071 - compras@unifal-mg.edu.br

ATA DE REGISTRO DE PREÇOS N° 00

PROCESSO Nº 23087.010345/2015-59

PREGÃO ELETRÔNICO Nº 110/2015

AOS _____ DIAS DO MÊS DE _____ DE 2015, A UNIVERSIDADE FEDERAL DE ALFENAS – UNIFAL-MG, AUTARQUIA DE REGIME ESPECIAL, "EX VI" DA LEI Nº 11.154, DE 29 DE JULHO DE 2005, POR MEIO DA REITORIA DA UNIVERSIDADE FEDERAL DE ALFENAS – UNIFAL - MG, LAVRA A PRESENTE ATA DE REGISTRO DE PREÇOS (ARP), REFERENTE AO PROCESSO LICITATÓRIO - PREGÃO ELETRÔNICO Nº 110/2015, QUE OBJETIVA O FORNECIMENTO FUTURO DE ATIVOS DE REDES E SOFTWARE DE GERENCIAMENTO DE REDES, SEGUNDO OS PREÇOS, QUANTITATIVOS E FORNECEDORES DEFINIDOS NA LICITAÇÃO SUPRA, BEM COMO OBSERVADAS AS CLÁUSULAS E CONDIÇÕES ABAIXO ESTABELECIDAS, CONSTITUINDO-SE ESTA, EM DOCUMENTO VINCULADO E OBRIGACIONAL ÀS PARTES, À LUZ DAS REGRAS INSERTAS NO DECRETO Nº 7.892 DE 23/01/2013:

CLÁUSULA PRIMEIRA - DA VINCULAÇÃO AO EDITAL

A presente ATA DE REGISTRO DE PREÇOS, vincula-se às regras dispostas no Edital de Licitação nº 110/2015 – modalidade Pregão Eletrônico e seus Anexos.

CLÁUSULA SEGUNDA - DA DELEGAÇÃO DE COMPETÊNCIA E ASSINATURAS DE ATA

De acordo com as normas aprovadas pela Portaria nº 1.002 de 16 de julho de 2010, publicada no D.O.U., dia 19 de julho de 2010, página 27, Seção 1, delegando a Pró-Reitora de Administração e Finanças da UNIVERSIDADE FEDERAL DE ALFENAS – UNIFAL-MG, a competência para assinar esta ARP em nome do REITOR.

A presente Ata será firmada pela UNIFAL-MG e a empresa _____, inscrita no CNPJ sob o nº _____, classificada no processo licitatório do SRP.

CLÁUSULA TERCEIRA - DO OBJETO

Fornecimento futuro de ativos de redes e software de gerenciamento de redes, para os Campi da UNIFAL-MG, conforme descrito na Cláusula Décima Segunda desta ARP, por um período de doze (12) meses, a contar da data da formalização desta ARP.

CLÁUSULA QUARTA – DAS OBRIGAÇÕES DA UNIFAL-MG

A UNIFAL-MG obriga-se a:

a) solicitar, o eventual fornecimento dos materiais, cujos preços encontram-se registrados na presente ARP, sendo considerada 1 (uma) unidade de fornecimento a quantidade mínima para efetuar o pedido;

b) efetuar o pagamento ao fornecedor no valor total, através de nota(s) fiscal(is) dos produtos entregues, se aceitos;

c) observar para que, durante a vigência da ARP, sejam mantidas todas as condições de habilitação e qualificação exigida na licitação, bem como a sua compatibilidade com as obrigações assumidas;

d) efetuar o pagamento em até 10 (dez) dias úteis, contados da apresentação da(s) nota(s) fiscal(is), correspondente(s) ao(s) fornecimento(s) executado(s), conforme previsto no item 26 do Edital de Licitação;

e) acompanhar e fiscalizar a perfeita execução da presente ARP, através de fiscal(is) designado(s) para tal; e

f) recusar materiais que estejam em desacordo com as especificações dos registrados nesta ARP.

CLÁUSULA QUINTA – DAS OBRIGAÇÕES DO FORNECEDOR REGISTRADO

O FORNECEDOR REGISTRADO obriga-se a:

a) manter, durante a vigência contratual, todas as condições demonstradas para habilitação na licitação efetuada, de modo a garantir o cumprimento das obrigações assumidas;

b) acusar o recebimento do pedido dos materiais , através de fac-símile ou assinatura na cópia do pedido de material caso o mesmo seja entregue "em mão";

c) fornecer os materiais solicitados no prazo máximo de até 30 (trinta) dias corridos para nacionais e até 60 (sessenta) dias para importados, conforme edital, contadas do recebimento do Empenho;

d) fornecer os materiais conforme especificações, marcas e preços indicados na licitação supracitada registrados nesta ARP;

e) obedecer aos requisitos mínimos de qualidade, conforme a licitação supracitada;

f) providenciar no prazo de 3 (três) dias, a imediata correção das deficiências, falhas ou irregularidades constatadas pelo responsável por seu recebimento, no cumprimento das obrigações assumidas nesta ARP;

g) prover e manter condições que possibilitem o atendimento das demandas previstas firmadas a partir da data da assinatura da presente ARP;

h) caso haja necessidade, assente ao que preceitua o § 1º, art. 65, da Lei nº 8.666/1993, aceitar o acréscimo de até 25% nos quantitativos que se fizerem necessários, sempre nas mesmas condições registradas. As supressões não estão adstritas ao limite citado;

i) ressarcir os eventuais prejuízos causados à UNIFAL-MG e/ou a terceiros, provocados por ineficiência ou irregularidade cometidas na execução das obrigações assumidas na presente ARP;

j) responsabilizar-se por todas as despesas diretas ou indiretas, tais como: salários, transportes, encargos sociais, fiscais, trabalhistas, previdenciários e de ordem de classe, indenizações, e quaisquer outras que forem devidas ao(s) seu(s) empregado(s), no desempenho dos serviços referentes à execução do objeto, ficando, ainda, a UNIFAL-MG isenta de qualquer vínculo empregatício, responsabilidade solidária ou subsidiária;

l) pagar pontualmente, seus fornecedores e suas obrigações fiscais, relativas ao material fornecido, com base na presente ARP, exonerando a UNIFAL-MG de responsabilidade solidária ou subsidiária por tal pagamento;

m) substituir, às suas expensas, no total ou em parte, os itens do objeto em que se verificarem vícios, defeitos ou incorreções resultantes da fabricação, de seus lacres ou embalagens; e

n) arcar com todas as despesas operacionais, incluindo despesas de transporte e entregas necessárias ao fornecimento do objeto.

CLÁUSULA SEXTA – DO PRAZO DE VALIDADE

O prazo de validade do presente Registro de Preços é de 12 (doze) meses, a partir do registro da homologação no sitio do Comprasnet e no Sistema SIASG, podendo ser registrado uma única data de vigência para todos os itens da licitação ou uma data para cada item homologado.

CLÁUSULA SÉTIMA – DOS RECURSOS ORÇAMENTÁRIOS

As despesas para atender ao objeto desta licitação correrão à conta do Orçamento Geral da União.

CLÁUSULA OITAVA – DO PREÇO

O preço para o objeto desta presente Ata de Registro de Preços importa na quantia especificada e detalhada na Cláusula Décima Segunda, correspondente ao valor unitário do objeto.

CLÁUSULA NONA – DO PAGAMENTO

O pagamento será efetuado, conforme descrito na Cláusula Quarta, alíneas c, d e e, desta ARP, após o aceite por parte do servidor responsável pela fiscalização.

CLÁUSULA DÉCIMA – DO LOCAL E HORÁRIO PARA ENTREGA DO OBJETO

Condições de Entrega:

a) o prazo para entrega do(s) material(is) será de até 30 (trinta) dias corridos para nacionais e até 60 (sessenta) dias para importados, a contar do recebimento do Pedido de Material(is);

b) a solicitação de material(is), será formalizada através da entrega do Empenho, numerado, datado, assinado pelo Ordenador de Despesa e Gestor Financeiro, ou o seu envio por fac-símile, a ser providenciada pela Universidade Federal de Alfenas – UNIFAL-MG;

c) os locais de entrega dos materiais serão;

- **Órgão Gerenciador: UASG 153028 -** Almoxarifado Central da Universidade Federal de Alfenas – UNIFAL-MG, Rua Pio XII, 794 – Centro- Alfenas/MG – CEP 37130-000, das 7h às 10h30 e das 13h às 16h30 horas, em dias úteis

d) todos os itens deverão ser transportados e acondicionados em meio de transporte e embalagens apropriados para cada tipo de material;

e) somente serão aceitos os produtos cujos prazos de validade tenham, no mínimo, 80% de validade no ato da entrega; e

f) o transporte dos itens até o local de entrega é de responsabilidade exclusiva da Empresa CONTRATADA.

CLÁUSULA DÉCIMA PRIMEIRA - DA FISCALIZAÇÃO

A fiscalização desta ARP será exercida pelo(s) servidor(es) designado(s) para o serviço de fiscalização e conferência, que terão plenos poderes para:

a) recusar material(is) em desacordo com o objeto;
b) promover as medidas que couberem para os casos amparados pelas cláusulas descritas nesta ARP; e
c) exigir da CONTRATADA a retirada e ou troca imediata de qualquer dos produtos que não estejam em conformidade com os requisitos exigidos e previstos nesta Ata de Registro de Preços ou no Edital.

CLÁUSULA DÉCIMA SEGUNDA - PREÇO, QUANTITATIVOS e ESPECIFICAÇÕES

O preço registrado, a quantidade, o fornecimento e as especificações dos materiais constantes deste Registro, encontram-se contidos na tabela abaixo e serão adquiridos e pagos conforme previsto no item 26 do Edital de Licitação e Cláusula Nona desta ARP:

Item	Descrição	Unidade	Quantidade	Valor Unitário

Marca:
Fabricante:

Subcláusula Primeira
As marcas, fabricantes e modelos registrados nesta Ata são as mesmas constantes das propostas ofertadas no Portal Compras Governamentais.

Subcláusula Segunda
O preço e fornecedor ora registrados observam a classificação final obtida no procedimento licitatório sobredito, o qual fora processado em estrita vinculação aos critérios estabelecidos no instrumento convocatório de tal certame.

Subcláusula Terceira

A Administração poderá contratar, de forma concomitante, dois ou mais fornecedores que tenham seus preços registrados, observado o limite e a capacidade de fornecimento particular.

CLÁUSULA DÉCIMA TERCEIRA – DA EXECUÇÃO DO PAGAMENTO

O pagamento será realizado através de depósito bancário em até 10 (dez) dias úteis, contados da apresentação da(s) nota(s) fiscal(is), desde que conste o atesto do recebimento definitivo, correspondente(s) ao(s) fornecimento(s) executado(s), conforme previsto no item 26 do Edital de Licitação, salvo por atraso na liberação de recursos financeiros, desde que o(s) adjudicatário(s):
a) esteja(m) em dia com as obrigações previdenciárias (INSS) e trabalhistas (FGTS);
b) da consulta ao Sistema de Cadastramento Unificado de Fornecedores (SICAF); e
c) Nota(s) Fiscail(s) que indique(m) o número do banco, da agência e da conta corrente (PESSOA JURÍDICA), na qual será realizado o crédito;
e) CNDT.

Subcláusula única
O pagamento será condicionado ao atesto no respectivo documento fiscal, pelo responsável pelo recebimento do material (Chefe do Almoxarifado).
Do montante a ser pago ao contratado, incidirá retenção tributária no percentual de que dispõe a Instrução Normativa SRF nº 480/2004, ou normatização que vier a lhe substituir, nos termos do que dispõe o art. 64 da Lei nº 9.430/96.

CLÁUSULA DÉCIMA QUARTA - DA EXISTÊNCIA DA ATA DE REGISTRO DE PREÇOS

A existência desta ARP não obriga a Administração a firmar as respectivas contratações, facultando-se-lhe a realização de procedimento específico para determinada aquisição, sendo assegurado ao beneficiário deste registro à preferência de fornecimento, em igualdade de condições.

CLÁUSULA DÉCIMA QUINTA - DA CONTRATAÇÃO

A contratação junto a cada fornecedor registrado será formalizada, por intermédio de emissão de Nota de Empenho.

CLÁUSULA DÉCIMA SEXTA - DA REVISÃO DE PREÇO

A qualquer tempo, o preço registrado poderá ser revisto em decorrência de **eventual redução** daqueles praticados no mercado, cabendo à Universidade Federal de Alfenas a convocação do fornecedor registrado para negociar o novo valor.

CLÁUSULA DÉCIMA SÉTIMA - DO CANCELAMENTO DE REGISTRO DE FORNECEDOR

O fornecedor terá seu registro cancelado:

I – Por iniciativa da Administração, quando:

a) não cumprir às exigências do instrumento convocatório que deu origem ao registro de preços, bem como as condições da presente ARP;

b) não formalizar contrato decorrente desta ARP ou não atender ao pedido de material no prazo estabelecido, salvo por motivo devidamente justificado e aceito pela Administração;

c) der causa a rescisão administrativa da contratação decorrente deste ARP;

d) em qualquer das hipóteses de inexecução total ou parcial desta presente ARP;

e) não aceitar a redução do preço registrado, na hipótese prevista na legislação; e

f) em face de razões de interesse público, devidamente justificado.

II – Por iniciativa do próprio fornecedor, quando mediante solicitação por escrito, comprovar a impossibilidade do cumprimento das exigências do instrumento convocatório que deu origem a esta ARP, tendo em vista fato superveniente e aceito pela Universidade Federal de Alfenas.

Subcláusula Primeira

A comunicação do cancelamento de preços registrados, nos casos previstos no inciso I desta Cláusula, será efetuada por correspondência com aviso de recebimento, para que o mesmo seja juntado aos autos que deram origem à presente Ata.

CLÁUSULA DÉCIMA OITAVA – DOS CASOS FORTUITOS OU DE FORÇA MAIOR

Serão considerados casos fortuitos ou de força maior, para efeito de não aplicação de multas, o inadimplemento decorrente de:

a) greve geral;

b) calamidade pública;

c) interrupção dos meios de transportes;

d) condições meteorológicas excepcionalmente prejudiciais; e

e) outros casos que se enquadrem no parágrafo único do art. 393 do Código Civil Brasileiro

Subcláusula Primeira

Os casos acima enumerados devem ser satisfatoriamente justificados pela CONTRATADA perante a Universidade Federal de Alfenas.

Subcláusula Segunda

Sempre que ocorrerem situações que impliquem caso fortuito ou de força maior, o fato deverá ser comunicado à Universidade Federal de Alfenas, até 24 horas após a ocorrência. Caso não seja cumprido este prazo, o início da ocorrência será considerado 24 horas antes da data de solicitação de enquadramento da ocorrência como caso fortuito ou de força maior.

Subcláusula Terceira

A comunicação por escrito, relativa ao início da ocorrência deverá conter, entre outras, as seguintes informações:

a) descrição detalhada da ocorrência;

b) causa (s) determinante (s) da ocorrência;

c) item da ARP em que se enquadraria a ocorrência;

d) estudo sintético sobre a possível repercussão da ocorrência no cumprimento do evento;

e) sugestões sobre possíveis providências, quando for o caso, a serem tomadas pela Universidade Federal de Alfenas para fazer cessar a ocorrência e/ou diminuir seu período de duração;

f) Providências tomadas pela CONTRATADA para fazer cessar a ocorrência ou minorar seus efeitos devidamente documentados.

Subcláusula Quarta

Cessados os casos ou fatos citados nesta Cláusula, a CONTRATADA deverá, no menor prazo possível, prosseguir no cumprimento do objeto, envidando todos os esforços para manter o prazo de execução estabelecido.

CLÁUSULA DÉCIMA NONA - DAS SANÇÕES ADMINISTRATIVAS

Subcláusula Primeira - Dos casos passíveis de penalização e multa

Ressalvados os casos fortuitos ou de força maior, devidamente comprovados e conforme parágrafo único do artigo 393 do Código Civil, as EMPRESAS LICITANTES estarão sujeitas às penalidades e multas, sem prejuízo das demais sanções legais, garantida a prévia defesa no respectivo processo, em decorrência das seguintes hipóteses:

a) comportar-se de modo inidôneo;

b) ensejar o retardamento da execução do certame;

c) recusa ou atraso injustificado em executar, total ou parcialmente, as Notas de Empenho de Despesas, Ordens de Compra, assinadas pelo Ordenador de Despesa da UNIFAL-MG, os Contratos decorrentes ou em retirar o instrumento substitutivo, quando convocado para tal; e

d) deixar de entregar ou apresentar documentação e fizer declaração falsa ou cometer fraude fiscal;

Subcláusula Segunda - Das penalidades

Em qualquer uma das hipóteses antes elevadas, estará o faltoso sujeito às seguintes sanções:

a) advertência;

b) multa;

c) suspensão temporária do direito de participar em licitação e impedimento de contratar com a Universidade Federal de Alfenas, por prazo não superior a cinco (5) anos, conforme o art. 7º do Lei nº 10.520, de 17/07/2002; e

d) declaração de inidoneidade para licitar ou contratar com a Administração Pública Federal, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação, perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a EMPRESA CONTRATADA ressarcir a Universidade Federal de Alfenas pelos prejuízos resultantes e depois de decorrido o prazo da sanção aplicada.

Subcláusula Terceira - Da aplicação das penalidades

As penalidades serão aplicadas administrativamente, independentemente de interpelação judicial ou extrajudicial.

Subcláusula Quarta - Das multas

As multas impostas a EMPRESA CONTRATADA serão descontadas dos pagamentos eventualmente devidos, ou ainda, quando for o caso, cobradas judicialmente.

Subcláusula Quinta - Da aplicação das multas

Incorrendo a EMPRESA LICITANTE em qualquer uma das hipóteses descritas nas alíneas a, b, c, e d da Subcláusula Primeira será sancionada as seguintes multas:

a) De mora no percentual correspondente a 0,5% (zero vírgula cinco por cento), calculada sobre o valor total da contratação, por dia de inadimplência, até o limite de 15 (quinze) dias úteis de atraso entrega do material, caracterizando inexecução parcial; e

b) Compensatória no valor de 10% (dez por cento), sobre o valor contratado.

Subcláusula Sexta - Da cumulatividade

A aplicação da penalidade "multa" não impede que seja rescindida unilateralmente a Ata e sejam aplicadas, cumulativamente, as sanções previstas na Subcláusula Segunda, alíneas c e d.

Subcláusula Sétima - Da extensão das penalidades

As sanções dispostas nas alíneas c e d da Subcláusula Segunda poderão ser também aplicadas àqueles que, em razão dos contratos regidos pela Lei nº 8.666/1993:

a) tenham sofrido condenação definitiva por praticarem, por meios dolosos, fraude fiscal no recolhimento de quaisquer tributos;

b) tenham praticado atos ilícitos visando frustrar aos objetivos da licitação; e

c) demonstrem não possuir idoneidade para contratar com a Administração Pública, em virtude de atos ilícitos praticados.

Subcláusula Oitava

Deverá ser observado o princípio do Devido Processo Legal na hipótese de aplicação das penalidades nesta Cláusula.

CLÁUSULA VIGÉSIMA - DOS MOTIVOS DE RECISÃO

Constituem motivos para a UNIVERSIDADE FEDERAL DE ALFENAS rescindir a presente ARP, independentemente de procedimento judicial:

a) não cumprimento de cláusula, subcláusula, inciso, alínea ou prazos constantes desta ARP;

b) cumprimento irregular de cláusula, subcláusula, inciso, alínea ou prazos constantes desta ARP;

c) lentidão no cumprimento desta ARP, levando a Universidade Federal de Alfenas a presumir sua não conclusão dos prazos nele estabelecidos;

d) atraso injustificado do início da execução do objeto desta ARP;

e) paralisação da execução do objeto desta ARP, sem justa causa e prévia comunicação à Universidade Federal de Alfenas;

f) a subcontratação total ou parcial do seu objeto, a associação do contrato com outrem, ou ainda a cessão ou transferência, total ou parcial, bem como a fusão, cisão ou incorporação, não admitidas no Edital e nesta ARP;

g) desatendimento das determinações regulares da autoridade designada para fiscalizar a execução do objeto, assim como a de seus superiores;

h) cometimento reiterado de faltas na execução desta ARP, anotadas na forma do § 1°, art. 67, da Lei n° 8.666/1993;

i) decretação de falência;

j) dissolução da sociedade;

k) alteração social ou a modificação da finalidade ou da estrutura da empresa que, a juízo da Universidade Federal de Alfenas, prejudique a execução desta ARP;

l) quando houver razões de interesse público, de alta relevância e amplo conhecimento, justificadas e determinadas pelo Reitor da Universidade Federal de Alfenas e exaradas no processo administrativo a que se refere esta ARP; e

m) a ocorrência de caso fortuito ou de força maior, regularmente comprovado, impeditivo da execução desta ARP.

Subcláusula Primeira

Os casos de rescisão serão formalmente motivados nos autos do processo, assegurado o direito ao contraditório e à ampla defesa.

Subcláusula Segunda

Fica assegurado à CONTRATADA, no caso de rescisão da presente Ata de Registro de Preço por ato unilateral da Universidade Federal de Alfenas, nas hipóteses previstas neste inciso, a defesa prévia no prazo de dez (10) dias da abertura de vista.

Subcláusula Terceira

Se a presente ARP for rescindida, o Termo de Rescisão deverá discriminar:

a) balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;

b) relação dos pagamentos já efetuados ou ainda devidos; e

c) indenizações e multas.

CLÁUSULA VIGÉSIMA PRIMEIRA - DAS DIVERGÊNCIAS E FORO

Para resolver as divergências entre as partes, oriundas da execução do presente acordo, fica eleito o FORO da Justiça Federal da Cidade de Varginha-MG.

CLÁUSULA VIGÉSIMA SEGUNDA - DOS ORIGINAIS, EXTRATO E CÓPIAS

Da presente Ata, são extraídos os seguintes exemplares:

a) um original, para a UNIVERSIDADE FEDERAL DE ALFENAS;

b) um original, para a CONTRATADA;

E por assim acordarem, as partes declaram aceitar todas as disposições estabelecidas nesta Ata de Registro de Preços que, lida e achadas conforme, vai assinada pelos representantes e testemunhas a seguir, a todo o ato presentes.

Alfenas, _____ de _____ de 2015.

Helena Maria dos Santos Couto
Pró-Reitora Adjunta de Administração e Finanças
Universidade Federal de Alfenas – UNIFAL-MG

Assinatura do Representante legal da Empresa

CPF:
RG:

Testemunha
CPF:

Testemunha
CPF:

MINUTA DE CONTRATO Nº /2016

MINUTA DO CONTRATO DE AQUISIÇÃO DE MATERIAL PERMANENTE, QUE ENTRE SI CELEBRAM A **UNIVERSIDADE FEDERAL DE ALFENAS – UNIFAL-MG** E A EMPRESA **_____**, NOS TERMOS QUE SEGUEM:

A **UNIVERSIDADE FEDERAL DE ALFENAS – UNIFAL-MG**, Autarquia de Regime Especial, de acordo com a Lei 11.154, de 29 de julho de 2005, publicada no DOU de 1°-8-2005, com sede na cidade de Alfenas-MG, na Rua Gabriel Monteiro da Silva, 700, inscrita no C.N.P.J sob o n° 17.879.859/0001-15 neste ato representada pelo **Prof. Paulo Márcio de Faria e Silva,** nomeado Reitor pelo Decreto de 13 de março de 2014 da Presidenta da República, publicado no DOU de 14 de março de 2014, Página 1, Seção 2, denominada **CONTRATANTE**, e a empresa _____, inscrita no CNPJ sob o nº : __, com sede em _____, na Rua _____- CEP: _____, neste ato representada por **_____,** portador do CPF nº _____ e RG: _____ - SSP/___, doravante denominada **CONTRATADA**, tendo em vista o Processo nº 23087.010345/2015-59, celebram o presente Contrato, submetendo-se as partes à Lei nº 10.520 de 17/07/2002, Lei Complementar 123 de 14/12/2006, Lei 11.488, de 15/06/2007, da Lei Complementar 147 de 07 de agosto de 2014, do Decreto nº 5.450 de 31/05/2005, do Decreto nº 6.204 de 05/09/2007 e do Decreto nº 7.892 de 23/01/2013, Decreto nº 7.174 de 12 de maio de 2010, Decreto 7.546, de 02 de agosto de 2011, Decreto 7.903, de 04 de fevereiro de 2013, Decreto nº 8.186 de 17 de janeiro de 2014, Decreto 8.194, de 12 de fevereiro de 2014, da Instrução Normativa nº 01, da SLTI/MPOG, de 19/01/2010, da Instrução Normativa nº 02, da SLTI/MPOG, de 16/09/2009, da Instrução Normativa nº 05, da SLTI/MPOG, de 27/06/2014 e da Lei nº 8.666 de 21/06/1993 em sua redação atual e pelas condições previstas no Edital e no presente contrato, a seguir estabelecidas:

CLÁUSULA PRIMEIRA - DO OBJETO

O objeto deste Contrato é a aquisição de ativos de redes e software de gerencimento de redes, para atender as necessidades das unidades da Universidade Federal de Alfenas – UNIFAL-MG, conforme descrição detalhada no Anexo I do Edital do Pregão Eletrônico nº 110/2015, Sistema de Registro de Preços e na proposta da **CONTRATADA**:

Item	**Descrição**	**Unid**	**Quant**	**Valor Unitário (R$)**	**Valor Total (R$)**
		Un		R$	R$

CLÁUSULA SEGUNDA - DA LICITAÇÃO

O fornecimento a que se refere este Contrato foi objeto da licitação, na modalidade Pregão Eletrônico nº 110/2015, Sistema de Registro de Preços, sendo que a proposta da **CONTRATADA**, o Edital de Licitação e seus anexos passam a fazer parte integrante deste Contrato, independentemente de suas transcrições.

CLÁUSULA TERCEIRA - DO PRAZO DE ENTREGA

O prazo de entrega dos materiais pela **CONTRATADA** será de até 30 (trinta) dias corridos para nacionais e até 60 (sessenta) dias para importados, contados da data do recebimento da nota de empenho.

CLÁUSULA QUARTA - DO RECEBIMENTO

1. Locais e horários para entrega:

1.1 Orgão Gerenciador: UASG 153028 - no Almoxarifado Central da Universidade Federal de Alfenas – UNIFAL-MG, Rua Pio XII, 794 – Centro – Alfenas/MG – CEP 37130-000, das 7h às 10h30 e das 13h às 16h30 horas, em dias úteis, e, será recebido:

1.2 Provisoriamente: Será recebido pelo Almoxarifado Central da Universidade Federal de Alfenas – UNIFAL-MG, sem a verificação do conteúdo (quando embalados) apenas verificando a quantidade de volumes constante na NF-E - Nota Fiscal Eletrônica/Danfe, no ato do recebimento do material para efeito de posterior verificação de conformidade do material com as especificações constantes do edital e seus anexos, mediante a emissão do Termo de Recebimento Provisório, desde que:

1.2.1 esteja compatível com os critérios estabelecidos na Licitação e não exista cobrança de frete;

1.2.2 Estejam os produtos embalados de acordo com a nota fiscal/empenho, não enviando materiais/produtos de notas fiscais/empenhos diferentes numa mesma embalagem;

1.2.3 não apresente avaria ou adulteração;

1.3.4 seja o material da mesma marca e modelo oferecido na proposta inicial, possua as mesmas características da amostra enviada, sob pena de devolução;

1.2.5 Seja entregue em embalagem original, contendo a data e número do lote de fabricação, informando, inclusive, seu prazo de validade;

1.2.5.1 Serão aceitos somente os produtos cujos prazos de validade tenham, no mínimo, 80% de validade no ato da entrega.

1.2.6 Esteja identificado quanto ao número da licitação, nome da Empresa, número do item a que se refere e outras informações de acordo com a legislação pertinente;

1.2.7 Estejam os materiais embalados de acordo com a nota fiscal/empenho, não enviando materiais diferentes numa mesma embalagem.

1.3 Definitivamente: Pelo requisitante, após o decurso do prazo de observação ou vistoria da quantidade e qualidade dos materiais fornecidos que comprove a adequação do objeto aos termos exigidos, mediante emissão de Termo de Recebimento Definitivo.

1.3.1 Após o recebimento dos materiais, mesmo que definitivamente, se, a qualquer tempo, durante a sua utilização normal, vier a se constatar discrepância com as especificações, proceder-se-á a imediata substituição dos mesmos, com ônus por exclusiva responsabilidade e custo da adjudicatária.

CLÁUSULA QUINTA – DO VALOR

Pelo fornecimento do objeto contratual, a **CONTRATANTE** pagará à **CONTRATADA** o valor de R$ ____ (___), fixo e irreajustável, conforme proposta anexa ao Edital do Pregão Eletrônico nº 110/2015, sendo que neste valor já estão incluídas todas as despesas necessárias, tais como frete, impostos, suporte técnico, incluindo a substituição de materiais defeituosos e quaisquer outros que incidam ou venham a incidir sobre o objeto deste Contrato.

CLÁUSULA SEXTA - DA VIGÊNCIA

A vigência do Contrato será de 12 (doze) meses, contados a partir de sua assinatura.

CLÁUSULA SÉTIMA – DO PAGAMENTO

1. O documento Fiscal terá que ser emitido obrigatoriamente com o número de inscrição no CNPJ apresentado para a Habilitação, não se admitindo documento Fiscal emitido com outros CNPJs, mesmo aqueles de filiais ou matriz;

2. O pagamento será efetuado no prazo máximo de 10 (dez) dias úteis, contados da data do recebimento definitivo e pela apresentação do documento fiscal, desde que atendidas as exigências deste Edital e o disposto no item 8.8 da Instrução Normativa nº 05, de 21/07/95, do Ministério da Administração Federal e Reforma do Estado, mediante crédito em Conta corrente bancária da **CONTRATADA**, através do Banco do Brasil S/A;

3. Conforme disposto no item 8.8 da Instrução Normativa nº 05, de 21/07/95, do Ministério da Administração Federal e Reforma do Estado, a UNIFAL-MG consultará junto ao SICAF (Sistema de Cadastramento Unificado de Fornecedores) a regularidade fiscal da **CONTRATADA**;

4. Considerar-se-á como último dia útil para pagamento, o de emissão da respectiva Ordem Bancária pelo SIAFI (Sistema da administração Financeira do Governo Federal);

5. No pagamento serão observadas as retenções, de acordo com a legislação e normas vigentes, no âmbito da União, Estado e Município;

6. Poderá ser deduzido do documento Fiscal o valor de multa aplicada;

7. Nenhum pagamento será efetuado à **CONTRATADA** enquanto pendente de liquidação ou qualquer obrigação financeira que lhe for imposta, em virtude de penalidade ou inadimplência.

8. Nos casos de eventuais atrasos de pagamento, desde que a Contratada não tenha concorrido, de alguma forma, para tanto, fica convencionado que a taxa de compensação financeira devida pela Contratante, entre a data do vencimento e o efetivo adimplemento da parcela, é calculada mediante a aplicação da seguinte fórmula:

EM = I x N x VP, sendo:

EM = Encargos moratórios;

N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;

VP = Valor da parcela a ser paga.

I = Índice de compensação financeira = 0,00016438, assim apurado:

I = (TX) I = (6/100) I = 0,00016438

365 TX = Percentual da taxa anual = 6%.

CLÁUSULA OITAVA – OBRIGAÇÕES DA CONTRATADA

1. A **CONTRATADA** se obriga a atender plenamente o compromisso assumido com a UNIFAL-MG;

2. Serão de responsabilidade da **CONTRATADA** todos os custos decorrentes do transporte dos materiais até a entrega definitiva na UNIFAL-MG;

3. Proceder à entrega dos materiais, devidamente embalado, de forma a não ser danificado durante a operação de transporte e de carga e descarga;

4. Responder por todos os ônus referentes a entrega do bem ora contratado;

5. A **CONTRATADA** deverá garantir o objeto deste contrato, por um período mínimo de 01 (um) ano a contar do recebimento definitivo do material, sendo que as despesas de quaisquer natureza que ocorrer serão por conta da **CONTRATADA**;

5.1 Para os itens 9, 10, 20, 21, 22, 23, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44 e 45 o período mínimo de garantia deverá ser de 60 (sessenta) meses, conforme descrito no anexo I do edital.

5.2 Para o item 46 o período mínimo de garantia deverá ser de 36 (trinta e seis) meses, conforme descrito no anexo I do edital.

6. A **CONTRATADA** ficará obrigada a efetuar a troca do material caso apresente qualquer vício ou defeito de fabricação ou decorrente do transporte inadequado**;**

7. substituir, às suas expensas, no total ou em parte, os itens do objeto em que se verificarem vícios, defeitos ou incorreções resultantes da fabricação, de seus lacres ou embalagens;

8. arcar com todas as despesas operacionais, incluindo despesas de transporte e entregas necessárias ao fornecimento do objeto.

9. Responsabilizar-se por todas as despesas diretas ou indiretas, tais como: salários, transportes, encargos sociais, fiscais, trabalhistas, previdenciários e de ordem de classe, indenizações, e quaisquer outras que forem devidas ao(s) seu(s) empregado(s), no desempenho dos serviços referentes à execução do objeto, ficando, ainda, a UNIFAL-MG isenta de qualquer vínculo empregatício, responsabilidade solidária ou subsidiária;

10. Pagar pontualmente, seus fornecedores e suas obrigações fiscais, relativas ao material fornecido, exonerando a UNIFAL-MG de responsabilidade solidária ou subsidiária por tal pagamento;

11. As despesas com o transporte (ida e volta) do equipamento defeituoso, dentro do prazo de garantia, será de responsabilidade da proponente ou do fabricante;

12. Fornecer os materiais, nas quantidades solicitadas na Nota de Empenho e em conformidade com as especificações contidas neste Contrato, no Edital e Anexos;

13. Sujeitar-se à mais ampla e irrestrita fiscalização por parte do servidor autorizado pela Universidade Federal de Alfenas – UNIFAL-MG, encarregado de acompanhar a execução do Contrato, prestando todos os esclarecimentos que lhes forem solicitados e atendendo às reclamações formuladas;

14. A **CONTRATADA** é obrigada a pagar todos os tributos, contribuições fiscais e parafiscais que incidem ou venham a incidir, direta ou indiretamente, sobre o material adquirido;

15. A **CONTRATADA** deverá manter os documentos de cadastramento no SICAF em pleno vigor, pelo período de execução do contrato;

16. Comunicar à Universidade Federal de Alfenas – UNIFAL-MG, por escrito, no prazo de 10 (dez) dias úteis, quaisquer alterações ocorridas no Contrato Social, durante o prazo de vigência do Contrato de fornecimento, bem como apresentar documentos comprobatórios.

17. A **CONTRATADA** é responsável pelos danos causados diretamente à Administração ou a terceiros, decorrente de sua culpa ou dolo, na execução do contrato, não excluindo esta responsabilidade a fiscalização ou o acompanhamento pela UNIFAL-MG;

18. A **CONTRATADA** se obriga a cumprir plenamente o previsto no artigo 71 e as demais obrigações contidas na Lei nº 8666/93, independentemente de transcrições.

CLÁUSULA NONA – DAS OBRIGAÇÕES DA CONTRATANTE

1. Fiscalizar o fornecimento dos materiais, objeto deste Contrato;

2. A **CONTRATANTE** obriga-se a efetuar o pagamento em até 10(dez) dias úteis, após o recebimento definitivo dos materiais;

3. Fornecer a qualquer tempo e com o máximo de presteza, mediante solicitação escrita da **CONTRATADA**, informações adicionais, dirimir dúvidas e orientá-la em todos os casos omissos;

4. Aplicar penalidades à **CONTRATADA**, quando for o caso;

5. Rejeitar, no todo ou em parte, o material que a **CONTRATADA** entregar fora das especificações do Edital e seus anexos;

6. Preparar o local para recebimento dos materiais;

7. Verificar a regularidade da situação fiscal da **CONTRATADA** (consulta ao SICAF).

CLÁUSULA DÉCIMA – DA FISCALIZAÇÃO

1. A fiscalização deste Contrato será exercida pelo(s) servidor(es) designado(s) para o serviço de fiscalização e conferência, que terão plenos poderes para:

1.1 recusar material(is) em desacordo com o objeto;

1.2 promover as medidas que couberem para os casos amparados pelas cláusulas descritas neste Contrato; e

1.3 exigir da **CONTRATADA** a retirada e ou troca imediata de qualquer dos produtos que não estejam em conformidade com os requisitos exigidos e previstos neste Contrato, no Edital e Anexos .

CLÁUSULA DÉCIMA PRIMEIRA – DOS RECURSOS FINANCEIROS E ORÇAMENTÁRIOS

Os recursos orçamentários e financeiros para atender os encargos deste Contrato serão acobertados à conta do Orçamento Geral da União, PTRES: _____, Elemento de Despesa: _____ e Fonte: _____, conforme Nota de Empenho 2015NE___.

CLÁUSULA DÉCIMA SEGUNDA - DAS SANÇÕES ADMINISTRATIVAS

1. Comete infração administrativa, nos termos da Lei nº 10.520, de 2002, o licitante/adjudicatário que:

1.1 não aceitar/retirar a nota de empenho, ou não assinar a ata de registro de preço e/ou o termo de contrato, quando convocado dentro do prazo de validade da proposta;

1.2 apresentar documentação falsa;

1.3deixar de entregar os documentos exigidos no certame;

1.4 ensejar o retardamento da execução do objeto;

1.5 não mantiver a proposta;

1.6 cometer fraude fiscal;

1.7 comportar-se de modo inidôneo;

2 . Considera-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de participação, quanto ao enquadramento como ME/EPP ou o conluio entre os licitantes, em qualquer momento da licitação, mesmo após o encerramento da fase de lances.

3. O licitante/adjudicatário que cometer qualquer das infrações discriminadas no subitem anterior e na forma dos artigos 77 a 80 da Lei 8.666/93, ficará sujeito, sem prejuízo da responsabilidade civil e criminal, garantida a prévia defesa, às seguintes sanções previstas nos artigos 81 a 88 da Lei 8.666/93, artigo 7º da Lei 10.520/02, no artigo 28 do Decreto 5.450/05 e do artigo 14 do Decreto 3.555/00:

3.1 Advertência

3.2 Multa:

3.2.1 Multa de mora no percentual correspondente a 0,5% (zero vírgula cinco por cento), calculada sobre o valor remanescente do contrato, por dia de inadimplência, até o limite de 15 (quinze) dias úteis de atraso na entrega do material caracterizando inexecução parcial; e

3.2.2 Compensatória no valor de 10% (dez por cento), sobre o valor remanescente do contrato.

3.2.3 Suspensão temporária de participação em licitação com a Administração;

3.2.4 Impedimento de licitar e contratar no âmbito da União;

3.2.5 Declaração de inidoneidade.

4. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa ao licitante/adjudicatário, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente na Lei nº 9.784, de 1999.

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

6. As penalidades serão obrigatoriamente registradas no SICAF.

CLÁUSULA DÉCIMA TERCEIRA - DA RESCISÃO

O presente Contrato poderá ser rescindido por ato unilateral e escrito da **CONTRATANTE**, nos casos enumerados no art. 77 e nos incisos I a XII e XVII do art.78 da Lei 8.666/93 ou amigável, por acordo entre as partes, desde que haja conveniência para a **CONTRATANTE.**

Parágrafo Primeiro - A rescisão imediata deste Contrato caberá, além de outras hipóteses legais, independentemente de interpelação judicial ou extrajudicial, e sem prejuízo de outras penalidades, se a **CONTRATADA**:

a) falir, for objeto de concurso de credores, dissolução ou liquidação;

b) transferir, no todo ou em parte, as obrigações decorrentes deste Instrumento sem prévia anuência da Universidade Federal de Alfenas - UNIFAL-MG;

c) deixar de cumprir, total ou parcialmente, as obrigações deste Contrato;

d) cometer, reiteradamente, faltas na execução do Contrato.

e) for objeto de fusão, cisão ou incorporação que prejudique a execução do Contrato, a critério da Universidade Federal de Alfenas - UNIFAL-MG.

Parágrafo Segundo – Em caso de rescisão deste Contrato, a Universidade Federal de Alfenas – UNIFAL-MG pagará à **CONTRATADA** o valor relativo ao material entregue, descontadas as multas porventura aplicadas.

CLÁUSULA DÉCIMA QUARTA – DO FORO

O foro para dirimir quaisquer litígios decorrentes deste Contrato é o da Justiça Federal, Subseção Judiciária de Varginha - MG, "ex vi" do art. 109-I da Constituição Federal.

E assim, por estarem de acordo com este contrato e com seus termos, as partes assinam-o em duas vias, juntamente com duas testemunhas.

Alfenas, ____ de _____ de 2015.

UNIVERSIDADE FEDERAL DE ALFENAS – UNIFAL-MG

Prof. Paulo Márcio de Faria e Silva

Reitor

CONTRATADA

TESTEMUNHAS:

1) _____ 2) _____