RECIBO DE RETIRADA DE EDITAL PELA INTERNET

FORNECIMENTO DE EQUIPAMENTOS PARA REESTRUTURAÇÃO DE REDE DE DADOS

CONVOCAÇÃO GERAL Nº 006/2014

PROCESSO Nº 0264/2014

TIPO DE SELEÇÃO: MENOR PREÇO

Razão Social: _____

C.N.P.J. Nº: _____

Endereço: _____

E-mail: _____

Cidade: _____ Estado: _____ Fone: _____ Fax: _____

Pessoa para contato: _____

RECEBEMOS ATRAVÉS DO:

ACESSO À PÁGINA HYPERLINK "http://www.e-negociospublicos.com.br" www.e-negociospublicos.com.br

ACESSO À PÁGINA HYPERLINK "http://www.tvcultura.com.br" www.tvcultura.com.br

NESTA DATA, CÓPIA DO INSTRUMENTO CONVOCATÓRIO DA SELEÇÃO ACIMA IDENTIFICADA.

Local: _____, _____ de _____ de 2014.

_____
Assinatura

Senhor Licitante,

Visando comunicação futura entre este Departamento de Compras e essa Empresa, solicitamos a V. Sa., preencher este recibo de retirada do Edital e remeter à TV CULTURA, por meio do Fax nº (11) 3611-1518 ou e-mail HYPERLINK "mailto:licitacao@tvcultura.com.br" licitacao@tvcultura.com.br.

A não remessa do recibo exime o Departamento de Compras da TV CULTURA, da responsabilidade de informar a empresa licitante eventuais retificações ocorridas no instrumento convocatório, bem como quaisquer informações adicionais.

Departamento de Compras
Marcos P. Silva/Roberto Lima
Tel.: (11) 2182.3162/3156
e-mail: HYPERLINK "mailto:licitacao@tvcultura.com.br" licitacao@tvcultura.com.br

CONVOCAÇÃO GERAL Nº 006/2014

PROCESSO Nº 0264/2014

DATA DE ABERTURA: 22/09/2014 às 10h30min

PREÂMBULO:

A FUNDAÇÃO PADRE ANCHIETA – CENTRO PAULISTA DE RÁDIO E TV EDUCATIVAS por meio do Presidente da Comissão de Seleção, designado pelo Senhor Diretor Administrativo e Financeiro, torna público que se encontra aberta, nesta unidade, Seleção na modalidade Convocação Geral nº 006/2014, do tipo

Menor Preço, para a seleção e contratação de empresa para fornecimento de conjunto de equipamentos para reestruturação de rede de dados.

Os envelopes contendo a Proposta de Preço (Envelope A) e Documentos de Habilitação (Envelope B) serão recebidos no **dia 22/09/2014 às 10:30 horas**, na Rua Cenno Sbrighi, nº 378 – Setor de Compras – Bloco A1 – Água Branca - São Paulo/SP**.** No mesmo dia e horário, em sessão pública, os Envelopes "A" (Proposta de Preço) serão abertos na presença dos interessados.

Os interessados deverão dirigir-se ao endereço acima, com antecedência, em tempo hábil, pois serão identificados na portaria antes de serem encaminhados à sala onde será realizada a sessão pública.
Esta Convocação Geral será regida por este Edital e seus anexos, pelo Regulamento de Compras e Contratos desta Fundação e demais disposições legais aplicáveis.

No dia, hora e local acima indicados, os envelopes "A" (Proposta de Preço) e "B" (Documentos de Habilitação) deverão ser entregues à Comissão de Seleção.

1 DO OBJETO:

1.1 A presente Seleção tem por objeto o fornecimento de 1 (um) conjunto de equipamentos para reestruturação da rede de dados da Fundação Padre Anchieta, incluindo consultoria de projeto, implantação, curso e treinamento, demais especificações e condições conforme Memorial Descritivo (Anexo I) deste Edital.

1.2 O prazo de entrega será de até 45 (quarenta e cinco) dias.

1.3 O fornecimento inclui garantia e suporte total pelo período de 12 (doze) meses com atendimento 8 x 5 x NBD realizada pelo fabricante ou representante no Brasil.

2 DAS CONDIÇÕES DE PARTICIPAÇÃO

2.1 Poderão participar desta Convocação Geral, todas as empresas interessadas, brasileiras ou estrangeiras, de forma isolada, que demonstrem possuir capacidade para fornecimento dos equipamentos, objeto desta Seleção, conforme condições de habilitação estabelecidas neste Edital.

2.2 Não poderão participar desta Convocação Geral:

2.2.1 Empresas que estiverem cumprindo suspensão temporária do direito de participar de licitação ou de contratar com a Administração Direta ou Indireta Federal, Estadual ou Municipal.

2.2.2 Empresas cuja falência tenha sido decretada ou que estiver em concurso de credores, em processo de liquidação, dissolução, cisão, fusão ou incorporação.

2.2.3 Empresas brasileiras ou estrangeiras, isoladamente em mais de uma proposta.

2.2.4 Não será permitida a participação de empresas em regime de consorcio.

2.3 Nenhuma proponente poderá participar desta Convocação Geral com mais de uma proposta.

2.4 A participação na presente Seleção implicará que a proponente:

recebeu da Comissão de Seleção, todos os documentos e informações necessárias para participação do presente certame;

aceita plena e irrevogavelmente todos os termos, cláusulas e condições constantes deste Edital e de seus anexos;

observará todos os preceitos legais e regulamentares em vigor e a responsabilidade pela fidelidade e legitimidade das informações e dos documentos apresentados em qualquer fase do processo;

A participação na seleção implica em total e irrestrita submissão das proponentes às condições deste Edital.

2.5 Em hipótese alguma serão concedidos prazos para a apresentação de documentos que não foram entregues na data e hora estabelecida no preâmbulo deste Edital, bem como fora dos respectivos envelopes.

3 DA REPRESENTAÇÃO E DO CREDENCIAMENTO

3.1 A proponente poderá apresentar-se, no dia previsto no preâmbulo deste Edital, para credenciamento junto a Comissão de Seleção, através de um representante que, devidamente munido de documento que o credencie a participar deste procedimento de Seleção, venha a responder por sua representada, devendo ainda, no ato do credenciamento, identificar-se exibindo a carteira de identidade ou outro documento equivalente. A proponente que não apresentar-se através de um representante devidamente credenciado, poderá participar do presente procedimento de Seleção, neste caso, existindo um portador da proposta o mesmo estará impedido de manifestar-se em nome da mesma.

3.2 Uma mesma pessoa não poderá representar mais de uma proponente.

3.3 No ato da entrega dos envelopes com os Documentos para Habilitação (Envelope “B”) e Proposta de Preço (Envelope “A”), o representante da proponente apresentará à Comissão de Seleção:

Tratando-se de representante legal, o estatuto social, contrato social ou outro instrumento de registro comercial, registrado na Junta Comercial, no qual estejam expressos seus poderes para exercer direitos e assumir obrigações em decorrência de tal investidura;

Tratando-se de procurador, a procuração por instrumento público ou particular, na qual constem poderes específicos para interpor recursos e desistir de sua interposição e praticar todos dos demais atos pertinentes ao certame, acompanhado do correspondente documento, dentre os indicados na alínea “a”, que comprove os poderes do mandante para a outorga;

Os documentos indicados na alínea “a” e “b” deverão ser apresentados

em original, por qualquer processo de cópia autenticada por tabelião de notas ou cópia acompanhada do original para autenticação pela Comissão de Seleção;

Em caso de mais de um representante, um exercerá a representação e os demais serão ouvintes/assistentes;

A falta de um representante não desclassifica a proponente do certame, apenas ficará impedida de manifestar-se durante a sessão.

Observação: Se a empresa proponente se enquadrar nos termos da Lei Complementar nº 123, de 14 de dezembro de 2006, como MICROEMPRESA (ME) ou EMPRESA DE PEQUENO PORTE (EPP), deverá a mesma, no momento do credenciamento, apresentar, também, a declaração constante do modelo em apenso (Anexo II), notadamente para efeito de aplicação do "direito de preferência" previsto na citada norma. Se, todavia, a referida declaração não estiver de posse do representante legal da empresa, o mesmo deverá declarar publicamente ao Presidente da Comissão de Seleção que a sua empresa se enquadra em uma dessas hipóteses, devendo tal afirmação ficar expressamente consignada em Ata.

4 DA APRESENTAÇÃO DOS DOCUMENTOS

4.1 A Proposta de Preço (Envelope "A") e os Documentos de Habilitação (Envelope "B") deverão ser apresentados no local, dia e hora mencionados no Preâmbulo deste Edital, pelas proponentes, conforme descrito no item anterior, mediante apresentação de 2 (dois) envelopes opacos, devidamente fechados e rubricados, identificados conforme abaixo:

ENVELOPE "A" – PROPOSTA DE PREÇO
Fundação Padre Anchieta – Centro Paulista de Rádio e TV Educativas
Convocação Geral n° 006/2014
Processo n° 0264/2014
Objeto: Fornecimento de equipamentos para reestruturação de rede de dados.
Razão Social da Empresa:

ENVELOPE "B" – DOCUMENTOS DE HABILITAÇÃO

Fundação Padre Anchieta – Centro Paulista de Rádio e TV Educativas
Convocação Geral n° 006/2014
Processo n° 0264/2014
Objeto Fornecimento de equipamentos para reestruturação de rede de dados.
Razão Social da Empresa:

PROPONENTES BRASILEIRAS

5 PROPONENTES BRASILEIRAS - PROPOSTA DE PREÇO -

ENVELOPE “A”

5.1 Deverá ser elaborada em 01 (uma) via, impressa em papel timbrado da proponente, em língua portuguesa, redigida com clareza, sem rasuras, acréscimos ou entrelinhas, devidamente datada, assinada pelo representante legal da proponente, na qual **deverão constar** as seguintes informações:

5.1.1 Especificação detalhada do sistema a ser fornecido, mencionando quantidade, marca e modelo de cada item que compõe o fornecimento ofertado, em conformidade com as condições do presente Edital e com as especificações constantes no Memorial Descritivo – Anexo I;

5.1.2 Indicar razão social do proponente, número do CNPJ, endereço completo, telefone, bem como dados do representante legal que assinar a proposta;

5.1.3 Validade da proposta, que não poderá ser inferior a 60 (sessenta) dias corridos, a contar da data de sua apresentação;

5.1.4 Planilha na qual deverá constar o **Preço Unitário e Preço Total**, de cada item mencionado no Memorial Descritivo (Anexo I) e também o **Total Geral**, correspondente a soma de todos os **Preços Total**, expressos em reais (R$), sem a inclusão de qualquer encargo financeiro ou previsão inflacionária;

5.1.4.1 O Preços deverão ser apurados à data de sua apresentação, sem inclusão de qualquer encargo financeiro ou previsão inflacionária. Nos preços propostos deverão estar incluídos, além do lucro, todas as despesas e custos, como por exemplo: transporte, tributos de qualquer natureza e todas as despesas, diretas ou indiretas, relacionadas com o fornecimento do objeto da presente Seleção;

5.1.4.2 Deverá ser **DEDUZIDO** do preço a parcela correspondente ao ICMS. Deverá ser considerada a isenção do ICMS, conforme artigo 55, ANEXO I, do Decreto estadual n° 45.490/00, alterado pelo Decreto estadual n° 48.034, de 19/08/03 (para operações internas).

5.1.5 Constar que os preços apresentados são fixos e irreajustáveis até o término do fornecimento;

5.1.6 Constar que no fornecimento esta incluída garantia e suporte total pelo período de 12 (doze) meses com atendimento 8 x 5 x NBD realizada pelo fabricante ou representante no Brasil;

5.1.7 A condição de pagamento, observando-se o item 5.3 abaixo;

5.1.8 O local de entrega, observando-se o item 5.2 abaixo;

5.1.9 O prazo de entrega que não poderá ser superior a 45 (quarenta

e cinco) dias;

5.2 O objeto deverá ser entregue na sede da Fundação Padre Anchieta, localizada na Rua Cenno Sbrighi, 378 – Bairro Água Branca – São Paulo/SP.

5.3 O pagamento será efetuado, mediante a apresentação da nota fiscal/ fatura, que deverá ser entregue juntamente com os equipamentos, no endereço mencionado no item 5.2, a qual deverá ser devidamente atestada pelo Departamento de Engenharia, desta Fundação, sendo que o pagamento será efetuado mediante depósito em conta corrente da contratada, no Banco do Brasil S/A, em conformidade com o artigo 1º, do Decreto nº 55.357, de 18 de janeiro de 2010, na seguinte forma:

25% em até 10 (dez) dias após a data de assinatura do contrato;

75% no dia 10 (dez) do mês subsequente ao mês da entrega.

5.3.1 Todos os títulos de cobrança eventualmente emitidos pela Contratada contra a Contratante não poderão ser negociados com terceiros, sendo certo que a Contratante não estará obrigada a efetuar pagamentos que contrariam em disposto neste item.

5.4 Constitui condição para a realização do pagamento a inexistência de registros em nome da Contratada no "Cadastro Informativo dos Créditos não Quitados de Órgãos e Entidades Estaduais do Estado de São Paulo – CADIN ESTADUAL", o qual deverá ser consultado por ocasião da realização do pagamento.

5.5 As notas fiscais/faturas que apresentarem incorreções serão devolvidas à Contratada e seu vencimento ocorrerá em 30 (trinta) dias após a data de sua apresentação válida.

5.6 Quaisquer tributos, custos e despesas diretos ou indiretos omitidos na proposta de preço ou, incorretamente cotados, serão considerados como inclusos nos preços, não sendo considerados pleitos de acréscimos, com esse teor, sob qualquer título, devendo o objeto desta Seleção ser fornecido à Fundação Padre Anchieta sem ônus adicionais.

5.7 Serão desclassificadas as propostas de preço que não atenderem às exigências do presente Edital, sejam omissas ou apresentem irregularidades ou defeitos capazes de dificultar ou impedir o seu julgamento.

5.8 A proposta apresentada deverá ser firme e precisa, sem alternativas de preço ou qualquer outra condição que induza seu julgamento a ter mais de um resultado.

5.9 O critério de analise das propostas de preço será pelo **menor preço,** considerado como tal o valor correspondente ao menor **Total Geral.**

5.10 Havendo divergência entre os valores registrados sob a forma

numérica e os valores apresentados por extenso, prevalecerá este último.

5.11 **Considerar-se-á incluída no conceito de "Proponentes Brasileiras" a empresa e/ou sociedade estrangeira autorizada e em efetivo funcionamento no Brasil, que participar através de seu estabelecimento local registrado ou autorizado para funcionamento no território nacional por ato expedido por órgão competente.**

5.12 A proponente, brasileira, vencedora, que não tenha o registro no Cadastro Geral de Fornecedores do Estado de São Paulo, em sua versão web – CAUFESP deverá apresentar uma declaração se comprometendo a providenciar o registro ou atualizá-lo até a data da assinatura do contrato, conforme modelo ANEXO III, deste Edital, a qual deverá ser inserida no Envelope "B", conforme mencionado na alínea "c", do item 6.1.3, sob pena de decadência do direito à contratação, sem prejuízo da aplicação das sanções cabíveis.
As informações a respeito das condições exigidas para o registro no CAUFESP estão disponíveis no endereço eletrônico HYPERLINK "http://www.bec.sp.gov.br" www.bec.sp.gov.br.

6 PROPONENTES BRASILEIRAS – DOCUMENTAÇÃO DE HABILITAÇÃO - ENVELOPE "B"

6.1 O Envelope "B" "Documentos de Habilitação" deverá conter os documentos a seguir relacionados, os quais dizem respeito a:

6.1.1 HABILITAÇÃO JURÍDICA

registro comercial, no caso de empresário individual;

ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado na Junta Comercial, em se tratando de sociedades empresariais;

documentos de eleição dos atuais administradores, tratando-se de sociedades por ações, acompanhados da documentação mencionada na alínea "b", deste subitem;

ato constitutivo devidamente registrado no Cartório de Registro Civil de Pessoas Jurídicas tratando-se de sociedades civis, acompanhado de prova da diretoria em exercício;

as empresas estrangeiras com subsidiárias, filial, agência, escritório ou agente no Brasil deverão apresentar autorização, mediante decreto ou ato expedido pelo Ministério do Desenvolvimento, Indústria e Comércio Exterior para funcionamento no Brasil, o ato de registro ou autorização para funcionamento pelo Órgão Competente se a atividade assim o exigir, e os documentos exigidos neste edital.

Observação: Os documentos apresentados no credenciamento não precisam constar no envelope "B".

6.1.2 REGULARIDADE FISCAL E TRABALHISTA

prova de inscrição no Cadastro Nacional de Pessoas Jurídicas do Ministério da Fazenda (CNPJ);

certidão de regularidade de débito com as Fazendas Estadual e Municipal**,** da sede da licitante ou outra prova equivalente, na forma da lei;

b.1) Mesmo que a proponente não esteja obrigada a inscrever-se na Fazenda Estadual, deverá apresentar a devida certidão de regularidade de débito, na qual constará a não obrigatoriedade da inscrição.

certidão de regularidade fiscal para com a Seguridade Social, expedida pelo Instituto Nacional do Seguro Social – INSS, válida na data da apresentação;

certidão de Regularidade perante o Fundo de Garantia do Tempo de Serviço (CRF – FGTS), valida na data de apresentação;

certidão conjunta negativa da Secretaria da Receita Federal e da Procuradoria da Fazenda Nacional;

prova da inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante apresentação de Certidão Negativa de Débitos Trabalhistas – CNDT.

6.1.3 OUTRAS COMPROVAÇÕES

Declaração da proponente, elaborada em papel timbrado e subscrita por seu representante legal, de que se encontra em situação regular perante o Ministério do Trabalho, Decreto Estadual nº 42.911, de 06.03.98, conforme modelo ANEXO IV deste Edital;

Declaração elaborada em papel timbrado e subscrita pelo representante legal da proponente, assegurando a inexistência de impedimento legal para licitar ou contratar com a Administração, conforme modelo ANEXO V deste Edital;

Declaração elaborada em papel timbrado e subscrita pelo representante legal da proponente, no que se refere ao Registro CAUFESP, conforme modelo ANEXO III deste Edital;

6.1.4 QUALIFICAÇÃO TÉCNICA

Comprovação de aptidão, mediante apresentação de Atestado(s) de Capacidade Técnica, emitido por pessoa Jurídica de Direito Público ou Privado, em papel timbrado, com assinatura do emitente, que comprove(m) que a proponente forneceu objeto com características semelhantes ao objeto do presente Edital.

6.2 DISPOSIÇÕES GERAIS DA HABILITAÇÃO

6.2.1 Os documentos relacionados nos itens anteriores deverão ser apresentados em original ou por cópia autenticada por tabelião de notas ou, se não autenticadas, acompanhada dos originais, para autenticação por representante da Fundação Padre

Anchieta. Os documentos mencionados nas alíneas “a”, “c”, “d”, “e” e “f” do subitem 6.1.2, deste item 6, e outros que possam ser obtidos via internet, poderão ser apresentados em cópia reprográfica simples, ficando condicionada sua aceitação à confirmação dos dados mediante consulta pela Internet:

6.2.1.1 Os documentos relacionados nos itens 6.1.3 e 6.1.4, deste item 6, devem ser apresentados por todas as proponentes;

6.2.1.2 Não serão aceitos protocolos de entrega ou solicitação de documento em substituição aos documentos requeridos no presente Edital e seus anexos.

6.2.2 Na hipótese de não constar prazo de validade nas certidões apresentadas, a Comissão de Seleção aceitará como válidas as expedidas até 180 (cento e oitenta) dias imediatamente anteriores à data de apresentação das propostas;

6.2.3 Será inabilitada a proponente que deixar de apresentar, de acordo com o exigido, qualquer documento solicitado ou apresentá-los com defeitos, bem como não atender às condições para habilitação;

6.2.4 As Microempresas - ME, e Empresas de Pequeno Porte - EPP, assim consideradas aquelas que se enquadram no estabelecido pelo artigo 3º da Lei Complementar nº. 123/2006 deverão comprovar que atendem aos requisitos do artigo para fazer jus aos benefícios previstos na referida lei;

6.2.5 A comprovação acima será feita mediante apresentação do ato constitutivo devidamente arquivado na junta comercial, ou registro civil das pessoas jurídicas, ou documento expedido pela Receita Federal, onde conste que a proponente é Microempresa ou Empresa de Pequeno Porte;

6.2.6 As Microempresas e Empresas de Pequeno Porte deverão apresentar toda a documentação exigida para efeito de comprovação de regularidade fiscal, mesmo que esta apresente alguma restrição;

6.2.7 Havendo alguma restrição na comprovação da regularidade fiscal das Microempresas ou Empresas de Pequeno Porte, será assegurado o prazo de até 02 (dois) dias úteis, cujo termo inicial corresponderá ao momento em que o proponente for declarado o vencedor do certame, prorrogáveis por igual período, a critério da Administração, para sua regularização;

6.2.8 A não regularização da documentação, no prazo previsto no subitem anterior, implicará decadência do direito à contratação sem prejuízo das sanções previstas neste Edital, sendo facultado à Fundação Padre Anchieta convocar os proponentes remanescentes, na ordem de classificação, para a assinatura do contrato, ou revogar a Seleção;

PROPONENTES ESTRANGEIRAS

7 PROPONENTES ESTRANGEIRAS – PROPOSTA DE PREÇO –

ENVELOPE "A"

7.1 Deverá ser elaborada em 01 (uma) via, impressa em papel timbrado da proponente, em idioma português do Brasil, sendo admitida no caso de PROPONENTE ESTRANGEIRA a sua elaboração no idioma inglês, com tradução pública juramentada, redigida com clareza, sem rasuras, acréscimos ou entrelinhas, devidamente datada, assinada pelo representante legal da proponente, na qual **deverão constar** as seguintes informações:

Nota: No caso de "Proponente Estrangeira" toda documentação de habilitação, proposta, seja original ou cópia, deverá ser notariada, quando aplicável, e, consularizada por Autoridade Consular Brasileira no seu país de origem e traduzida para o português por tradutor público juramentado no Brasil ou no exterior.

7.1.1 Especificação detalhada do sistema a ser fornecido, mencionando quantidade, marca e modelo de cada item que compõe o fornecimento ofertado, em conformidade com as condições do presente Edital e com as especificações constantes no Memorial Descritivo – Anexo I;

7.1.2 Indicar razão social do proponente, endereço completo, telefone, bem como dados do representante legal que assinar a proposta;

7.1.3 Validade da proposta, que não poderá ser inferior a 60 (sessenta) dias corridos, a contar da data de sua apresentação;

7.1.4 Constar que os preços apresentados são fixos e irreajustáveis até o término do fornecimento;

7.1.5 Planilha na qual deverá constar o **Preço Unitário e Preço Total**, de cada item mencionado no Memorial Descritivo (Anexo I) e também o **Total Geral**, correspondente a soma de todos os **Preços Total**, expressos em reais (R$), e valor correspondente em **MOEDA ESTRANGEIRA** mencionando a data da conversão, sem a inclusão de qualquer encargo financeiro ou previsão inflacionária;

7.1.5.1 A proposta deverá evidenciar **o preço na forma EWX (Ex Works – INCOTERMS 2010)** a proponente deverá indicar em sua proposta o endereço do local (fábrica, armazém, etc.) em que os equipamentos serão colocados a disposição da Fundação Padre Anchieta. Os equipamentos deverão ser devidamente embalados para o transporte. A Fundação Padre Anchieta assume todos os custos relativos ao embarque internacional, bem como a contratação de frete internacional, seguro e demais despesas relativas ao transporte dos equipamentos.

7.1.6 Constar que no fornecimento esta incluída garantia e suporte total pelo período de 12 (doze) meses com atendimento 8 x 5 x

NBD realizada pelo fabricante ou representante no Brasil;

7.1.7 O prazo de entrega que não poderá ser superior a 45 (quarenta e cinco) dias;

7.1.8 A condição de pagamento, observando-se o item 7.2 abaixo;

7.1.9 O local de embarque (coleta) dos equipamentos, observando-se o item 7.1.5.1.

7.2 Os pagamentos serão efetuados, mediante a apresentação da Commercial Invoice que deverá ser encaminhada ao Setor de Compras/Importação da Fundação Padre Anchieta, A/C do Sr. Cássio Jorge, telefone (5511) 2182.3458 – e-mail: HYPERLINK "mailto:cassiojorge@tvcultura.com.br" cassiojorge@tvcultura.com.br, sendo que o pagamento será efetuado ao exportador, em reais, através do Banco do Brasil, mediante ordem de pagamento bancária no exterior, na seguinte forma:

- 25% em até 10 (dez) dias após a data de assinatura do contrato;

- 75% em 30(trinta) dias da data de confirmação do embarque.

7.2.1 Os valores correspondentes a MOEDA ESTRANGEIRA, serão convertidos pela taxa de câmbio para moeda estrangeira segundo o valor para venda comercial vigente no dia útil imediatamente anterior à data do efetivo pagamento, e disponibilizado pelo Sistema de informação do Banco Central do Brasil – SISBACEN, Boletim de Fechamento;

7.2.2 O pagamento será efetuado em Reais (R$) de acordo com o disposto no Regulamento do Mercado de Câmbio e Capitais Internacionais, devendo a Contratada adotar o cumprimento dos ditames legais e regulamentares previstos para as providências condicionais de recebimento;

7.2.2.1 O pagamento será efetuado através de transferência financeira para o exterior, a ser realizada para banco indicado pela contratada.

7.2.3 O pagamento da 2ª parcela, correspondente aos 75%, somente será devido após o desembarque dos equipamentos nas dependências Fundação Padre Anchieta e consequente inspeção do objeto contratado pelos técnicos do Departamento de Engenharia da Fundação Padre Anchieta.

7.3 Serão desclassificadas as propostas de preço que não atenderem às exigências do presente Edital, sejam omissas ou apresentem irregularidades ou defeitos capazes de dificultar ou impedir o seu julgamento.

7.4 Quaisquer custos e despesas diretos ou indiretos omitidos na proposta de preço ou, incorretamente cotados, serão considerados como

inclusos nos preços, não sendo considerados pleitos de acréscimos, com esse teor, sob qualquer título, devendo o objeto desta Seleção ser fornecido a Fundação Padre Anchieta sem ônus adicionais.

7.5 A proposta apresentada deverá ser firme e precisa, sem alternativas de preço ou qualquer outra condição que induza seu julgamento a ter mais de um resultado.

7.6 O critério de analise das propostas de preço será pelo **menor preço,** considerado como tal o valor correspondente ao menor **Total Geral.**

7.7 Havendo divergência entre os valores registrados sob a forma numérica e os valores apresentados por extenso, prevalecerá este último.

7.8 Os preços apresentados **na forma EWX** deverão ser apurados à data de sua apresentação, sem inclusão de qualquer encargo financeiro ou previsão inflacionária. Nos preços propostos deverão estar incluídos, além do lucro, todas as despesas e custos, como por exemplo: embalagem, tributos de qualquer natureza e todas as despesas, diretas ou indiretas, relacionadas com o fornecimento do objeto da presente Seleção, **na forma EWX (Ex Works – INCOTERMS 2010).**

7.9 Com o propósito de facilitar o julgamento das propostas, a Fundação Padre Anchieta converterá o preço cotado diretamente para a moeda brasileira (R$) às taxas de câmbio para a venda, publicada pelo Banco Central do Brasil, vigente na data limite fixada para apresentação das propostas.

7.10 As propostas classificadas serão ordenadas após a aplicação dos cálculos de homogeneização de preços. Os preços ofertados por PROPONENTE ESTRANGEIRA, na forma na forma **EWX (Ex Works – INCOTERMS 2010)**, serão homogeneizados com aplicação de despesas relativas ao frete internacional e doméstico, armazenagem, despesas aeroportuárias, etc e taxas nas suas respectivas alíquotas vigentes na data de abertura das propostas.

7.11 A Fundação Padre Anchieta goza de imunidade tributária para fins de importação.

8 PROPONENTES ESTRANGEIRAS – DOCUMENTAÇÃO DE HABILITAÇÃO – ENVELOPE “B”

8.1 O Envelope “B” "Documentos de Habilitação" deverá conter os documentos a seguir relacionados os quais dizem respeito a:

8.1.1 HABILITAÇÃO JURÍDICA

prova de estar legalmente constituída no seu país de origem, emitida por entidade governamental;

prova de estar legalmente representado no Brasil, por pessoa física ou jurídica que tenha poderes específicos (PROCURAÇÃO) para receber citação e responder, administrativa e judicialmente,

conforme modelo (em português/inglês) constante no Anexo VI, deste Edital.

8.1.2 REGULARIDADE FISCAL

Documento que comprove regularidade fiscal em seu país.

8.1.3 OUTRAS COMPROVAÇÕES

Deverá ser apresentado, o documento mencionado na alínea **"b" do item 6.1.3**.

8.1.4 QUALIFICAÇÃO TÉCNICA

Comprovação de aptidão, mediante apresentação de Atestado(s) de Capacidade Técnica, emitido por pessoa Jurídica de Direito Publico ou Privado, em papel timbrado, com assinatura do emitente, que comprove(m) que a proponente forneceu objeto com características semelhantes ao objeto do presente Edital.

8.2 DISPOSIÇÕES GERAIS DA HABILITAÇÃO

8.2.1 Toda documentação de habilitação (itens 8.1.1, 8.1.2, 8.1.3 e 8.1.4), seja original ou cópia, deverá ser notariada, quando aplicável, e, consularizada por Autoridade Consular Brasileira no seu país de origem e traduzida para o português por tradutor público juramentado no Brasil ou no exterior.

8.2.2 Será inabilitada a proponente que deixar de apresentar, de acordo com o exigido, qualquer documento solicitado ou apresentá-los com defeitos, bem como não atender às condições para habilitação.

PROPONENTES BRASILEIRAS REPRESENTANTES DE EMPRESAS ESTRANGEIRAS

9 PROPONENTES BRASILEIRAS REPRESENTANTES DE EMPRESAS ESTRANGEIRAS - PROPOSTA DE PREÇO – ENVELOPE "A"

9.1 Deverá ser elaborada em 01 (uma) via, impressa em papel timbrado da proponente, em idioma português do Brasil, redigida com clareza, sem rasuras, acréscimos ou entrelinhas, devidamente datada, assinada pelo representante legal da proponente, na qual **deverão constar** as seguintes informações:

9.1.1 Especificação detalhada do sistema a ser fornecido, mencionando quantidade, marca e modelo de cada item que compõe o fornecimento ofertado, em conformidade com as condições do presente Edital e com as especificações constantes no Memorial Descritivo – Anexo I;

9.1.2 Indicar razão social do proponente, endereço completo, telefone, bem como dados do representante legal que assinar a proposta;

9.1.3 Indicar a razão social do exportador, endereço completo, telefone, domicilio bancário;

9.1.4 Validade da proposta, que não poderá ser inferior a 60 (sessenta) dias corridos, a contar da data de sua apresentação;

9.1.5 Constar que os preços apresentados são fixos e irreajustáveis até o término do fornecimento;

9.1.6 Planilha na qual deverá constar o **Preço Unitário e Preço Total**, de cada item mencionado no Memorial Descritivo (Anexo I) e também o **Total Geral**, correspondente a soma de todos os **Preços Total**, expressos em reais (R$), e valor correspondente em **MOEDA ESTRANGEIRA** mencionando a data da conversão, sem a inclusão de qualquer encargo financeiro ou previsão inflacionária;

9.1.6.1 A proposta deverá evidenciar **o preço na forma EWX (Ex Works – INCOTERMS 2010)** a proponente deverá indicar em sua proposta o endereço do local (fábrica, armazém, etc.) em que os equipamentos serão colocados a disposição da Fundação Padre Anchieta. Os equipamentos deverão ser devidamente embalados para o transporte. A Fundação Padre Anchieta assume todos os custos relativos ao embarque internacional, bem como a contratação de frete internacional, seguro e demais despesas relativas ao transporte dos equipamentos.

9.1.7 Constar que no fornecimento esta incluída garantia e suporte total pelo período de 12 (doze) meses com atendimento 8 x 5 x NBD realizada pelo fabricante ou representante no Brasil;

9.1.8 O prazo de entrega que não poderá ser superior a 45 (quarenta e cinco) dias;

9.1.9 A condição de pagamento, observando-se o item 9.2 abaixo;

9.1.10 O local de embarque (coleta) dos equipamentos, observando-se o item 9.1.6.1.

9.2 Os pagamentos serão efetuados, mediante a apresentação da Commercial Invoice que deverá ser encaminhada ao Setor de Compras/Importação da Fundação Padre Anchieta, A/C do Sr. Cássio Jorge, telefone (5511) 2182.3458 – e-mail: HYPERLINK "mailto:cassiojorge@tvcultura.com.br" cassiojorge@tvcultura.com.br, sendo que o pagamento será efetuado ao exportador, em reais, através do Banco do Brasil, mediante ordem de pagamento bancária no exterior, na seguinte forma:

- 25% em até 10 (dez) dias após a data de assinatura do contrato;

- 75% em 30(trinta) dias da data de confirmação do embarque.

9.2.1 Os valores correspondentes a MOEDA ESTRANGEIRA, serão convertidos pela taxa de câmbio para moeda estrangeira segundo o valor para venda comercial vigente no dia útil imediatamente anterior à data do efetivo pagamento, e disponibilizado pelo Sistema de informação do Banco Central do Brasil – SISBACEN, Boletim de Fechamento.

9.2.2 O pagamento será efetuado em Reais (R$) de acordo com o disposto no Regulamento do Mercado de Câmbio e Capitais Internacionais, devendo a Contratada adotar o cumprimento dos ditames legais e regulamentares previstos para as providências condicionais de recebimento.

9.2.2.1 O pagamento será efetuado através de transferência financeira para o exterior, a ser realizada para banco indicado pela contratada.

9.2.3 O pagamento da 2ª parcela, correspondente aos 75%, somente será devido após o desembarque dos equipamentos nas dependências Fundação Padre Anchieta e consequente inspeção do objeto contratado pelos técnicos do Departamento de Engenharia da Fundação Padre Anchieta.

9.3 Serão desclassificadas as propostas de preço que não atenderem às exigências do presente Edital, sejam omissas ou apresentem irregularidades ou defeitos capazes de dificultar ou impedir o seu julgamento.

9.4 Quaisquer custos e despesas diretos ou indiretos omitidos na proposta de preço ou, incorretamente cotados, serão considerados como inclusos nos preços, não sendo considerados pleitos de acréscimos, com esse teor, sob qualquer título, devendo o objeto desta Seleção ser fornecido a Fundação Padre Anchieta sem ônus adicionais.

9.5 A proposta apresentada deverá ser firme e precisa, sem alternativas de preço ou qualquer outra condição que induza seu julgamento a ter mais de um resultado.

9.6 O critério de analise das propostas de preço será pelo **menor preço,** considerado como tal o valor correspondente ao menor **Total Geral.**

9.7 Havendo divergência entre os valores registrados sob a forma numérica e os valores apresentados por extenso, prevalecerá este último.

9.8 Os preços apresentados **na forma EWX** deverão ser apurados à data de sua apresentação, sem inclusão de qualquer encargo financeiro ou previsão inflacionária. Nos preços propostos deverão estar incluídos, além do lucro, todas as despesas e custos, como por exemplo: embalagem, tributos de qualquer natureza e todas as despesas, diretas

ou indiretas, relacionadas com o fornecimento do objeto da presente Seleção, **na forma EWX (Ex Works – INCOTERMS 2010).**

9.9 Com o propósito de facilitar o julgamento das propostas, a Fundação Padre Anchieta converterá o preço cotado diretamente para a moeda brasileira (R$) às taxas de câmbio para a venda, publicada pelo Banco Central do Brasil, vigentes na data limite fixadas para apresentação das propostas.

9.10 As propostas classificadas serão ordenadas após a aplicação dos cálculos de homogeneização de preços. Os preços ofertados por PROPONENTES BRASILEIRAS REPRESENTANTES DE EMPRESAS ESTRANGEIRAS, na forma **EWX (Ex Works - INCOTERMS 2010)**, serão homogeneizados com aplicação de despesas relativas ao frete internacional e doméstico, armazenagem, despesas aero portuárias, etc e taxas nas suas respectivas alíquotas vigentes na data de abertura das propostas.

9.11 A Fundação Padre Anchieta goza de imunidade tributária para fins de importação.

10 PROPONENTES BRASILEIRAS REPRESENTANTES DE EMPRESAS ESTRANGEIRAS – DOCUMENTAÇÃO DE HABILITAÇÃO – ENVELOPE "B"

10.1 O Envelope "B" "Documentos de Habilitação" deverá conter os documentos a seguir relacionados os quais dizem respeito a:

10.1.1 HABILITAÇÃO JURÍDICA

Deverão ser apresentados os documentos mencionados n**o** item 6.1.1.

Declaração ou contrato que comprove o vínculo comercial no ramo de atividade entre as empresas (Representante e Representada), caso a declaração ou contrato esteja no idioma estrangeiro apresentar também a tradução pública juramentada. Ficando a critério exclusivo da Fundação Padre Anchieta o diligenciamento para confirmação das informações.

10.1.2 REGULARIDADE FISCAL E TRABALHISTA

Deverão ser apresentados os documentos mencionados no **item 6.1.2**.

10.1.3 OUTRAS COMPROVAÇÕES

Deverão ser apresentados os documentos mencionados no **item 6.1.3**.

10.1.4 QUALIFICAÇÃO TÉCNICA

Comprovação de aptidão, mediante apresentação de Atestado(s) de Capacidade Técnica, emitido por pessoa Jurídica de Direito Publico ou Privado, em papel timbrado, com assinatura do emitente, que comprove(m) que a proponente forneceu objeto

com características semelhantes ao objeto do presente edital.

10.2 DISPOSIÇÕES GERAIS DA HABILITAÇÃO

10.2.1 Os documentos relacionados nos itens anteriores deverão ser apresentados em original ou por cópia autenticada por tabelião de notas ou, se não autenticadas, acompanhadas dos originais, para autenticação por representante da Fundação Padre Anchieta. Os documentos mencionados nas alíneas “a”, “c”, “d”, “e” e “f” do subitem 6.1.2, do item 6, e outros que possam ser obtidos via internet, poderão ser apresentados em cópia reprográfica simples, ficando condicionada sua aceitação à confirmação dos dados mediante consulta pela Internet:

10.2.1.1 Os documentos relacionados nos itens 6.1.3 (10.1.3) e 10.1.4, devem ser apresentados por todas as proponentes.

10.2.1.2 Não serão aceitos protocolos de entrega ou solicitação de documento em substituição aos documentos requeridos no presente Edital e seus anexos.

10.2.2 Na hipótese de não constar prazo de validade nas certidões apresentadas, a Comissão de Seleção aceitará como válidas as expedidas até 180 (cento e oitenta) dias imediatamente anteriores à data de apresentação das propostas.

10.2.3 Será inabilitada a proponente que deixar de apresentar, de acordo com o exigido, qualquer documento solicitado ou apresentá-los com defeitos, bem como não atender às condições para habilitação.

10.2.4 As Microempresas - ME, e Empresas de Pequeno Porte - EPP, assim consideradas aquelas que se enquadram no estabelecido pelo artigo 3º, da Lei Complementar nº. 123/2006 deverão comprovar que atendem aos requisitos do artigo para fazer jus aos benefícios previstos na referida lei;

10.2.5 A comprovação acima será feita mediante apresentação do ato constitutivo devidamente arquivado na junta comercial, ou registro civil das pessoas jurídicas, ou documento expedido pela Receita Federal, onde conste que a proponente é Microempresa ou Empresa de Pequeno Porte.

10.2.6 As Microempresas e Empresas de Pequeno Porte deverão apresentar toda a documentação exigida para efeito de comprovação de regularidade fiscal, mesmo que esta apresente alguma restrição.

10.2.7 Havendo alguma restrição na comprovação da regularidade fiscal das Microempresas ou Empresas de Pequeno Porte, será assegurado o prazo de até 02 (dois) dias úteis, cujo termo inicial corresponderá ao momento em que o proponente for declarado o vencedor do certame, prorrogáveis por igual período, a critério da Administração, para sua regularização.

10.2.8 A não regularização da documentação, no prazo previsto no subitem anterior, implicará decadência do direito à contratação sem prejuízo das sanções previstas neste Edital, sendo facultado à Fundação Padre Anchieta

convocar os proponentes remanescentes, na ordem de classificação, para a assinatura do contrato, ou revogar a Seleção.

11 DO PROCEDIMENTO

11.1 Os documentos de Habilitação (Envelope “B”) e a Proposta de Preço (Envelope “A”) deverão ser entregues a Comissão de Seleção, em envelopes distintos, no local, data e horário previstos no preâmbulo deste Edital.

11.2 Após o Presidente da Comissão de Seleção declarar instalada a sessão de recebimento dos envelopes “habilitação” e “proposta de preço” desta Seleção, não mais se admitirá novos proponentes, dando-se inicio a abertura dos envelopes.

11.3 Os membros da Comissão de Seleção e os representantes presentes a sessão rubricarão todos os envelopes, ainda fechados.

11.4 Do ato da abertura dos envelopes será lavrada ata circunstanciada da qual deverão constar às observações ou declarações de qualquer dos proponentes presentes que assim julgar necessário, devendo a mesma ser assinada pela Comissão de Seleção e por todos os representantes presentes.

11.5 Os envelopes (Proposta de Preço) serão abertos em primeiro lugar e os documentos neles contidos serão rubricados pelos membros da Comissão de Seleção e pelos representantes das proponentes participantes da sessão.

11.6 A Comissão de Seleção analisará a Proposta de Preço, para verificação do cumprimento das exigências deste Edital. Depois de analisadas, as Propostas de Preço serão classificadas em ordem crescente, lavrando-se a ata, e as proponentes serão comunicadas quanto à referida classificação, ocasião em que será concedido prazo de 5 (cinco) dias úteis para que as partes interessadas interponham os recursos que entenderem cabíveis.

11.7 Havendo recursos, assim como suas eventuais impugnações, a Comissão de Seleção, após o seu julgamento dará prosseguimento aos trabalhos, em nova sessão pública convocada mediante publicações no Diário Oficial do Estado de São Paulo e site da Fundação Padre Anchieta, importando em preclusão do proponente desclassificado do direito de participar da fase subsequente.

11.8 Manifestando os licitantes expressa renúncia ao prazo recursal (item 11.6), a sessão prosseguirá.

11.9 Depois de encerrada a fase de análise da Proposta de Preço (Envelope “A”), será aberto o Envelope “B” (Documento de Habilitação), do primeiro classificado.

11.9.1 Os Envelopes “B” das proponentes desclassificadas na fase de análise de propostas, serão devolvidos as proponentes após

o julgamento ou denegação de recursos, havendo.

11.10 Por ocasião da abertura do Envelope “B”, o procedimento será o mesmo adotado para o “Envelope A” – Proposta de Preço.

11.11 A proponente melhor classificada, ou seja, que apresentar os melhores preços, somente será declarada vencedora se atender aos requisitos de habilitação.

11.12 É expressamente proibida, sob qualquer alegação, a abertura, no recinto de realização da Seleção, dos envelopes de “Documentos de Habilitação” das empresas desclassificadas.

11.13 Somente os representantes credenciados das proponentes terão direito de usar da palavra, rubricar propostas, apresentar reclamações ou recursos, em nome das licitantes.

12 DA ANÁLISE E JULGAMENTO DAS PROPOSTAS

12.1 A análise das propostas visará a verificação do atendimento das condições estabelecidas neste Edital de Convocação Geral, sendo desclassificada a proposta que:

estiver em desacordo com as exigências estabelecidas neste Edital ou incompatível com os preços correntes no mercado;

que apresente preços globais ou unitários simbólicos, irrisórios ou de valor zero, incompatíveis com os preços de mercado;

omitir qualquer elemento solicitado neste Edital.

12.2 Não serão consideradas, para fins de julgamento da proposta:

oferta de vantagem não prevista neste Edital e nem preço ou vantagem baseados nas ofertas dos demais proponentes;

oferta de prazo ou condições diferentes dos fixados neste Edital.

12.3 Na hipótese de inabilitação ou desclassificação das propostas de todos as proponentes, a Fundação Padre Anchieta poderá fixar aos licitantes o prazo de 8 (oito) dias uteis para a apresentação de nova documentação ou de outra proposta.

12.4 Após a entrega da PROPOSTA, nenhuma informação ou documentação adicional será aceita pela Comissão de Seleção ou considerada no julgamento, exceto eventuais esclarecimentos que esta julgue necessários, conforme mencionado a seguir:

12.4.1 a Comissão de Seleção solicitará, por escrito, esclarecimentos sobre quaisquer aspectos da documentação, conforme o caso requeira. As respostas dos PROPONENTES deverão ser prestadas também por escrito, vedada a inclusão, de qualquer informação ou documento que deveria constar originalmente da Documentação de Habilitação Preliminar.

12.5 **O julgamento das propostas será procedido, sendo considerada**

vencedora a proposta que, atendendo a todas as condições deste Edital de Convocação Geral, oferecer o menor preço, considerado como tal o valor correspondente ao menor Total Geral, homogeneizado no caso de PROPONENTES ESTRANGEIRAS OU PROPONENTES BRASILEIRAS REPRESENTANTES DE EMPRESAS ESTRANGEIRAS.

12.6 Na hipótese de ocorrência de empate entre duas ou mais PROPOSTAS, como critério de desempate, será assegurada preferência, sucessivamente, aos equipamentos:

produzidos no Brasil;

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

12.6.1 Persistindo o empate entre duas ou mais PROPOSTAS, mesmo após a aplicação dos critérios dispostos no item 12.6, será adotado o sorteio, como último critério de desempate, a ser realizado em data previamente estabelecida, para o qual serão convocados todos os PROPONENTES classificados.

12.7 Os envelopes “B” (Habilitação) das empresas classificadas na fase de proposta ficarão lacrados em poder da Comissão de Seleção até a assinatura do contrato, após o que serão devolvidos aos licitantes.

13 DO RECEBIMENTO DO EQUIPAMENTO:

13.1 Por ocasião do recebimento dos equipamentos, a Fundação Padre Anchieta reserva-se o direito proceder a inspeção de qualidade dos mesmos e a rejeitá-lo, no todo ou em parte, se estiver em desacordo com as especificações técnicas (Anexo I), obrigando-se a proponente contratada a promover a devida substituição, observados os prazos contratuais.

13.2 O aceite do produto, pela Fundação Padre Anchieta, não exclui a responsabilidade civil da proponente contratada por vícios de qualidade ou técnico do produto ou em desacordo com as especificações estabelecidas neste Edital, verificadas posteriormente.

13.3 Os equipamentos serão recusados se:

13.1 forem entregues com as marcas e especificações diferentes das contidas na proposta da Contratada, conforme Memorial Descritivo (Anexo I).

13.2 apresentarem avarias.

13.4 Todos os equipamentos deverão ser novos e sem prévio uso.

13.5 Correrão por conta da proponente vencedora, no que couber, as despesas para efetivo atendimento ao objeto desta Seleção, tais como embalagens, seguro, transporte, tributos, seguro, encargos trabalhistas e previdenciários.

14 DAS SANÇÕES PARA O CASO DE INADIMPLEMENTO

14.1 Se a Contratada inadimplir, no todo ou em parte, ficará sujeita, sem prejuízo das sanções previstas na legislação própria, às estabelecidas na Resolução FPA nº 005/PR/05, de 10/08/05, desta Fundação (Anexo VII).

15 DOS RECURSOS E DAS IMPUGNAÇÕES

15.1 Até 02 (dois) dias úteis, antes da data fixada para recebimento das propostas, qualquer interessado poderá solicitar esclarecimentos, providências ou impugnar o ato convocatório desta Convocação Geral.

15.2 Não serão reconhecidas as impugnações enviadas por fax ou, com os respectivos prazos legais vencidos.

15.3 A ausência de resposta da Fundação à impugnação apresentada, não impedirá a proponente de participar da abertura desta Seleção, sendo esta respondida, posteriormente, na hipótese da impugnação não prejudicar as propostas.

15.4 Acolhida a petição contra o ato convocatório, será designada nova data para a realização do certame, observando-se os prazos, no caso de alteração do teor das propostas.

15.5 Comunicado o julgamento da proposta, habilitação, da revogação ou da anulação desta licitação, caberá Recurso Administrativo, no prazo de 05 (cinco) dias úteis.

15.6 Interposto o recurso, será comunicado aos demais proponentes, que poderão impugná-lo no prazo de 05 (cinco) dias úteis.

15.7 Os Recursos cabíveis deverão ser interpostos no prazo de 5 (cinco) dias úteis, contados da data de divulgação da decisão recorrida, sendo dirigidos a Comissão Seleção, que poderá reconsiderar sua decisão no prazo de 05 (cinco) dias úteis.

15.8 Decididos os recursos e constatada a regularidade dos atos praticados, a Comissão de Seleção adjudicará seu objeto e encaminhará o processo devidamente instruído, à autoridade competente para homologação da contratação.

16 DO CONTRATO

16.1 A contratação decorrente desta Seleção será formalizada mediante celebração de termo de contrato, cuja minuta constitui o **Anexo VIII** do presente Edital.

16.1.1 O contrato será devidamente adaptado considerando o tipo de empresa contemplada, em conformidade com os itens 5, 7 ou 9 deste Edital.

16.2 A Fundação convocará regularmente a empresa vencedora do presente certame para assinar o Contrato, no prazo de 5 (cinco) dias úteis, após a publicação do ato da homologação.

16.3 A vigência do Contrato será pelo período de 6 (seis) meses e terá início na data de sua assinatura.

16.4 É facultado à Fundação, quando o convocado não assinar o Termo de Contrato, no prazo e condições estabelecidos, convocar as proponentes remanescentes, pela ordem de classificação, para fazê-lo

nas mesmas condições propostas pelo primeiro classificado, sem prejuízo das penalidades cabíveis ao licitante desistente.

16.5 A CONTRATADA fica obrigada a aceitar, nas mesmas condições contratadas, os acréscimos ou supressões que se fizerem necessários ao objeto, a critério exclusivo da CONTRATANTE, até o limite de 25% (vinte e cinco inteiros percentuais) do valor atualizado do CONTRATO.

16.5.1 Eventual alteração será obrigatoriamente formalizada por meio de Termo Aditivo.

16.6 Constituem motivo para rescisão do contrato:

o não cumprimento, total ou parcial, ou o cumprimento irregular ou insatisfatório de cláusulas do contrato;

o atraso injustificado na entrega dos equipamentos;

a subcontratação total ou parcial do objeto do contrato, sem autorização desta Fundação;

a associação com terceiros, a cessão ou transferência total ou parcial do contrato;

a fusão, incorporação, cisão ou dissolução da contratada ou qualquer alteração social que possa, a critério desta Fundação Padre Anchieta, prejudicar a execução do contrato;

o não atendimento das determinações regulares desta Fundação;

o requerimento de recuperação judicial ou extrajudicial ou a decretação de falência da contratada, ou o protesto de títulos, ou emissão de cheques sem a devida provisão de fundos caracterizadores de sua insolvência;

a ocorrência de caso fortuito ou de força maior, devidamente comprovados, que possa impedir a execução do contrato.

16.7 No caso de rescisão contratual será formalmente motivada nos autos do processo, assegurado o contraditório e a ampla defesa.

17 DAS DISPOSIÇÕES FINAIS:

17.1 A entrega da proposta equivale à aceitação, irrestrita, de todas as condições estabelecidas neste Edital.

17.2 Esta Seleção poderá ser revogada por motivos de interesse público decorrente de fato superveniente ou anulada por motivos de ilegalidade no seu procedimento.

17.3 Os esclarecimentos relativos a esta Convocação Geral serão prestados nos dias de expediente, das 9:00 às 12:00 e das 13:00 às 18:00 horas, no Setor de Compras, no endereço indicado no preâmbulo desta, Convocação Geral ou pelo endereço eletrônico HYPERLINK "mailto:licitacao@tvcultura.com.br" licitacao@tvcultura.com.br ou Fax: 3611-1518.

17.4 Os casos omissos na presente Convocação Geral serão solucionados pelo Setor de Compras, situado no endereço indicado no preâmbulo desta, ou pelo endereço eletrônico HYPERLINK "mailto:licitacao@tvcultura.com.br" licitacao@tvcultura.com.br ou Fax:

3611-1518.

17.5 Integram o presente Edital:

ANEXO I - Memorial Descritivo;

ANEXO II – Declaração de Micro e Pequena Empresa;

ANEXO III – Declaração CAUFESP;

ANEXO IV - Declaração de situação regular perante o Ministério do Trabalho;

ANEXO V - Declaração de que inexiste impedimento legal para licitar;

ANEXO VI – Modelo de Procuração;

ANEXO VII - Cópia da Resolução FPA nº 005/PR/2005;

ANEXO VII - Minuta de Contrato/ Termo de Ciência e de Notificação;

São Paulo, 05 de setembro de 2014.

Marcos P. da Silva
Coord. de Suprimentos

Roberto Lima
Setor de Compras

ANEXO I

MEMORIAL DESCRITIVO

Objetivo: Compra de equipamentos para melhorar a estabilidade do acesso à rede local, rede metro ethernet e Internet.

Item:	Quantidade:	Descrição:
01	**01**	**Sistema de Wireless com 50 antenas**

Sistema para rede Wireless corporativo composto por controlador e 50 antenas.

Especificações gerais do Controlador:

Wireless Controller com suporta no mínimo 50 AP (Access Point) Conectados para gerenciamento, suportara no mínimo 1000 clientes WLAN;

LAN via portas PoE (Power over Ethernet);

Gestão de RF em tempo real e informações históricas sobre a interferência de RF que afeta o desempenho da rede em controladores;

Segurança Global End-to-End, CAPWAP, (DTLS) criptografia;

End-to-end de voz, Suporte as Comunicações Unificadas para melhor colaboração por meio de mensagens, presença e conferência;

Suportar telefones IP Wireless para serviços de baixo custo, de voz em tempo real;

Padrões sem fio IEEE 802.11a, 802.11b, 802.11g, 802.11d, WMM/802.11e, 802.11h, 802.11k, 802.11n, 802.11r, 802.11u, 802.11w;

Wired / Switching / Routing IEEE 802.3 10BASE-T, IEEE 802.3u especificação 100BASE-TX, 1000BASE-T e IEEE 802.1Q VLAN;

Data Requets for Comments (RFC) RFC 768 UDP, RFC 791 IP, RFC 2460 IPv6, RFC 792 ICMP, RFC 793 TCP, RFC 826 ARP, RFC 1122 Requisitos para a Internet Hosts, RFC 1519 CIDR, RFC 1542 BOOTP, RFC 2131 DHCP, RFC 5415 CAPWAP;

Padrões de Segurança Acesso Wi-Fi Protected (WPA), IEEE 802.11i (WPA2, RSN), RFC 1321 MD5 Message-Digest Algorithm, RFC 1851 O ESP Triple DES Transform, RFC 2104 HMAC: hash para autenticação Mensagem, RFC 2246 protocolo TLS Versão 1.0, RFC 2401 Arquitetura de Segurança para o Internet Protocol, RFC 2403 HMAC-MD5-96 dentro de ESP e AH, RFC 2404 HMAC-SHA-1-96 dentro de ESP e AH, RFC 2405 ESP DES-CBC Cipher Algorithm com explícita IV, RFC 2406 encapsular IP Security Payload (ESP), RFC 2407 Interpretação para ISAKMP, RFC 2408 ISAKMP, RFC 2409 IKE, RFC 2451 ESP CBC-Mode Cipher Algoritmos, RFC 3280 Internet X.509 PKI certificado e CRL perfil ou RFC 5280, RFC 3602 A AES-CBC Cipher Algorithm e sua utilização com IPsec, RFC 3686 Usando o modo de contador AES com IPsec ESP, RFC 4347 Datagram Transport Layer Security, RFC 4346 protocolo TLS Versão 1.1;

Criptografia, WEP ou WPA/WPA-2, Temporal Key Integrity Protocol-Message Integrity Check (TKIP-MIC): RC4 de 40, 104 e 128 bits (chaves estáticas e compartilhadas), Advanced Encryption Standard (AES): CBC, CCM, Contador Modo com Cipher Block Chaining Mensagem Authentication Código Protocol (CCMP), DES: DES-CBC, 3DES, Secure Sockets Layer (SSL) e Transport Layer Security (TLS): 128-bit RC4 e RSA 1024 - e 2048-bit, DTLS: AES-CBC;

Authentication, Authorization, and Accounting (AAA), IEEE 802.1X, RFC 2548 Microsoft

RADIUS, RFC 2716 PPP EAP-TLS, Autenticação RADIUS RFC 2865, RFC 2866 RADIUS Accounting, RFC 2867 RADIUS Túnel, RFC 3576 Dynamic Extensions Autorização para RADIUS, RFC 3579 RADIUS Suporte para EAP, RFC 3580 Diretrizes IEEE 802.1X RADIUS, RFC 3748 Extensible Authentication Protocol, A autenticação baseada em Web, TACACS suporte para usuários administradores;

Suporte a gerenciamento, SNMP v1, v2c, v3, RFC 854 Telnet, RFC 1155 Informações para IP baseados em internet TCP / Gestão, RFC 1156 MIB, RFC 1157 SNMP, RFC 1213 SNMP MIB II, RFC 1350 TFTP, RFC 1643 Ethernet MIB, RFC 2030 SNTP, RFC 2616 HTTP, RFC 2665 tipos Ethernet como interface MIB, RFC 2674 Definições de objetos gerenciados para Pontes com classes de tráfego, filtragem Multicast e extensões virtuais, RFC 2819 RMON MIB, RFC 2863 interfaces grupo MIB, RFC 3164 Syslog,RFC 3414-Based User Security Model (USM) para SNMPv3, RFC 3418 MIB para SNMP, RFC 3636 Definições de objetos gerenciados para IEEE 802.3 MAUs;

Possuir interfaces de gerenciamento para uso no Wireless Control System, Web: HTTP / HTTPS gerenciador de dispositivos individuais, interface de linha de comando: Telnet, SSH, porta serial;

Possuir interfaces, porta de Console: conector RJ-45,Rede: Quatro 1 Gbps Ethernet (RJ-45), LEDs indicadores: Link Atividade (cada porta Ethernet 1 Gigabit), Power, Status, Alarme;

Padrões de Temperatura, Operação: 32 a 104 ° F (0 a 40 ° C), Armazenagem: -13 a 158 ° F (-25 a 70 ° C), Umidade de operação: 10 a 95 por cento, sem condensação, Umidade de armazenamento: Até 95 por cento, Adaptador de energia: Poder de entrada: 100 a 240 VAC; 50/60 Hz, A dissipação de calor: 72 BTU / hora;

Integração com Ambiente Microsoft, Active Directory, ldap;

Payment Card Industry apoio (PCI);

Suporte detecção de ponto de acesso não autorizado;

Detectar usuários mal-intencionados, possuir envio de alertas;

Deve ser fornecido kit para montagem em rack padrão 19”;

Deve ser fornecido com documentação técnica e manuais que contenham informações suficientes para possibilitar a instalação, configuração e operacionalização do equipamento;

Fornecer garantia e suporte total por um período de 12 meses com atendimento 8x5xNBD realizada pelo fabricante no Brasil;

Especificações gerais Antenas/Access Point:

Suporte para integrar com Wireless Controller;

LAN via portas PoE (Power over Ethernet);

Suporte 802.11n, 3 x 3 multiple-input multiple-output (MIMO) with two spatial streams, Maximal ratio combining (MRC), 20- and 40-MHz channels, PHY data rates up to 300 Mbps, Packet aggregation: A-MPDU (Tx/Rx), A-MSDU (Tx/Rx), 802.11 dynamic frequency selection (DFS) (Bin 5);

Padrões sem fio IEEE 802.11a, 802.11b, 802.11g, 802.11d, WMM/802.11e, 802.11h, 802.11k, 802.11n, 802.11r, 802.11u, 802.11w, 802.11ac;

Suporte data rates, 802.11a: 6, 9, 12, 18, 24, 36, 48, and 54 Mbps, 802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48 e 54 Mbps, 802.11n (2,4 GHz [1] e 5 GHz);

Banda de frequência de 20 MHz.;

Antena Integrada de 2.4 GHz, 4.0 dBi ganho, largura de feixe horizontal de 360 °, • 5 GHz, o ganho de 4,0 dBi, feixe horizontal de 360 °;

Entrada auxiliar para Antena Externa;

Possuir interface de rede 10/100/1000BASE-T com detecção automática (RJ-45);

Possuir porta de console de gerenciamento (RJ-45);

Possuir LED de status indica o estado do carregador de inicialização, o status da associação, estado de funcionamento, os avisos do carregador de inicialização, erros de boot loader;

Padrões sem fio IEEE 802.11a, 802.11b, 802.11g, 802.11d, WMM/802.11e, 802.11h, 802.11k, 802.11n, 802.11r, 802.11u, 802.11w;

Wired / Switching / Routing IEEE 802.3 10BASE-T, IEEE 802.3u especificação 100BASE-TX, 1000BASE-T e IEEE 802.1Q VLAN;

Data Requets for Comments (RFC) RFC 768 UDP, RFC 791 IP, RFC 2460 IPv6, RFC

792 ICMP, RFC 793 TCP, RFC 826 ARP, RFC 1122 Requisitos para a Internet Hosts, RFC 1519 CIDR, RFC 1542 BOOTP, RFC 2131 DHCP, RFC 5415 CAPWAP;

Padrões de Segurança Acesso Wi-Fi Protected (WPA), IEEE 802.11i (WPA2, RSN), RFC 1321 MD5 Message-Digest Algorithm, RFC 1851 O ESP Triple DES Transform, RFC 2104 HMAC: hash para autenticação Mensagem, RFC 2246 protocolo TLS Versão 1.0, RFC 2401 Arquitetura de Segurança para Internet Protocol, RFC 2403 HMAC-MD5-96 dentro de ESP e AH, RFC 2404 HMAC-SHA-1-96 dentro de ESP e AH, RFC 2405 ESP DES-CBC Cipher Algorithm com explícita IV, RFC 2406 encapsular IP Security Payload (ESP), RFC 2407 Interpretação para ISAKMP, RFC 2408 ISAKMP, RFC 2409 IKE, RFC 2451 ESP CBC-Mode Cipher Algoritmos, RFC 3280 Internet X.509 PKI certificado e CRL perfil, RFC 3602 A AES-CBC Cipher Algorithm com utilização a IPsec, RFC 3686 Usando o modo de contador AES com IPsec ESP, RFC 4347 Datagram Transport Layer Security, RFC 4346 protocolo TLS Versão 1.1, UL 60950-1, CAN/CSA-C22.2 No. 60950-1, UL 2043, IEC 60950-1, EN 60950-1;

Criptografia, WEP ou WPA/WPA-2, Temporal Key Integrity Protocol-Message Integrity Check (TKIP-MIC): RC4 de 40, 104 e 128 bits (chaves estáticas e compartilhadas), Advanced Encryption Standard (AES): CBC, CCM, Contador Modo com Cipher Block Chaining Mensagem Authentication Código Protocol (CCMP), DES: DES-CBC, 3DES, Secure Sockets Layer (SSL) e Transport Layer Security (TLS): 128-bit RC4 e RSA 1024 - e 2048-bit, DTLS: AES-CBC;

Authentication, Authorization, and Accounting (AAA), IEEE 802.1X, RFC 2548 Microsoft RADIUS, RFC 2716 PPP EAP-TLS, Autenticação RADIUS RFC 2865, RFC 2866 RADIUS Accounting, RFC 2867 RADIUS Túnel, RFC 3576 Dynamic Extensions Autorização para RADIUS, RFC 3579 RADIUS Suporte para EAP, RFC 3580 Diretrizes IEEE 802.1X RADIUS, RFC 3748 Extensible Authentication Protocol, A autenticação baseada em Web, TACACS suporte para usuários administradores;

Suporte a gerenciamento, SNMP v1, v2c, v3, RFC 854 Telnet, RFC 1155 Informações para IP baseados em internet TCP / Gestão, RFC 1156 MIB, RFC 1157 SNMP, RFC 1213 SNMP MIB II, RFC 1350 TFTP, RFC 1643 Ethernet MIB, RFC 2030 SNTP, RFC 2616 HTTP, RFC 2665 Ethernet como interface MIB, RFC 2674 Definições de objetos gerenciados para Pontes com classes de tráfego, filtragem Multicast e extensões virtuais, RFC 2819 RMON MIB, RFC 2863 interfaces grupo MIB, RFC 3164 Syslog,RFC 3414-Based User Security Model (USM) para SNMPv3, RFC 3418 MIB para SNMP, RFC 3636 Definições de objetos gerenciados para IEEE 802.3 MAUs;

Possuir interfaces de gerenciamento para uso no Wireless Control System, baseado na

Web: HTTP / HTTPS gerenciador de dispositivos individuais, interface de linha de comando: Telnet, SSH, porta serial;

Possuir Wi-Fi Multimedia (WMM ™), FCC OET Bulletin-65C, RSS-102;

Possuir acessórios para fixação em parede ou teto.

Deve vir acompanhado de fonte de alimentação

Deve ser fornecido com documentação técnica e manuais que contenham informações suficientes para possibilitar a instalação, configuração e operacionalização do equipamento;

Fornecer garantia e suporte total por um período de 12 meses com atendimento 8x5xNBD realizada pelo fabricante no Brasil;

Especificações gerais Antenas:

Antena externa - 802.11n - 2 dBi (2,4 GHz), 4 dBi (para 5 GHz)

Faixa de Freqüência 2.4 GHz, 5 GHz;

Gain 2 dBi (para 2,4 GHz), 4 dBi (para 5 GHz);

Antena Dual-band dipolo;

Faixa de frequência de operação 2400-2500 MHz ou 5150-5850 MHz;

Impedância de entrada nominal 50 Ohms;

VSWR Inferior a 2:01;

Peak Gain@2.4. GHz 2 dBi;

Ganho Peak @ 5 GHz 4 dBi;

Elevation plane 3dB beamwidth @2.4 GHz 63 graus, Elevation plane 3dB beamwidth @ 5 GHz 39 graus;

Conector ficha RP-TNC;

Requisitos do sistema com suporte a operação simultânea na faixa de 2,4 GHz e a banda de 5 GHz e que as portas têm de antena de banda dupla;

Antena com base articulada que pode ser rodado 360 graus no ponto de ligação e de 0 a

90 graus no seu conjunto;

Deve ser fornecido com documentação técnica e manuais que contenham informações suficientes para possibilitar a instalação, configuração e operacionalização do equipamento;

Fornecer garantia e suporte total por um período de 12 meses com atendimento 8x5xNBD realizada pelo fabricante no Brasil;

Especificações gerais do sistema:

Fornecimento de Ponto de Acesso WiFi Externo, novo e sem uso anterior. O modelo ofertado deverá estar em linha de produção, sem previsão de encerramento de fabricação na data de entrega da proposta.

Deve possuir certificação da Wi-Fi Alliance para 802.11a/b/g e 802.11n draft 2.0 ou superior;

Deve ser homologado pela ANATEL;

Deve ser capaz de operar simultaneamente nos padrões 802.11a/n e 802.11b/g/n, através de rádios independentes (Dual Radio AP);

Deve ser um equipamento ponto de acesso WiFi para rede local sem fio de uso interno, com antenas aparentes, que atenda os padrões IEEE 802.11b/g/n na faixa de 2.4GHz e 802.11a/n na faixa de 5GHz simultaneamente com configuração via software. O equipamento deve ter capacidade de análise espectral.

Possuir funcionamento em modo autônomo sem a necessidade de controlador. Neste modo, permitir configuração e funcionamento do ponto de acesso sem a necessidade do controlador.

Possuir funcionamento em modo gerenciado por Controlador WiFi para configuração de seus parâmetros, gerenciamento das políticas de segurança, QoS e monitoramento de RF.

Deverá estar logicamente conectado a um Controlador WiFi, inclusive via roteamento da camada de rede OSI, através de rede pública ou privada.

Deve implementar cliente DHCP, para configuração automática de rede;

Possuir mecanismo de funcionamento para trabalhar com Controladores WiFi em redundância (principal e redundante).

Deve poder operar de tal forma que realize o chaveamento (switching) do tráfego local dos usuários sem que este tráfego tenha que passar através do(s) Controlador(es) WiFi - operação em modo de “chaveamento de tráfego local”.

Operando no modo de “chaveamento de tráfego local”, o controlador WiFi e os pontos de acesso devem:

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

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

Uma vez que a comunicação entre o ponto de acesso e o(s) Controlador(es) WiFi seja interrompida por qualquer motivo, como por exemplo falha no link WiFi ou no(s) próprio(s) Controlador(es) WiFi, o ponto de acesso WiFi em modo de chavemaento de tráfego local deve possuir meios de continuar operando e ter funcionalidade que permita que os usuarios efetuem roaming sem qualquer prejuízo de acesso aos mesmos.

Deve permitir a operação de usuários configurados nos padrões IEEE 802.11b/g/n e 802.11a/n simultaneamente.

Atender os seguintes requisitos em 802.11n (faixas de 2.4GHz e 5GHz): 3x3 multiple-input multiple-output (MIMO); operar em Canais de 20MHz para 2,4GHz e possibilitar channel bounding ou canal de 40 MHz para 5GHz.

Possuir pelo menos as seguintes taxas de transmissão e com fallback automático: IEEE 802.11 a/g: 54, 48, 36, 24, 18, 12, 9 e 6 Mbps.

Possuir pelo menos as seguintes taxas de transmissão e com fallback automático: IEEE 802.11n: MSC0 – MCS15 (6.5Mbps - 300Mbps).

Possuir capacidade de selecionar automaticamente o canal de transmissão.

Implementar o protocolo de enlace CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) para acesso ao meio de transmissão.

Operar nas modulações DSSS e OFDM.

Permitir o ajuste dinâmico de nível de potência e canal de rádio de modo a otimizar o tamanho da célula de RF.

Possuir suporte a pelo menos 16 SSIDs.

Possuir suporte a pelo menos 16 Vlans.

Permitir habilitar e desabilitar a divulgação do SSID.

Possuir padrão WMM (Wi-Fi Multimedia) da Wi-Fi Alliance para priorização de tráfego.

Não deve haver licença restringindo o número de usuários por ponto de acesso. O Ponto de Acesso deve permitir, no mínimo, 128 usuários por rádio.

O Ponto de acesso deve permitir configuração de base de usuários local para utilização com protocolo 802.1X, com no mínimo 100 usuários. Caso o ponto de acesso não possua capacidade de armazenamento de usuários refira-se ao item 1.1.1.12.4.

Deve possuir no mínimo 02 rádios (dual radio) operando simultaneamente em frequências distintas.

Possuir potência máxima de transmissão de, no mínimo, 20 dBm para IEEE 802.11a/b/g/n.

Possuir antenas compatíveis com as freqüências de radio dos padrões 2.4GHz e 5GHz com ganho de, pelo menos, 3dBi e 5 dBi, respectivamente, com padrão de irradiação omnidirecional.

Possuir, no mínimo, um valor maximo de transmissão maior ou igual a 22 dBm com todas as antenas habilitadas.

Possuir, no mínimo, uma interface IEEE 802.3 10/100/1000BaseT Ethernet, auto-sensing, auto MDI/MDX, com conectores RJ-45, para conexão à rede local fixa.

Permitir a atualização remota do sistema operacional e arquivos de configuração utilizados no equipamento via interfaces ethernet ou serial (terminal assíncrono).

Possuir no mínimo 01 LED indicativo do estado de operação;

Deve possuir uma trava de segurança compatível à utilizada em desktops e notebooks e que permita a instalação de um cabo de segurança com a finalidade de evitar o furto do equipamento.

Deve implementar um mecanismo de controle de associação de banda, de forma que usuários com capacidade de comunicação 802.11a/b/g/n em 2,4GHz e 5GHz sejam preferencialmente, e sempre que possível, alocados nos canais da banda de 5GHz do Ponto de Acesso, quando os mesmos se associem à rede WLAN.

Implementar balanceamento de carga de usuários de modo automático através de múltiplos pontos de acesso, para otimizar o desempenho quando grande quantidade de usuários estão associados aos pontos de acesso.

Deve permitir a configuração da técnica "beamforming" de transmissão de forma otimizar a relação de sinal ruído e a performance de transmissão de dados para determinados usuários da rede WLAN. Deve perimitir esta formação de banda para cliente 802.11n.

Deve possuir, em conjunto com a controladora, mecanismo de otimização de tráfego multicast para vídeo, permitindo a definição de largura de banda por grupo multicast. Este mecanismo deve permitir que o tráfego de multicast seja enviado aos clientes da rede WiFi na velocidade de conexão destes clientes mesmo que esta velocidade não seja o “rate” mandatório.

Possibilitar a alimentação via padrão PoE (IEEE 802.3af) utilizando apenas uma porta do switch onde estiver conectado.

Possuir estrutura que permita fixação do equipamento em teto e também em parede, devem ser fornecidos os acessórios para que possa ser feita a fixação.

Deve ser entregue com todos os acessórios necessários para operacionalização do equipamento, tais como: kits de instalação, softwares, documentação técnica e manuais que contenham informações suficientes para possibilitar a instalação, configuração e operacionalização.

Possuir varredura de RF nas bandas 802.11 b/g/n e 802.11 a/n para identificação de pontos de acesso intrusos não autorizados (rogues) e interferências no canal habilitado

no ponto de acesso sem impacto no seu desempenho.

Deve implementar o protocolo IEEE 802.1X, com pelo menos os seguintes métodos EAP:

EAP-Transport Layer Security (EAP-TLS);

EAP-TTLS/MSCHAPv2;

PEAPv0/EAP-MSCHAPv2;

PEAPv1/EAP-GTC;

EAP Subscriber Identity Module (EAP-SIM).

Deve suportar a autenticação com geração dinâmica de chaves criptográficas por sessão e por usuário;

Possuir criptografia do tráfego local.

Suportar a autenticação com geração dinâmica de chaves criptográficas por sessão e por usuário;

Implementar WEP (Wired Equivalent Privacy), chaves de 40 bits e 128 bits;

Implementar WPA (Wi-Fi Protected Access com algoritmo de criptografia TKIP e Message Integrity Check-MIC).

Implementar WPA-2 (Wi-Fi Protected Access com algoritmo de criptografia AES, 128 bits);

3Deve ser capaz de atender os usuários e realizar a função de “mesh indoor” ou modo “repetidor” de forma simultânea.

Deve possuir hardware dedicado para a análise de espectro (ASIC) dedicado para esta função localizado dentro do ponto de acesso.

O equipamento deverá suportar a realização de monitoração real-time das frequências de Rádio Frequência (análise espectral) em busca de interferências WiFi e Interferências Não-WiFi.

Quando em operação de monitoração de espectro, as funções de monitoração real-time em Rádio Frequência (análise espectral) devem ser realizadas via hardware, com chipset (ASIC) dedicado para esta função localizado dentro do ponto de acesso.

Quando em operação de monitoração de espectro,, dever detectar e gerar alarmes de interferências WiFi (provenientes de dispositivos padrão IEEE802.11) e detectar, classificar, identificar e localizar em mapa com certa precisão além de gerar alarmes de interferências não-WiFi, tais como Bluetooth, telefones sem fio, câmeras de video sem fio, Microondas e outros

Quando em operação de monitoração de espectro, deve ter a capacidade de mudar de canal caso seja detectada alguma das interferências listadas no item anterior no canal de operação atual e devem permanecer no novo canal caso a interferência seja persistente.

Suportar operar nos seguintes modos: “Modo Local”, “Modo Monitor” e “Modo Analisador de Espectro”.

Operando em “Modo Local” o ponto de accesso deve fornecer informações ao Controlador WiFi ao qual está associado referentes à qualidade do espectro de RF no canal de operação atual ao mesmo tempo que processa dados 802.11 dos usuários da rede WiFi. Deverá fazer tanto a transmissão de dados WiFi quanto a análise de espectro simultaneamente.

Operando em “Modo Monitor” deverá fornecer informações ao Controlador WiFi referente à qualidade do espectro de RF para todos os canais monitorados identificando equipamentos interferentes na rede WiFi e rogue APs.

Operando em “Modo Analisador de Espectro” deverá operar de forma exclusiva apenas para monitorar o espectro de RF de forma a fornecer informações para um software analisador de espectro ou para o software de gerenciamento WiFi em todos os canais de 2.4GHz e 5GHz UNII1, UNII2, UNII2 Ext e UNII3 simultaneamente. Se o equipamento não analisar todo o espectro simultaneamente com um único ponto de acesso em modo monitor, será aceita a quantidade necessária de pontos de acesso para análise espectral dos canais de todas as frequências acima descritas de forma simultânea. Este quantitativo será necessário para cada ponto de acesso monitor inserido na rede e os custos totais devem ser adicionados no ítem.

Ser fornecido com fonte de alimentação com ajuste automático de tensão 110 e 220 volts e freqüência de 60 Hz.

Deve possuir consumo de energia igual ou inferior a 12,95Watts.

O equipamento ponto de acesso deve ser homologado pela ANATEL.

Deve permitir a conexão de usuários em IPv4, IPv6 e Dual-stack.

O equipamento deve ser capaz de implementar 802.11 dynamic frequency selection (DFS).

Deve possuir suporte à 802.11 Cyclic Shift Diversity (CSD).

Deve implementar Maximal Ratio Combining (MRC)

Item:	Quantidade:	Descrição:
02	**02**	**F I R E W A L L – A P P L I A N C E D E SEGURAÇA**

Especificações gerais:

Hardware dedicado para funções de segurança de rede, com as suporte às seguintes funcionalidades: “firewall statefull inspection”, gateway VPN IPSec, gateway VPN Web/ SSL; composto de hardware, software, firmware e acessórios necessários a sua instalação, configuração e operação completas;

Deve ser montável em rack de 19 polegadas (devem ser fornecidos os kits de fixação necessários). O equipamento fornecido deve ocupar no máximo 01 unidade de rack (01 RU).

Dispositivo fisicamente independente, com gabinete e fonte de alimentação próprios, que implemente as funções acima. O equipamento deverá ser uma solução utilizando um único gabinete para montagem em rack padrão 19”, e deve possuir 01 (uma) U (unidade de rack) de altura;

O equipamento deverá possuir fonte de alimentação interna e operar em 110 V ou 220 V; 60Hz com chaveamento automático;

Deve ser fornecido com pelo menos 08 (oito) interfaces UTP 10/100/1000

Deve possuir 02 (duas) portas seriais, sendo uma porta para console e outra porta auxiliar para acesso remoto; e 02 (duas) portas USB 2.0;

Deve suportar o acréscimo de pelo menos 06 (seis) interfaces Gigabit Ethernet

Deve suportar agregação de portas GigabitEthernet. Deve ser possível formar grupos de até 04 portas GigabitEthernet. Deve ser suportado o padrão LACP (Link Aggregation Control Protocol)

Deve suportar pelo menos 500.000 (quinhentos mil) conexões simultâneas em sua tabela de estados.

Deve suportar a criação de pelo menos 20.000 (vinte mil) novas conexões TCP por segundo.

Os valores de desempenho especificados nos ítens 7 e 8 devem ser ofertados de forma

centralizada. Não serão aceitas soluções que se baseiem em combinação de módulos de firewalls em um chassi.

Deve suportar funcionalidade de Stateful Firewall com desempenho mímino de 2 Gbps (dois gigabits por segundo).

Deve suportar taxa de encaminhamento de pelo menos 600.000 (seiscentos mil pacotes por segundo).

Não deve haver restrição de número de usuários simultâneos através do equipamento para a licença de software fornecida para a funcionalidade de Stateful Firewall.

Deve suportar a definição de VLAN trunking conforme padrão IEEE 802.1q. Deve ser possível criar pelo menos 200 (duzentos) interfaces lógicas associadas a VLANs e estabelecer regras de filtragem (Stateful Firewall) entre estas;

Deve construir registro de fluxos de dados relativos a cada sessão iniciada, armazenando para cada uma destas sessões informações tais como endereços de origem e destino dos pacotes, portas TCP (e UDP) de origem e destino, bem como números de seqüência dos pacotes TCP, status dos flags “ACK”, “SYN” e “FIN”.

O equipamento deve permitir a “randomização” do número de seqüência TCP, ou seja, funcionar como um “proxy” de número de seqüência TCP de modo a garantir que um host situado em uma interface considerada “externa” (insegura), sob o ponto de vista de política de segurança do firewall, nunca tenha acesso ao número de seqüência TCP real do host seguro (interno ao firewall) em uma sessão estabelecida entre os referidos hosts;

Possibilitar o registro de toda a comunicação realizada através do firewall e de todas as tentativas de abertura de sessões e conexões que por ele forem recusadas.

Deve suportar agrupamento lógico de objetos (“object grouping”) para criação de regras de filtragem. Deve ser possível criar grupos de pelo menos os seguintes tipos de objetos : hosts, redes IP, serviços. Deve ser possível verificar a utilização (“hit counts”) de cada regra de filtragem (“Access Control Entry”) individualmente, independentemente do fato de a configuração da política ter utilizado o conceito de agrupamento lógico de objetos.

A solução fornecida deve possuir a funcionalidade de “proxy” de autenticação (“authentication proxy”), permitindo a criação de políticas de segurança de forma dinâmica, com autenticação e autorização do acesso aos serviços de rede sendo efetuadas por usuário. Deve ser possível obter as informações de usuário/senha por

meio de pelo menos os seguintes protocolos : HTTP, HTTPS e Telnet. Deve ser possível ao Firewall exigir autenticação inclusive para uso de protocolos que não possuam nativamente recursos de autenticação.

Deve ser possível a integração do Firewall com a solução Microsoft Active Directory (MS-AD), permitindo a criação de políticas de filtragem baseados em usuários e grupos de usuários existentes na base MS AD;

Deve implementar listas de controle de acesso com no mínimo os seguintes campos: IP de Origem, Nome do Usuário/Grupo do AD, IP de Destino, Serviço de origem, Serviço de destino e Ação (permit/deny). O “nome de usuário” deverá ser identificado de forma automática e transparente para o usuário final através de consultas à base MS-AD;

Deve suportar autenticação usando base local de usuários (interna ao equipamento).

Implementar políticas de controle de acesso baseadas em informações de horário (“time-based access control”)

Deve implementar remontagem virtual de fragmentos (“Virtual Fragment Reassembly”) em conjunto com o processo de inspeção stateful. Deve ser possível estabelecer o número máximo de fragmentos por pacotes e timeouts de remontagem.

Possuir suporte a inspeção “stateful” para pelo menos os seguintes protocolos de aplicação: Oracle SQL*Net Access, Remote Shell, FTP, HTTP, SMTP, ILS (Internet Locator Service), LDAP, ESMTP, TFTP.

Deve suportar a tradução do endereço IP carregado em uma mensagem DNS Reply (NAT na camada de aplicação) juntamente com a tradução do endereço IP presente no cabeçalho L3.

Possuir suporte a inspeção stateful dos protocolos de sinalização de telefonia H. 323(v1,v2,v3,v4), SIP (Session Initiation Protocol), MGCP e SCCP. A partir da inspeção dos protocolo de sinalização o firewall deve criar dinamicamente as permissões pertinentes para o tráfego de mídia (RTP/RTCP) entre os telefones envolvidos. Para o protocolo SIP deve ser possível criar dinamicamente e terminar dinamicamente inclusive as conexões com sinalização criptografada (SIP over TLS) e mídia criptografada (Secure RTP).

Possuir capacidade de limitar o número de conexões TCP simultâneas para cada IP de origem (sem necessidade de especificar tal endereço IP).

Possuir capacidade de limitar o número de conexões TCP incompletas (‘half-open’)

simultâneas para cada IP de origem (sem necessidade de especificar tal endereço IP).

Possuir capacidade de limitar o número de conexões TCP simultâneas para um endereço de destino especificado.

Possuir capacidade de limitar o número de conexões TCP incompletas ('half-open') simultâneas para um endereço de destino especificado.

Deve permitir simultaneamente com a implementação "Network Address Translation" a filtragem "stateful" de pelo menos as seguintes aplicações:

H.323 (v1,v2, v3,v4) , Real Time Streaming Protocol (RTSP), SIP (Session Initiation Protocol), MGCP (Media Gateway Control Protocol)

Microsoft Networking client and server communication (NetBIOS over IP)

Oracle SQL*Net client and server communication;

Domain Name System (DNS)

SUN Remote Procedure Call (RPC);

File Transfer Protocol (FTP) – modos "standard" e "passive"

O equipamento deve permitir a inspeção detalhada de conexões HTTP, contemplando, no mínimo, as seguintes funcionalidades:

Verificação de conformidade das requisições HTTP com a RFC 2616 e suporte a bloqueio de requisições não conformes

Verificação do comprimento do "Header" das mensagens HTTP (requisições dos clientes e respostas dos servidores). Deve ser possível bloquear conexões cujos comprimentos do Header HTTP não estejam em conformidade com os valores pré-definidos na política de Segurança aplicada ao equipamento.

Possibilidade de bloqueio de requisições cujo comprimento do URI não esteja dentro dos limites pré-definidos pela Política de Segurança aplicada ao equipamento.

Possibilidade de bloqueio de requisições cujo comprimento da parte de dados do HTTP ("content-length") não esteja dentro dos limites pré-definidos pela Política de Segurança aplicada ao equipamento.

Possibilidade de bloqueio de conexões HTTP de acordo com o tipo de conteúdo por elas transportado. O equipamento deve prover suporte a filtragem de no mínimo os seguintes

tipos de conteúdo : audio/mpeg, audio/x-ogg, audio/x-adpcm, audio/x-wav , image/jpeg, image/x-3ds, image/portable-bitmap, image/cgf, image/png, image/x-bitmap, image/x-portable-greymap, image/gif, , video/-flc, video/sgi, video/x-mng, video/mpeg, video/x-avi, video/x-msvideo, video/quicktime, video/x-fli, video/x-niff, video/tiff , application/zip, application/x-gzip, application/postscript

Possibilidade de bloqueio de requisições HTTP de acordo do método (“request method”) utilizado pelo cliente web.

Deve possuir capacidade de filtrar “applets” Java e controles ActiveX.

O equipamento deve permitir a inspeção detalhada de conexões FTP , contemplando, no mínimo, as seguintes funcionalidades :

Permitir o bloqueio seletivo de comandos utilizados em requisições FTP (“request commands”).

Verificar se os comandos “PORT” e “PASV” foram truncados, permitindo o “reset” da sessão TCP caso isto tenha ocorrido.

Garantir que o comando “PORT” só ocorra na parte cliente da conexão FTP, sendo possível promover o “reset” da sessão TCP caso tal comando seja detectado em uma mensagem enviada por um servidor FTP.

Garantir que o comando “PASV” só ocorra na parte servidor da conexão FTP, sendo possível promover o “reset” da sessão TCP caso tal comando seja detectado em uma mensagem enviada por um cliente FTP.

Verificar a negociação de portas TCP a serem usadas na conexão, permitindo a finalização da sessão TCP caso uma porta entre 1 e 1024 tenha sido negociada.

Permitir a substituição da resposta enviada pelo servidor FTP a um comando “SYST” para evitar que o “system-type” do servidor seja revelado aos clientes.

Possuir suporte a tecnologia de Firewall Virtual, sendo fornecido com pelo menos 2 (duas) instâncias totalmente isoladas entre si. O equipamento fornecido deve suportar expansão para pelo menos 10 instâncias simultâneas, por meio de licenciamento de software. Dentro de cada instância de Firewall deve ser possível definir regras independentes de filtragem, regras de NAT, rotas e VLANs alocadas.

Dentro de cada instância de Firewall deve ser possível alocar no mínimo os seguintes

tipos de recursos: número conexões simultâneas, número de endereços IP traduzidos, número de sessões de gerenciamento simultâneas, número de endereços MAC.

Dentro de cada instância de Firewall deve ser possível limitar (promover “rate limiting”) os seguintes recursos: taxa de estabelecimento de novas conexões, taxa de inspeção de aplicações, taxa de transmissão de mensagens Syslog.

A exaustão dos recursos alocados para uma dada instância de Firewall não deve ter influência sobre a operação das demais instâncias.

Deve suportar a adição de novas instâncias virtuais através de licenças de software. Devem ser suportadas pelo menos 100 instâncias virtuais de Firewall.

A solução deve suportar a terminação de pelo menos 1000 (mil) túneis IPSEC VPN simultaneamente. Devem ser fornecidas licenças de Cliente IPSEC VPN para pelo menos 1.000 usuários.

Deve haver versões do cliente IPSEC VPN fornecido com o concentrador para, no mínimo, os seguintes sistemas operacionais : Windows XP, Windows Vista, Windows 7 e Linux (Intel).

A solução deve suportar a terminação de pelo menos 1.000 (mil) sessões SSL-VPN simultaneamente.

Devem ser fornecidos clientes de VPN SSL para uso em pelo menos 1000 dispositivos móveis (tablets, smartphones). Devem ser suportados, no mínimo, os sistemas operacionais Apple iOS e Google Android.

Deve ser suportada a terminação simultânea de túneis IPSEC e SSL-VPN, de modo que se suporte um total de pelo menos 750 (setecentos e cinquenta) usuários simultâneos para VPN de acesso remoto. Caso a solução não suporte todas as especificações de VPN (SSL e IPSEC) em um único chassis, poderá ser fornecido um concentrador VPN externo, do mesmo fabricante do firewall, desde que conectado a este através de pelo menos 02 interfaces 1Gbps. Tais interfaces 1Gbps deverão ser distintas daquelas originalmente especificadas para o firewall e não podem ser contabilizadas para atendimento aos ítens 4 e 5.

Devem ser fornecidas 1000 licenças de cliente SSL-VPN e 100 licenças para operação SSL-VPN no modo clientes.

Deve ser possível ao concentrador terminar túneis IPSEC do tipo “site-to-site” (LAN-to-

LAN)

O concentrador VPN deve suportar a terminação simultânea de conexões IPSEC VPN e SSL VPN.

Suporte à criação de VPNs IPSEC com criptografia 168-bit 3DES, 128-bit AES e 256-bit AES. Deve possuir desempenho de no mínimo 400Mbps para tratamento de conexões IPSEC (padrões AES e 3DES). A criptografia deve ser realizada em hardware dedicado.

Deve ser possível ao concentrador fornecido operar em modo “cluster”. O líder do “cluster” deve ser responsável por direcionar conexões para os demais membros do “cluster”.

Suportar alta disponibilidade das conexões IPSEC VPN, permitindo a utilização de uma segunda unidade em “standby”. Em caso de falha de uma das unidades, não deverá haver perda das conexões ativas (stateful failover) e a transição destas conexões entre as duas unidades deve ser completamente transparente para o usuário final.

Deve suportar negociação de túneis VPN IPSEC utilizando o protocolo IKE (Internet Key Exchange) nas versões 1 e 2, para garantir a geração segura das chaves de criptografia simétrica.

Suporte à integração com servidores RADIUS para tarefa de autenticação, autorização e accounting (AAA) dos usuários que ganharam acesso via conexão VPN (“Extended Authentication”)

O concentrador VPN deve ser capaz de passar pelo menos os seguintes parâmetros para o cliente : endereço IP do cliente VPN, endereço IP do WINS Server, endereço IP do DNS Server e Default Domain Name. A configuração do cliente VPN deve ser completamente automatizada, sendo exigida do usuário apenas a instalação do cliente VPN em seu PC.

O concentrador de VPN deve ser capaz de configurar nos VPN clients uma lista de acesso de “split tunneling”, de modo a explicitar quais as redes podem continuar sendo acessíveis de forma direta (sem IPSEC) durante uma conexão VPN à rede corporativa. Deve também ser possível a operação no modo “all tunneling”, em que todo o tráfego do VPN client só poderá ser transportado através da conexão protegida.

O concentrador deve permitir a criação de “banners” personalizados para indicar se houve sucesso ou falha na requisição de acesso VPN e, em caso de sucesso, mensagens de natureza administrativa.

Deve suportar o uso de certificados digitais emitidos pela autoridade certificadora ICP Brasil para autenticação das VPNs IPSec e SSL.

O concentrador VPN deve permitir a criação de base de usuários e grupos de usuários que compartilham a mesma política de segurança de forma interna ao equipamento.

O concentrador deve permitir a criação de pools de endereços IP de VPN (endereços privados) internamente ao equipamento.

O concentrador VPN deve se integrar com servidores RADIUS para que estes façam a atribuição dos endereços IP de VPN (endereços privados) aos clientes .

O concentrador deve permitir que os endereços IP de VPN (endereços privados) sejam obtidos a partir de um servidor DHCP especificado pelo administrador do sistema.

Deve ser possível a associação de diferentes pools de endereços IP aos diferentes grupos de usuários que solicitarem conexão ao concentrador VPN.

O concentrador deve permitir a definição dos horários do dia e dos dias das semana em que um dado usuário pode requisitar uma conexão VPN.

O concentrador VPN deve suportar NAT (Network Address Translation)

O concentrador VPN deve suportar operação no modo transparente a NAT (“NAT-transparent mode”), permitindo a utilização dos clientes VPN em ambientes em que já se efetue PAT (Port Address Translation)

O concentrador VPN deve permitir a terminação de conexões no modo IPSEC over TCP.

O concentrador VPN deve permitir a terminação de conexões no modo IPSEC over UDP

Deve ser possível visualizar no concentrador o número de conexões VPN estabelecidas em um dado instante e os respectivos usuários que estão fazendo uso destas.

Deve ser posível visualizar no cliente VPN o endereço privado adquirido durante a negociação da conexão IPSEC.

Deve ser possível definir vários templates de conexão no cliente VPN antes que seja enviado para instalação no computador do usuário final. Estes templates devem conter o endereço IP ou nome DNS associado ao concentrador e parâmetros definidores das Security Associations (SAs) a serem usadas nas fases 1 (IKE) e 2 (IPSEC) de negociação dos túneis, incluindo algoritmo de criptografia (DES, 3DES,AES), algoritmo de hash (MD5, SHA), grupo Diffie-Hellman (1, 2, 5) e tempo de duração (“lifetime”) da

conexão. A configuração destes parâmetros deve ser totalmente transparente para o usuário do VPN client.

Deve suportar a utilização de certificados digitais padrão X.509 para o próprio concentrador VPN, possuindo integração com pelo menos as seguintes Certificate Authorities (CAs) : Baltimore, Entrust, Verisign, Microsoft e RSA. Os clientes VPNs devem ter o mesmo suporte a certificados digitais. Deve ser suportado o protocolo SCEP para “enrollment” automático na autoridade certificadora (tanto para o concentrador como para os clientes IPSEC).

O concentrador VPN deve suportar protocolo Syslog para geração de logs de sistema.

Para SSL VPN devem ser suportadas no mínimo as seguintes aplicações transportadas sobre conexões SSL para o concentrador : HTTP, POP3S, IMAP4S, SMTPS.

Para SSL VPN devem ser suportados, via “Port Forwarding”, no mínimo as seguintes aplicações : Telnet, SSH, FTP over SSH, Windows Terminal Services, Outlook/Outlook Express e Lotus Notes.

Deve ser possível criar diferentes grupos de usuários SSL VPN, com definição por grupo, do tipo de serviço permitido sobre as conexões SSL para o concentrador (WEB, e-mail, sistemas de arquivos).

Deve ser possível a criação de portal customizado para acesso SSL VPN. O portal deve refletir os recursos disponíveis (aplicações e URLs acessíveis, possibilidade de download do cliente SSL VPN, "banner de acesso") para o grupo a que o usuário que requisita acesso pertence. Deve ser possível especificar as URLs acessíveis através de conexões SSL VPN.

Deve ser possível acesso SSL-VPN a pelo menos os seguintes aplicativos (Telnet, SSH, VNC, RDP e Citrix) sem necessidade de software cliente na máquina remota. O acesso será viabilizado através de “plug-ins” para browsers.

Deve suportar autenticação SSL-VPN através de teclado virtual apresentado ao usuário.

Deve implementar protocolo DTLS (TLS over UDP) de acordo com a RFC 4748

Deve ser possível realizar verificação de parâmetros na máquina do usuário antes da apresentação das credenciais de identificação ("pre-login") . Deverá ser possível verificar pelo menos os seguintes atributos : Chaves de Registro, Arquivos, Endereços IP, Versão do Sistema Operacional e Certificados Digitais.

Deve ser possível a criação de regras para verificação da conformidade da máquina com a política de segurança. Dever ser possível verificar no mínimo os seguintes elementos : a instalação, habilitação e atualização do software antivírus e anti-spyware e existência de personal firewall habilitado.

Deve ser possível estabelecer, por grupo, os serviços de acesso remoto disponíveis para os usuários deste : IPSEC VPN, SSL-VPN (com cliente), SSL-VPN (sem cliente) e qualquer combinação destes métodos.

Deve ser possível definir no concentrador VPN o mapeamento de atributos LDAP e RADIUS para parâmetros existentes na configuração local de grupos do concentrador. Deve ser possível escolher, para cada grupo, se os parâmetros usados serão os definidos localmente ou os mapeados de um grupo externo LDAP/RADIUS.

Deve ser possível a criação de políticas de SSL VPN dinâmicas baseadas pelo menos nos seguintes parâmetros:

Sistema Operacional Utilizado

Anti-vírus

Anti-spyware

Chave de Registro (existência e valor específico a ela atribuído)

Arquivos do sistema

Existência de um certificado digital na máquina de onde provém a tentativa de acesso

Atributos LDAP

Implementar NTP (Network Time Protocol), conforme RFC 1305, contemplando autenticação MD5 entre os peers.

Deve ser gerenciável via SNMP, SNMPv2c e SNMPv3.

Deve ser gerenciável via porta de console, Telnet, SSHv2 e HTTPS.

Deve ser fornecido com pelo menos uma interface 10/100/1000 dedicada a gerenciamento (out-of-band). Esta interface deverá ser distinta daquelas originalmente especificadas para o firewall e não podem ser contabilizadas para atendimento aos ítens

4 e 5.

Deve possuir mecanismo interno de captura de pacotes. Deve ser possível selecionar através de guias de configuração (“wizards”) quais os pacotes (IP de origem e destino, portas TCP/UDP de origem e destino e interfaces de entrada devem ser capturados).

Deve permitir o armazenamento de pacotes capturados em formato tcpdump.

Deve possuir memória flash para armazenamento de imagem do sistema operacional e arquivos de configuração do equipamento.

Implementar completamente a porção cliente do protocolo TACACS+ para controle de acesso administrativo ao equipamento. Deve ser possível especificar conjuntos de comandos acessíveis a cada grupo de usuários administrativos e cada comando deve ser autorizado individualmente no servidor TACACS+. Todos os comandos executados bem como todas as tentativas não autorizadas de execução de comandos devem ser enviadas ao servidor TACACS+.

Deve vir acompanhado de interface gráfica para gerenciamento das funcionalidades de VPN e Firewall.

Deve implementar, por interface, as funções de DHCP Server, Client e Relay.

Deve suportar a criação de rotas estáticas e pelo menos os seguintes protocolos de roteamento dinâmicos : RIP, RIPv2 e OSPF. Deve suportar a utilização de pelo menos dois processos de roteamento simultâneos e independentes.

Implementar o protocolo PIM (Protocol Independent Multicast) em Sparse Mode

Suporte a operação como IGMP Proxy Agent.

Deve suportar inspeção stateful de tráfego IPv6.

Deve suportar simultaneamente a criação de regras IPv4 e IPv6.

Deve suportar roteamento estático Deve implementar randomização do número de seqüência TCP para conexões TCP que trafegam sobre IPv6.

Deve suportar anti-spoofing (sem uso de ACLs) para endereços IPv6.

Deve suportar pelo gerenciamento sobre IPv6. Devem ser suportados pelo menos os seguintes protocolos de gerência: Telnet, SSH e HTTPS.

Deve suportar stateful failover de conexões IPv6.

Deve suportar agrupamento lógico de objetos IPv6 (redes, hosts, serviços) e criação de regras (ACLs) usando tais objetos.

A solução deverá suportar alta disponibilidade em modo ativo-ativo ou ativo-standby. A transição das conexões entre as duas unidades deve ser completamente transparente para o usuário final. Em qualquer dos modelos deve ser implementada a replicação automática de configurações entre os elementos do cluster.

O appliance fornecido deve suportar (por meio de adição futura de licença de software ou hardware específico) a funcionalidade de IPS (Intrusion Prevention System). A performance mínima para tal serviço deve ser de 600 Mbps. Deve ser possível ao firewall selecionar o tráfego sujeito à análise do IPS.

O sistema de detecção de intrusão deve ser composto por dois elementos : sensor (“probe”) e console de gerenciamento . A probe deverá ser responsável por monitorizar a rede a que está conectada, analisando tanto o cabeçalho(header) como a área de dados(payload) de cada pacote que trafega pela rede citada, de modo a verificar se os referidos pacotes constituem tráfego autorizado

A console de gerenciamento deverá permitir a configuração gráfica dos sensores (“probes”) e receber os alertas e notificações de ataques de todos os sensores que monitoram a rede.

Toda a comunicação entre o sensor e a console de gerenciamento deve ser criptografada.

Deve suportar operação em modo promíscuo (IDS).

Deve suportar operação em modo “in-line” (IPS), descartando pacotes identificados como associados a ataques. Deve ser possível a seleção, por interface, do modo de operação desejado (IPS in-line/IDS). Deve ser possível operar simultaneamente como IPS e IDS.

Deve possuir capacidade de detecção de intrusos e ataques no segmento de rede que está monitorando e analisando

Deve suportar a análise simultânea de tráfego associado a pelo menos 100 VLANs IEEE 802.1q

Deve analisar cada um dos pacotes que trafegam pela rede a que está conectado e

também a relação de tais pacotes com os adjacentes a ele no fluxo de dados da rede (análise de contexto). Imediatamente após a identificação de uma eventual violação da política de segurança o sensor deve enviar um alarme para o software de controle.

Deverá ter uma base de assinaturas com descrição da utilização de cada uma delas e tipos de ataques detectados. Deverá ser possível a atualização gratuita de assinaturas em caso de detecção de novas vulnerabilidades.

Deve suportar a modificação de assinaturas, isto é, permitir a edição de assinaturas existentes na base de dados, ajustando-se ao perfil de tráfego de rede

Deve suportar a criação de assinaturas, isto é, permitir que se possam criar novas assinaturas e anexá-las à base de dados existente, adaptando-se as reais necessidades de tráfego de rede (na criação das novas assinaturas deve ser permitida a utilização de parâmetros de nível 2 a nível 7 do modelo OSI)

Deve ser possível criar assinaturas do tipo “string-match” e associá-las a qualquer porta TCP para verificação da ocorrência de conjunto de caracteres definidos pelo administrador de política de segurança no conteúdo dos pacotes IP que trafegam pela rede.

O software de controle deve ser capaz de enviar alarmes para um sistema de pager ou via e-mail para notificar a violação de uma dada regra de segurança.

O sistema deve registrar informações tais como origem, destino, horário e tipo dos ataques ocorridos.

Deve suportar “Protocol Anomaly Detection” como método de análise de tráfego

Deve suportar verificação de adequação dos protocolos que trafegam na rede às definições destes constantes nas RFCs (análise de “RFC compliance”)

Deve suportar análise “stateful” de pacotes para garantir maior acurácia de detecção (“Stateful Pattern Matching”)

Deve suportar detecção de anomalias de tráfego da Rede (anomalias associadas a definições estatísticas de tráfego)

Deve detectar ataques associados a protocolos que não estejam usando as portas canônicas de serviço (portas padrão reservadas para os protocolos de aplicação)

Deve promover reordenação e remontagem de fragmentos IP antes de efetuar análise.

Deve possuir estrutura de “normalização” de tráfego para que possam combater as técnicas de evasão

Quando da operação em modo “in-line”(IPS) devem ser suportados no mínimo os seguintes tipos de reação (configuráveis por assinatura de ataque) : geração de alerta, gerar trap SNMP, fazer “logging”dos pacotes gerados pelo sistema “vítima”, fazer “logging” dos pacotes gerados pelo sistema que está efetuando o ataque, promover “reset” da conexão TCP, bloquear o pedido de conexão, bloquear o endereço que está gerando o ataque de conexão, negar pacotes associados ao ataque “in-line”

O sistema deve suportar “logging” de sessão via IP (“IP session logging”). Os logs devem ser compatíveis com o formato “TCPDump”.

Deve possuir opção de gravação de sessões completas para servir como subsídio para análise forense (IP Session Logging). Estes dados devem ficar armazenados em arquivos no sensor e ser visualizáveis através da console de gerência. Estes arquivos devem ser protegidos por controle de acesso.

Deve suportar filtragem de assinaturas por endereço IP de origem/destino (possibilidade de definir que uma dada assinatura de ataque deverá ser disparada somente quando estiver associada a endereços IP origem/destino específicos)

Implementar NTP (Network Time Protocol), conforme RFC 1305, contemplando autenticação MD5 entre os peers.

Deve suportar prevenção de ataques em redes IPv6.

Capacidade de gerar relatórios personalizados, por sensor, por horário, por evento, por endereço, por porta

O sistema deve permitir a detecção das seguintes classes de ataques:

ataques com nomes específicos: tais como PHF e Smurf

ataques genéricos: (ataques nomeados com múltiplas variações) tais como Pacotes IP fragmentados, Teardrop, Land, Ping Sweep, Port Sweep (UDP e TCP), “Remote Shell Code”

ataques com assinaturas complexas: tais como Simplex-Mode TCP hijacking , E-mail Spam, BackOriffice 2000 StealthMode, Unicode Decodes, IIS Unicode exploit, cross-site scripting, directory traversal, command injection, SQL Injection, Header Spoofing

Port Scanning (“Full connect”, “SYN Stealth”, “FIN Stealth”, UDP)

Detecção de tráfego de pelo menos os seguintes protocolos “peer-to-peer” (kazaa, gnutella, qtella, bearshare, gnucleus, limewire, morpheus, mutella, hotline, edonkey, soulseek, napster, bittorrent

Detecção de tráfego de pelo menos os seguintes sistemas de “instant messaging” (yahoo messenger, ICQ, AOL, MSN)

Internet Worms : o sistema deve ser capaz de detectar pelo menos os seguintes vírus de rede : Code-Red CRv1, Code-Red CRv2, Code-Red II, Nimda, Bagle

Ataques de DoS (Denial-of –Service) direcionados à rede IP.

O sistema deve permitir a criação de regras personalizadas de identificação de invasões para que possa ser adaptado à estrutura particular disponível na DPF (no próprio sistema devem ser disponibilizados recursos para que se criem assinaturas de ataques personalizadas usando-se atributos dos níveis 2 até 7 do modelo de referência OSI)

Deve ser fornecido kit para montagem em rack padrão 19”;

Deve ser fornecido com documentação técnica e manuais que contenham informações suficientes para possibilitar a instalação, configuração e operacionalização do equipamento;

Fornecer garantia e suporte total por um período de 12 meses com atendimento 8x5xNBD realizada pelo fabricante no Brasil;

Item:	Quantidade:	Descrição:
03	**02**	**SWITCH ROTEADOR LAYER 3**

Especificações gerais:

Layer 03;

Possuir, no mínimo, 24 portas Ethernet 10/100/1000 com auto sensing de velocidade e com conectores RJ-45;

Possuir, no mínimo, 4 portas 1000Base-SX switching gigabit ethernet, full-duplex, para fibras óticas multímodo. Deverão ser fornecidos os GBIC/SFP necessários;

As interfaces 10/100/1000 devem obedecer às normas técnicas IEEE802.3 (10BaseT), IEEE802.3u (100BaseTX), 802.3ab (1000BaseT) e IEEE802.3x (Flow Control);

Todas as portas Ethernet 10/100/1000 devem suportar configuração Half-Duplex e Full-Duplex, com a opção de negociação automática;

Todas as portas Ethernet 10/100/1000 devem suportar auto configuração de crossover (Auto MDIX);

Deverá vir acompanhado de 2(dois) GBIC SFP/Giga compatível com o equipamento.

Possuir capacidade de associação das portas 10/100/1000 e 1000Base-SX, no mínimo, em grupo de oito portas, formando uma única interface lógica com as mesmas facilidades das interfaces originais, compatível com a norma IEEE 802.3ad;

Possuir LEDs para a indicação do status das portas e atividade, além de duplex;

Possibilitar a configuração dinâmica de portas por software, permitindo a definição de portas ativas e inativas;

Implementar VLANs por porta;

Implementar VLANs compatíveis com o padrão IEEE 802.1q;

Implementar mecanismo de seleção de quais vlans serão permitidas através de trunk; 802.1q. Deve ser permitida a configuração dessa seleção de forma dinâmica;

Possuir porta de console para ligação, direta e através de modem, de terminal RS-232 para acesso à interface de linha de comando. Poderá ser fornecida porta de console com

interface USB;

Deverá ser fornecido cabo de console compatível com a porta de console do equipamento;

Implementar os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps;

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

Sem autenticação e sem privacidade (noAuthNoPriv);

Com autenticação e sem privacidade (authNoPriv);

Com autenticação e com privacidade (authPriv);

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

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

Implementar empilhamento físico com cabos de empilhamento dedicados, não podendo ser utilizados portas 10 Gbps com SFPs para empilhamento, permitindo empilhamento de até 8 unidades, com velocidade de empilhamento de 64 Gbps full-duplex;

A pilha deverá ser gerenciada através de um único endereço IP, permitir agregação lógica de links utilizando qualquer porta da pilha e permitir espelhamento de portas de qualquer porta para qualquer porta da pilha;

Possuir ferramentas para depuração e gerenciamento em primeiro nível, tais como debug, trace, log de eventos;

Permitir o espelhamento do tráfego de portas que residem em um dado switch para uma porta que reside em switch diferente da pilha;

Permitir a adição manual de endereços MAC multicast na tabela de comutação, sem restrição à quantidade de portas a serem associadas;

Implementar funcionalidade de separação do tráfego de voz e dados em uma mesma porta de acesso (Voice VLAN), sem a necessidade de utilização de 802.1q;

Implementar DHCP Relay, DHCP Snooping e DHCP Server em múltiplas VLANS;

Permitir a virtualização das tabelas de roteamento camada 3 através de VRFs “Virtual

Routing and Forwarding";

Implementar port-security;

Implementar roteamento estático para IPv4;

Implementar roteamento dinâmico RIPv1 (RFC 1058), RIPv2 (RFC 2453);

Implementar protocolo de roteamento dinâmico OSPF (RFC 2328, 1587, 1765 e 2370);

Implementar mecanismo de segurança do protocolo OSPF permitindo a autenticação mutua entre peers OSPF;

Implementar protocolo de roteamento EIGRP ou OSPF;

Permitir o roteamento nível 3 entre VLANs;

Implementar protocolo de redundância de gateway HSRP ou VRRP;

Implementar, no mínimo, 32 grupos HSRP ou VRRP;

Implementar roteamento baseado em origem, com possibilidade de definição do próximo salto camada 3 e VRF, baseado em uma condição de origem;

Possuir capacidade para pelo menos 12.000 endereços MAC na tabela de comutação;

Implementar, no mínimo, 1000 vlans simultaneamente;

Deve possuir switch-capacity de no mínimo 64 Gbps e taxa de encaminhamento de no mínimo 64 Mbps;Suportar Jumbo frames de no mínimo 9216 Bytes;

Implementar, no mínimo, 1000 interfaces vlans simultaneamente, para roteamento nível 3 entre as vlans configuradas;

Implementar mecanismo de autenticação para acesso local ou remoto ao equipamento baseada em um Servidor de Autenticação/Autorização do tipo TACACS e RADIUS;

Implementar listas de controle de acesso (ACLs) baseadas em endereço IP de origem e destino, portas TCP e UDP de origem e destino;

Proteger a interface de comando do equipamento através de senha;

Possuir controle de broadcast, multicast e unicast por porta;

Permitir a configuração de endereços IPv6 para gerenciamento;

Implementar ICMPv6 com as seguintes funcionalidades:

ICMP request / reply;

ICMP Neighbor Discovery Protocol (NDP);

Implementar mecanismo de Dual Stack (IPv4 e IPv6), para permitir migração de IPv4/ IPv6;

Deve vir acompanhado de 04 conversores de Interface Gigabit (GBIC) do mesmo fabricante, tipo SX.

Deve ser fornecido kit para montagem em rack padrão 19";

Deve ser fornecido com documentação técnica e manuais que contenham informações suficientes para possibilitar a instalação, configuração e operacionalização do equipamento;

Fornecer garantia e suporte total por um período de 12 meses com atendimento 8x5xNBD realizada pelo fabricante no Brasil;

Item:	Quantidade:	Descrição:
04	**02**	**Roteador**

Especificações gerais:

Possuir, no mínimo 3 (três) interfaces Ethernet 10BaseT/100BaseTX/1000BaseT;

Possibilitar a configuração dinâmica de portas por software, permitindo a definição de portas ativas e inativas;

Implementar VLANs por porta;

Implementar VLANs compatíveis com o padrão IEEE 802.1q;

Implementar mecanismo de seleção de quais vlans serão permitidas através de trunk 802.1q. Deve ser permitida a configuração dessa seleção de forma dinâmica;

Possuir configuração de CPU e memória (RAM e Flash) suficiente para a implementação de todas as funcionalidades descritas nesta especificação;

Possuir porta de console para ligação, direta e através de modem, de terminal RS-232 para acesso à interface de linha de comando. Poderá ser fornecida porta de console com interface USB;

Deverá ser fornecido cabo de console compatível com a porta de console do equipamento.

Suportar simultaneamente em sua memória Flash (ou semelhante), duas imagens do sistema operacional entregue com a solução;

Possuir LEDs para a indicação do status das portas e atividade;

Implementar os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps;

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

Sem autenticação e sem privacidade (noAuthNoPriv);

Com autenticação e sem privacidade (authNoPriv);

Com autenticação e com privacidade (authPriv);

Possuir suporte a MIB II, conforme RFC 1213;

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

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

Possuir armazenamento interno das mensagens de log geradas pelo equipamento de no mínimo 2048 bytes;

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

Permitir o gerenciamento via CLI e Web, utilizando SSH e HTTPS;

Possuir uma porta auxiliar serial assíncrona para acesso gerencial remoto;

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

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

Deve permitir a atualização de sistema operacional através do protocolo TFTP ou FTP;

Permitir o armazenamento de sua configuração em memória não volátil, podendo, numa queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior à queda de alimentação;

Possuir ferramentas para depuração e gerenciamento em primeiro nível, tais como debug, trace, log de eventos;

Deve suportar IPv6;

Implementar NAT (Network Address Translation);

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

Implementar DHCP Relay e DHCP Server;

Implementar o protocolo VRRP (RFC 2338) ou mecanismo similar de redundância de gateway. Suportar mecanismo de autenticação MD5 entre os peers VRRP;

Suporte aos encapsulamentos frame-relay, PPP, HDLC e SDLC nas interfaces seriais;

Implementar balanceamento de carga entre circuitos seriais de velocidades diferentes;

Implementar “dial-backup” (no caso de “queda” do circuito serial o roteador deve efetuar discagem automática) por meio de interface serial assíncrona distinta das interfaces seriais principais;

Implementar PPP (Point to Point Protocol) sobre Frame Relay (PPP Over Frame Relay);

Implementar PPP (Point to Point Protocol) sobre Ethernet (PPP Over Ethernet);

Implementar roteamento estático;

Implementar roteamento dinâmico RIPv2 (RFC 2453 e 2082);

Implementar protocolo de roteamento dinâmico OSPF (RFC 2328, 3101, 3137, 3623 e 2370);

Implementar protocolo de roteamento EIGRP ou OSPF;

Permitir o roteamento nível 3 entre VLANs;

Implementar, no mínimo, 100 grupos VRRP ou de mecanismo similar de redundância de gateway simultaneamente;

Permitir a virtualização das tabelas de roteamento camada 3. As tabelas virtuais deverão ser completamente segmentadas;

Suporte ao protocolo de Tunelamento GRE (General Routing Encapsulation - RFCs 2784), contemplando, no mínimo, os seguintes recursos;

Permitir a associação do túnel GRE a uma tabela virtual de roteamento específica, definida pelo administrador do equipamento;

Operação em modo multiponto (“multipoint GRE”);

Possibilidade de configuração de “Keepalive” nos túneis;

Suporte a QoS (qualidade de serviço) - deve ser possível a cópia da informação de classificação de tráfego existente no cabeçalho do pacote original para os pacotes transportados com encapsulamento GRE;

Implementar roteamento baseado em origem, com possibilidade de definição do próximo

salto camada 3, baseado em uma condição de origem;

Suportar roteamento estático para IPv6;

Implementar, no mínimo, 100 vlans simultaneamente;

Implementar, no mínimo, 100 interfaces vlans simultaneamente, para roteamento nível 3 entre as vlans configuradas;

Possuir backplane de, no mínimo, 2 Gbps;

Suportar pelo menos 1 (um) Gbps de throughput com todas as funcionalidades de roteamento e segurança ativas simultaneamente;

Implementar mecanismo de autenticação para acesso local ou remoto ao equipamento baseada em um Servidor de Autenticação/Autorização do tipo TACACS e RADIUS;

Implementar filtragem de pacotes (ACL - Access Control List), para IPv4 e IPv6;

Deve ser possível especificar o horário e dias da semana em que devem ser automaticamente ativadas as ACLs;

Implementar listas de controle de acesso (ACLs), para filtragem de pacotes, baseadas em endereço IP de origem e destino, portas TCP e UDP de origem e destino e flags TCP;

Proteger a interface de comando do equipamento através de senha;

Permitir a criação de listas de acesso baseadas em endereço IP para limitar o acesso ao roteador via Telnet, SSH e SNMP. Deve ser possível definir os endereços IP de origem das sessões Telnet e SSH;

Implementar a criptografia de todos os pacotes enviados ao servidor de controle de acesso e não só os pacotes referentes à senha;

Suportar serviços de VPN baseados no padrão IPSec (IP Security Protocol);

Suportar serviços de VPN baseados no padrão IKE (Internet Key Exchange);

Suportar criação de VPNs de acordo com o conjunto de padrões IPSEC em modo túnel;

Devem ser implementados os modos de operação “tunnel mode” e “transport mode”;

Devem ser suportadas no mínimo as RFCs 1828, 1829, 2401, 2402, 2406, 2407, 2408 e

2409;

Suportar o tráfego protocolo GRE sobre IPSEC;

Suportar o tráfego de IP multicast sobre IPSEC;

Implementar padrão IEEE 802.1q (Vlan Frame Tagging);

Implementar padrão IEEE 802.1p (Class of Service) para cada porta;

Implementar padrão IEEE 802.3ad;

Implementar o protocolo de negociação Link Aggregation Control Protocol (LACP);

Implementar controle de acesso por porta, usando o padrão IEEE 802.1x (Port Based Network Access Control);

Possuir a facilidade de priorização de tráfego através do protocolo IEEE 802.1p;

Classificação e Reclassificação baseadas em endereço IP de origem/destino, portas TCP e UDP de origem/destino, endereços MAC de origem/destino;

Suportar funcionalidades de QoS de “Traffic Shaping” e “Traffic Policing”;

Deve ser possível a especificação de banda por classe de serviço;

Implementar IPv6;

Permitir a configuração de endereços IPv6 para gerenciamento;

Implementar ICMPv6 com as seguintes funcionalidades:

ICMP request / reply;

ICMP Neighbor Discovery Protocol (NDP);

ICMP MTU Discovery;

Implementar protocolos de gerenciamento Ping, Traceroute, Telnet, SSH, SNMP, SYSLOG e DNS sobre IPv6;

Implementar mecanismo de Dual Stack (IPv4 e IPv6), para permitir migração de IPv4 para IPv6;

Possuir cabo de alimentação para a fonte com, no mínimo, 1,80m (um metro e oitenta

centímetros) de comprimento;

Deve ser fornecido kit para montagem em rack padrão 19”;

Deve ser fornecido com documentação técnica e manuais que contenham informações suficientes para possibilitar a instalação, configuração e operacionalização do equipamento;

Fornecer garantia e suporte total por um período de 12 meses com atendimento 8x5xNBD realizada pelo fabricante no Brasil;

Item:	Quantidade:	Descrição:
05	**01**	**Switch concentrador (Core)**

Especificações gerais:

Layer 02, 03 e 04;

Possuir, no mínimo, 7 (sete) número de slots com no mínimo de 48Gbps por slot;

Possuir slot para controlador redundante;

Todos os componentes devem possuir tecnologia Hot swappable, possibilitando a substituição sem a necessidade de desligar o equipamento;

Possuir fonte de alimentação redundante;

Ter no mínimo, 96 portas x 10/100/1000 (PoE) RJ-45

Possuir no mínimo, 2 módulos de 24 portas SFP (mini-GBIC) – Plug-in, com suporte de interruptores de alta densidade, oferecer alto desempenho a camada integrada (Layer) 2, 3 e 4 de comutação com serviços inteligentes para controle de rede; Deverá vir acompanhado de 48 SFP (mini-GBIC) transceiver module - LC/PC multi-mode;

Possuir módulo com, no mínimo, 6 portas 10GE (padrão 10GBASE-SR). Cada módulo deverá vir acompanhado de, no mínimo, 6 transceivers SFP+ ou XFP.

As interfaces 10/100/1000 devem obedecer às normas técnicas IEEE802.3 (10BaseT), IEEE802.3u (100BaseTX), 802.3ab (1000BaseT) e IEEE802.3x (Flow Control);

Todas as portas Ethernet 10/100/1000 devem suportar configuração Half-Duplex e Full-Duplex, com a opção de negociação automática;

Todas as portas Ethernet 10/100/1000 devem suportar auto configuração de crossover (Auto MDIX);

Possuir LEDs para a indicação do status das portas e atividade, além de duplex;

Possibilitar a configuração dinâmica de portas por software, permitindo a definição de portas ativas e inativas;

Possuir modulo de control processor, supervisor plug-in module;

Implementar VLANs por porta;

Implementar VLANs compatíveis com o padrão IEEE 802.1q;

Implementar mecanismo de seleção de quais vlans serão permitidas através de trunk 802.1q. Deve ser permitida a configuração dessa seleção de forma dinâmica;

Possuir porta de console para ligação, direta e através de modem, de terminal RS-232 para acesso à interface de linha de comando. Poderá ser fornecida porta de console com interface USB;

Deverá ser fornecido cabo de console compatível com a porta de console do equipamento.

Implementar os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps;

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

Sem autenticação e sem privacidade (noAuthNoPriv);

Com autenticação e sem privacidade (authNoPriv);

Com autenticação e com privacidade (authPriv);

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

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

Possuir ferramentas para depuração e gerenciamento em primeiro nível, tais como debug, trace, log de eventos;

Permitir o espelhamento do tráfego de portas que residem em um dado switch para uma porta que reside em switch diferente da pilha;

Permitir a adição manual de endereços MAC multicast na tabela de comutação, sem restrição à quantidade de portas a serem associadas;

Implementar funcionalidade de separação do tráfego de voz e dados em uma mesma porta de acesso (Voice VLAN), sem a necessidade de utilização de 802.1q;

Implementar DHCP Relay, DHCP Snooping e DHCP Server em múltiplas VLANS;

Permitir a virtualização das tabelas de roteamento camada 3 através de VRFs “Virtual Routing and Forwarding”;

Implementar port-security;

Implementar roteamento estático para IPv4;

Implementar roteamento dinâmico RIPv1 (RFC 1058), RIPv2 (RFC 2453);

Implementar protocolo de roteamento dinâmico OSPF (RFC 2328, 1587, 1765 e 2370);

Implementar mecanismo de autenticação para acesso local ou remoto ao equipamento baseada em um Servidor de Autenticação/Autorização do tipo TACACS e RADIUS;

Implementar listas de controle de acesso (ACLs) baseadas em endereço IP de origem e destino, portas TCP e UDP de origem e destino;

Proteger a interface de comando do equipamento através de senha;

Possuir controle de broadcast, multicast e unicast por porta;

Permitir a configuração de endereços IPv6 para gerenciamento;

Implementar ICMPv6 com as seguintes funcionalidades:

ICMP request / reply;

ICMP Neighbor Discovery Protocol (NDP);

Implementar mecanismo de Dual Stack (IPv4 e IPv6), para permitir migração de IPv4/ IPv6;

Deve ser fornecido kit para montagem em rack padrão 19”;

Deve ser fornecido com documentação técnica e manuais que contenham informações suficientes para possibilitar a instalação, configuração e operacionalização do equipamento;

Fornecer garantia e suporte total por um período de 12 meses com atendimento 8x5xNBD realizada pelo fabricante no Brasil;

Item:	Quantidade:	Descrição:
06	**01**	**Sistema de VOIP para 25 ramais**

Sistema de telefonia baseado em IP (VOIP) com capacidade de no mínimo 20 ramais integrados a estrutura de rede proposta nesse edital.

Aparelhos Telefônicos VOIP

Deverá ser fornecido 05 (cinco) telefones com tecnologia VOIP handset com visor colorido e câmera que permita a realização de vídeo conferencias, viva voz e funções de memória.

Deverá ser fornecido 02 (dois) telefones com tecnologia VOIP especifico para realização de áudio conferencias com viva voz e no mínimo 3 microfones.

Deverá ser fornecido 15 (quinze) telefones com tecnologia VOIP handset com visor, viva voz e funções de memória.

Especificações Gerais

Possuir Serviços de Voice Mail, Caller ID, Call Waiting, Call Forwarding, Call Transfer, Call Hold, Message Waiting Capability;

Integrated Ethernet switch;

Protocolo VoIP SIP;

Ter Codecs de Voz G.722, G.729a, G.729ab, G.711u, G.711a, iLBC;

Possuir Codecs de Video H.264;

Suporte Multiline;

QoS IEEE 802.1Q (VLAN);

Suporte DHCP, estático;

Possuir no mínimo 2 x Ethernet 10Base-T/100Base-TX/1000Base-T;

Observações Gerais

Deverá ser fornecido todos os itens necessários para integração ao sistema de telefonia existente na TV Cultura como licenças de software, módulos de portas de voz, gatewais para linhas analógicas, módulos para troncos E1 e demais itens que possibilitarão o funcionamento de no mínimo 25 ramais VOIP.

Item:	Quantidade:	Descrição:
07	**02**	**Switch empilhável de 24 PORTAS 10/100/1000 PoE/PoE+ (370W), com uplinks SFP/SFP+ 1/10GbE**

Especificações gerais:

DESEMPENHO

Possuir capacidade para pelo menos 16.000 endereços MAC na tabela de comutação.

Deve possuir taxa de encaminhamento de no mínimo 108Gbps full-duplex (216Gbps total).

Implementar , no mínimo, 1023 vlans simultaneamente.

Suportar Jumbo frames de no mínimo 9216 Bytes

Deverá ser fornecido com capacidade instalada para tratar a taxa de, pelo menos, 95 Mpps

PORTAS

Deverá ser fornecido com, no mínimo, 24 portas 10/100/1000 suportando o padrão 802.3af (15,4W PoE) e 802.3at (30W PoE+) em todas as 24 portas com, pelo menos, 370W disponíveis para PoE/PoE+ (15,4 W para 24 portas simultaneamente e 30W em 12 portas simultaneamente).

Deverá possuir para uplink, pelo menos, 2 (dois) slots para conectores do tipo SFP/SFP +, com suporte tanto a Gigabit Ethernet como 10 Gigabit Ethernet, além das 24 portas UTP solicitadas anteriormente;

A Deverá vir acompanhado de 2(dois) GBIC SFP ou XFP compatível com o equipamento(10GE padrão 10GBASE-SR).

Deverá ser fornecido modulo e cabos para empilhamento através de porta dedicada.

Deverá ser fornecido modulo com no mínimo 2interfaces 10Ge SFP+

Todas as portas RJ-45 devem suportar configuração Full-Duplex, com a opção de

negociação automática.

Todas as portas solicitadas devem poder operar simultaneamente, sem característica de combo.

Todas as portas RJ-45 devem suportar auto configuração de crossover (Auto MDIX)

Possuir capacidade de associação das portas, no mínimo, em grupo de oito, formando uma única interface lógica com as mesmas facilidades das interfaces originais, compatível com a norma IEEE 802.3ad (LACP).

Possibilitar a configuração dinâmica de portas por software, permitindo a definição de portas ativas/inativas.

Implementar VLANs por porta.

Implementar VLANs compatíveis com o padrão IEEE 802.1q.

Implementar mecanismo de seleção de quais vlans serão permitidas através de trunk IEEE 802.1q. Deve ser permitida a configuração dessa seleção de forma dinâmica.

Possuir porta de console para ligação, direta e através de modem, de terminal RS-232 para acesso à interface de linha de comando. Poderá ser fornecida porta de console com interface USB.

Deverá ser fornecido cabo de console compatível com a porta de console do equipamento.

FONTE DE ALIMENTAÇÃO

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

Suportar alimentação elétrica redundante externa capaz de alimentar o equipamento com todas as funcionalidades.

Possuir cabo de alimentação para a fonte com, no mínimo, 1,80m (um metro e oitenta centímetros) de comprimento.

DIMENSÕES

Permitir ser montado em rack padrão de 19 (dezenove) polegadas, incluindo todos os acessórios necessários.

SINALIZAÇÃO VISUAL

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

GERENCIAMENTO

Implementar os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps.

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

Sem autenticação e sem privacidade (noAuthNoPriv);

Com autenticação e sem privacidade (authNoPriv);

Com autenticação e com privacidade (authPriv).

Possuir suporte a MIB II, conforme RFC 1213.

Implementar MIB que forneça informações sobre utilização e reserva de energia para PoE.

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

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

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

Possuir armazenamento interno das mensagens de log geradas pelo equipamento de no mínimo 4096 bytes.

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

Permitir o controle da geração de traps por porta, possibilitando restringir a geração de

traps a portas específicas.

Implementar nativamente 4 grupos RMON (History, Statistcs, Alarms e Events) conforme RFC 1757

Implementar os protocolos LLDP (IEEE 802.1ab) e LLDP-MED

Possuir porta out-of-band para gerenciamento.

FACILIDADES

Implementar Telnet para acesso à interface de linha de comando.

Permitir a atualização remota do sistema operacional e arquivos de configuração utilizados no equipamento via interfaces ethernet e serial.

Ser configurável e gerenciável via GUI (graphical user interface), CLI (command line interface), SNMP, Telnet, SSH, FTP, HTTP e HTTPS com, no mínimo, 5 sessões simultâneas e independentes.

Permitir a atualização de sistema operacional através do protocolo TFTP ou FTP.

Permitir a transferência segura de arquivos para o equipamento através do protocolo SCP (Secure Copy) utilizando um cliente padrão ou SFTP (Secure FTP).

Gerenciamento remoto protocolo SSH para, implementando pelo menos o algoritmo de encriptação de dados 3DES.

Possuir SSH client, permitindo acessar servidores SSH.

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

Permitir a gravação de log externo (syslog).

Permitir o armazenamento de sua configuração em memória não volátil, podendo, numa queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior à queda de alimentação.

Possuir ferramentas para depuração e gerenciamento em primeiro nível, tais como debug, trace, log de eventos.

Suportar pelo menos quatro sessões simultâneas de espelhamento.

Permitir o espelhamento da totalidade do tráfego de uma porta, de um grupo de portas e de VLANs para outra porta localizada no mesmo switch e em outro switch do mesmo tipo conectado à mesma rede local. Deve ser possível definir o sentido do tráfego a ser espelhado: somente tráfego de entrada, somente tráfego de saída e ambos simultaneamente.

Permitir a adição manual de endereços MAC multicast na tabela de comutação, sem restrição à quantidade de portas a serem associadas.

Deve ser fornecido com documentação técnica e manuais que contenham informações suficientes para possibilitar a instalação, configuração e operacionalização do equipamento.

Implementar funcionalidade de separação do tráfego de voz e dados em uma mesma porta de acesso (Voice VLAN), sem a necessidade de utilização de IEEE 802.1q.

Permitir a criação de subgrupos dentro de uma mesma VLAN com conceito de portas isoladas e portas compartilhadas (“promíscuas”), onde portas isoladas não se comunicam com outras portas isoladas, mas apenas com as portas compartilhadas (“promíscuas”) de uma dada VLAN.

Suportar estabelecer quais VLANs serão permitidas em cada um dos troncos configurados.

Permitir a criação, remoção, gerenciamento e distribuição de VLANs de forma dinâmica através de portas configuradas como tronco IEEE 802.1q.

Responder a pacotes para teste da implementação dos níveis de serviço especificados (SLA).

Suportar no mínimo as seguintes operações de teste:

ICMP echo;

TCP connect (em qualquer porta TCP do intervalo 1-50000 que o administrador especifique).

UDP echo (em qualquer porta UDP do intervalo 1-50000 que o administrador especifique).

O switch deve suportar pelo menos 5 (cinco) destas operações de testes simultaneamente.

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

Implementar DHCP Relay, DHCP Snooping e DHCP Server em múltiplas VLANS;

Suportar empilhamento físico com cabos de empilhamento dedicados, não podendo ser utilizados portas 10Gbps com SFPs para empilhamento, permitindo empilhamento de no mínimo 8 unidades, com velocidade de empilhamento de 40Gbps full-duplex (mínimo 80Gbps total).

A pilha deverá ser gerenciada através de um único endereço IP, permitir agregação lógica de links utilizando qualquer porta da pilha e permitir espelhamento de portas de qualquer porta para qualquer porta da pilha.

Deverá possuir porta USB ou protocolos TFTP, FTP para armazenamento de arquivos.

Deverá possuir funcionalidade que permita configuração automática de portas de acordo com o equipamento conectado

Suportar sFLOW, IPFIX ou funcionalidade similar.

SEGURANÇA

Implementar mecanismo de autenticação para acesso local ou remoto ao equipamento baseada em um Servidor de Autenticação/Autorização do tipo TACACS+ e RADIUS.

Implementar filtragem de pacotes (ACL - Access Control List).

Proteger a interface de comando do equipamento através de senha.

Implementar o protocolo SSH V2 para acesso à interface de linha de comando.

Permitir a criação de listas de acesso baseadas em endereço IP para limitar o acesso ao switch via Telnet, SSH e SNMP. Deve ser possível definir os endereços IP de origem das sessões Telnet e SSH.

Possibilitar o estabelecimento do número máximo de MACs que podem estar associados a uma dada porta do switch. Deve ser possível desabilitar a porta e enviar um trap SNMP caso o número de endereços MAC configurados para a porta seja excedido.

Implementar listas de controle de acesso (ACLs) baseadas em endereço IP de origem e

destino, portas TCP e UDP de origem e destino.

Permitir a associação de um endereço MAC específico a uma dada porta do switch, de modo que somente a estação que tenha tal endereço possa usar a referida porta para conexão.

Implementar mecanismos de AAA (Authentication, Authorization e Accounting) com garantia de entrega.

Possuir controle de broadcast, multicast e unicast por porta.

Implementar a criptografia de todos os pacotes enviados ao servidor de controle de acesso e não só os pacotes referentes à senha.

Permitir controlar quais comandos os usuários ou grupos de usuários podem emitir em determinados elementos de rede.

Possuir suporte a mecanismo de proteção da “Root Bridge” do algoritmo “Spanning-Tree” para defesa contra ataques do tipo “Denial of Service” no ambiente nível 2.

Possuir suporte à suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta do switch esteja colocada no modo “Fast Forwarding” (conforme previsto no padrão IEEE 802.1w).

Possuir análise do protocolo DHCP e permitir que se crie uma tabela de associação entre endereços IP atribuídos dinamicamente, MAC da máquina que recebeu o endereço e porta física do switch em que se localiza tal MAC.

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

Possuir análise do protocolo ARP (Address Resolution Protocol) e possuir proteção nativa contra ataques do tipo “ARP Poisoning”.

Os processos de Autenticação, Autorização e Accounting associados a controle de acesso administrativo ao equipamento devem ser completamente independentes dos processos AAA no contexto IEEE 802.1x.

Implementar controle de acesso por porta, usando o padrão IEEE 802.1x (Port Based Network Access Control). Devem ser atendidos, no mínimo, os seguintes requisitos:

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

casos:

A estação não tem cliente IEEE 802.1x (suplicante);

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

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

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

Nome do usuário;

Switch em que o computador do usuário está conectado;

Porta do switch utilizada par acesso;

Endereço MAC da máquina utilizada pelo usuário;

Endereço IP do usuário;

Horários de início e término da conexão;

Bytes transmitidos e recebidos durante a conexão.

Deve ser possível definir, por porta, o intervalo de tempo para obrigar o cliente a se reautenticar (reautenticação periódica).

Deve ser possível forçar manualmente a reautenticação de um usuário conectado a uma porta do switch habilitada para 802.1x.

Suportar a autenticação IEEE 802.1x via endereço MAC em substituição à identificação de usuário, para equipamentos que não disponham de suplicantes.

Implementar suporte ao serviço DHCP Server em múltiplas VLANS simultaneamente, para que possa atribuir endereços IP aos clientes 802.1x autenticados e autorizados.

Deve ser suportada a autenticação de múltiplos usuários em uma mesma porta.

Deve ter tratamento de autenticação IEEE 802.1x diferenciado entre "Voice Vlan" e "Data LAN", na mesma porta para que um erro de autenticação em uma Vlan não interfira na outra.

Suportar atribuição de autenticação através do navegador (Web Authentication) caso a máquina que esteja utilizando para acesso à Rede não tenha cliente IEEE 802.1x operacional, o portal de autenticação deve utilizar protocolo seguro tal como HTTPS.

Suportar protocolo Radius CoA (Change of Authorization), conforme RFC 5176

PADRÕES IEEE

Implementar padrão IEEE 802.1d (Spanning Tree Protocol) por VLAN.

Implementar padrão IEEE 802.1q (Vlan Frame Tagging).

Implementar padrão IEEE 802.1p (Class of Service) para cada porta.

Implementar padrão IEEE 802.1w (Rapid spanning Tree Protocol).

Implementar padrão IEEE 802.1s (Multi-Instance Spanning-Tree), com suporte a, no mínimo, 16 instâncias simultâneas do protocolo Spanning-Tree.

Implementar padrão IEEE 802.3ad Link Aggregation Control Protocol (LACP).

Implementar padrão IEEE 802.3af (PoE)

Implementar padrão IEEE 802.3at (PoE+)

MULTICAST

Implementar em todas as interfaces do switch o protocolo IGMP Snooping (v1, v2 e v3), não permitindo que o tráfego multicast seja tratado como broadcast no switch.

Implementar em todas as interfaces do switch o protocolo MLD Snooping (v1 e v2), não permitindo que o tráfego multicast IPv6 seja tratado como broadcast no switch.

QUALIDADE DE SERVIÇO (QoS)

Priorização de tráfego através do protocolo IEEE 802.1p.

Suportar fila com prioridade estrita (prioridade absoluta em relação às demais classes dentro do limite de banda que lhe foi atribuído) para tratamento do tráfego “real-

time” (voz e vídeo).

Suportar Weighted Round Robin (WRR) ou Shaped Round Robin (SRR).

Classificação e Reclassificação baseadas em endereço IP de origem/destino, portas TCP e UDP de origem e destino, endereços MAC de origem e destino.

Classificação, Marcação e Remarcação baseadas em CoS ("Class of Service" - nivel 2) e DSCP ("Differentiated Services Code Point"- nivel 3), conforme definições do IETF (Internet Engineering Task Force).

Suportar funcionalidades de QoS de “Traffic Shaping” e “Traffic Policing”.

Suportar especificação de banda por classe de serviço.

Para os pacotes que excederem a especificação, deve ser possível configurar ações tais como : transmissão do pacote sem modificação, transmissão com remarcação do valor de DSCP, descarte do pacote.

Suportar mapeamento de prioridades nível 2, definidas pelo padrão IEEE 802.1p, em prioridades nível 3 (IETF DSCP – Differentiated Services Code Point definido pela Internet Engineering Task Force) e vice-versa.

Suportar mecanismos de QoS de prevenção de congestionamento como WRED (Weighted Random Early Detection) ou WTD (Weighted Tail Drop)

Suportar pelo menos quatro filas de prioridade por porta de saída (egress port)

Suportar diferenciação de QoS por VLAN

Internet Protocol versão 6 (IPv6)

Implementar IPv6.

Permitir a configuração de endereços IPv6 para gerenciamento.

Implementar protocolos de gerenciamento Ping, Traceroute, Telnet, SSH, TFTP, FTP, SNMP, SYSLOG, HTTP, HTTPS e DNS sobre IPv6.

Implementar mecanismo de Dual Stack (IPv4 e IPv6), para permitir migração de IPv4 para IPv6.

ROTEAMENTO

Suportar roteamento inter-VLAN

Suportar roteamento estático com no mínimo 16 rotas.

Implementar o protocolo VRRP ou mecanismo similar de redundância de gateway, para IPv4.

Item:	Quantidade:	Descrição:
08	**10**	**Switch empilhável de 48 PORTAS 10/100/1000 PoE/PoE+ (740W), com uplinks SFP GbE**

Especificações gerais:

DESEMPENHO

Possuir capacidade para pelo menos 16.000 endereços MAC na tabela de comutação.

Deve possuir taxa de encaminhamento de no mínimo 108Gbps full-duplex (216Gbps total).

Implementar , no mínimo, 1023 vlans simultaneamente.

Suportar Jumbo frames de no mínimo 9216 Bytes

Deve ser fornecido com capacidade instalada para tratar a taxa de, pelo menos, 107 Mpps

PORTAS

Deverá ser fornecido com, no mínimo, 48 portas 10/100/1000, suportando o padrão 802.3af (15,4W PoE) e 802.3at (30W PoE+) em todas as 48 portas com, pelo menos, 740W disponíveis para PoE/PoE+ (15,4 W para 48 portas simultaneamente e 30W em 24 portas simultaneamente).

Deverá possuir para uplink, no mínimo, 4 (quatro) portas SFP GigabitEthernet, além das 48 portas UTP solicitadas anteriormente;

Deverá vir acompanhado de 2(dois) GBIC SFP/Giga multimodo compatível com o

equipamento.

Deverá ser fornecido modulo e cabos para empilhamento através de porta dedicada.

Todas as portas RJ-45 devem suportar configuração Full-Duplex, com a opção de negociação automática.

Todas as portas solicitadas devem poder operar simultaneamente, sem característica de combo.

Todas as portas RJ-45 devem suportar auto configuração de crossover (Auto MDIX)

Possuir capacidade de associação das portas, no mínimo, em grupo de oito, formando uma única interface lógica com as mesmas facilidades das interfaces originais, compatível com a norma IEEE 802.3ad (LACP).

Possibilitar a configuração dinâmica de portas por software, permitindo a definição de portas ativas/inativas.

Implementar VLANs por porta.

Implementar VLANs compatíveis com o padrão IEEE 802.1q.

Implementar mecanismo de seleção de quais vlans serão permitidas através de trunk IEEE 802.1q. Deve ser permitida a configuração dessa seleção de forma dinâmica.

Possuir porta de console para ligação, direta e através de modem, de terminal RS-232 para acesso à interface de linha de comando. Poderá ser fornecida porta de console com interface USB.

Deverá ser fornecido cabo de console compatível com a porta de console do equipamento.

FONTE DE ALIMENTAÇÃO

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

Suportar alimentação elétrica redundante externa capaz de alimentar o equipamento com todas as funcionalidades.

Possuir cabo de alimentação para a fonte com, no mínimo, 1,80m (um metro e oitenta

centímetros) de comprimento.

DIMENSÕES

Permitir ser montado em rack padrão de 19 (dezenove) polegadas, incluindo todos os acessórios necessários.

SINALIZAÇÃO VISUAL

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

GERENCIAMENTO

Implementar os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps.

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

Sem autenticação e sem privacidade (noAuthNoPriv);

Com autenticação e sem privacidade (authNoPriv);

Com autenticação e com privacidade (authPriv).

Possuir suporte a MIB II, conforme RFC 1213.

Implementar MIB que forneça informações sobre utilização e reserva de energia para PoE.

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

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

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

Possuir armazenamento interno das mensagens de log geradas pelo equipamento de no mínimo 4096 bytes.

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

Permitir o controle da geração de traps por porta, possibilitando restringir a geração de traps a portas específicas.

Implementar nativamente 4 grupos RMON (History, Statistcs, Alarms e Events) conforme RFC 1757

Implementar os protocolos LLDP (IEEE 802.1ab) e LLDP-MED

Possuir porta out-of-band para gerenciamento.

FACILIDADES

Implementar Telnet para acesso à interface de linha de comando.

Permitir a atualização remota do sistema operacional e arquivos de configuração utilizados no equipamento via interfaces ethernet e serial.

Ser configurável e gerenciável via GUI (graphical user interface), CLI (command line interface), SNMP, Telnet, SSH, FTP, HTTP e HTTPS com, no mínimo, 5 sessões simultâneas e independentes.

Permitir a atualização de sistema operacional através do protocolo TFTP ou FTP.

Permitir a transferência segura de arquivos para o equipamento através do protocolo SCP (Secure Copy) utilizando um cliente padrão ou SFTP (Secure FTP).

Gerenciamento remoto protocolo SSH para, implementando pelo menos o algoritmo de encriptação de dados 3DES.

Possuir SSH client, permitindo acessar servidores SSH.

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

Permitir a gravação de log externo (syslog).

Permitir o armazenamento de sua configuração em memória não volátil, podendo, numa queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior à queda de alimentação.

Possuir ferramentas para depuração e gerenciamento em primeiro nível, tais como

debug, trace, log de eventos.

Suportar pelo menos quatro sessões simultâneas de espelhamento.

Permitir o espelhamento da totalidade do tráfego de uma porta, de um grupo de portas e de VLANs para outra porta localizada no mesmo switch e em outro switch do mesmo tipo conectado à mesma rede local. Deve ser possível definir o sentido do tráfego a ser espelhado: somente tráfego de entrada, somente tráfego de saída e ambos simultaneamente.

Permitir a adição manual de endereços MAC multicast na tabela de comutação, sem restrição à quantidade de portas a serem associadas.

Deve ser fornecido com documentação técnica e manuais que contenham informações suficientes para possibilitar a instalação, configuração e operacionalização do equipamento.

Implementar funcionalidade de separação do tráfego de voz e dados em uma mesma porta de acesso (Voice VLAN), sem a necessidade de utilização de IEEE 802.1q.

Permitir a criação de subgrupos dentro de uma mesma VLAN com conceito de portas isoladas e portas compartilhadas (“promíscuas”), onde portas isoladas não se comunicam com outras portas isoladas, mas apenas com as portas compartilhadas (“promíscuas”) de uma dada VLAN.

Suportar estabelecer quais VLANs serão permitidas em cada um dos troncos configurados.

Permitir a criação, remoção, gerenciamento e distribuição de VLANs de forma dinâmica através de portas configuradas como tronco IEEE 802.1q.

Responder a pacotes para teste da implementação dos níveis de serviço especificados (SLA).

Suportar no mínimo as seguintes operações de teste:

ICMP echo;

TCP connect (em qualquer porta TCP do intervalo 1-50000 que o administrador especifique).

UDP echo (em qualquer porta UDP do intervalo 1-50000 que o administrador

especifique).

O switch deve suportar pelo menos 5 (cinco) destas operações de testes simultaneamente.

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

Implementar DHCP Relay, DHCP Snooping e DHCP Server em múltiplas VLANS;

Suportar empilhamento físico com cabos de empilhamento dedicados, não podendo ser utilizados portas 10Gbps com SFPs para empilhamento, permitindo empilhamento de no mínimo 8 unidades, com velocidade de empilhamento de 40Gbps full-duplex (80Gbps total).

A pilha deverá ser gerenciada através de um único endereço IP, permitir agregação lógica de links utilizando qualquer porta da pilha e permitir espelhamento de portas de qualquer porta para qualquer porta da pilha.

Deverá possuir porta USB ou protocolos TFTP, FTP para armazenamento de arquivos.

Deverá possuir funcionalidade que permita configuração automática de portas de acordo com o equipamento conectado

Suportar sFLOW, IPFIX ou funcionalidade similar.

SEGURANÇA

Implementar mecanismo de autenticação para acesso local ou remoto ao equipamento baseada em um Servidor de Autenticação/Autorização do tipo TACACS+ e RADIUS.

Implementar filtragem de pacotes (ACL - Access Control List).

Proteger a interface de comando do equipamento através de senha.

Implementar o protocolo SSH V2 para acesso à interface de linha de comando.

Permitir a criação de listas de acesso baseadas em endereço IP para limitar o acesso ao switch via Telnet, SSH e SNMP. Deve ser possível definir os endereços IP de origem das sessões Telnet e SSH.

Possibilitar o estabelecimento do número máximo de MACs que podem estar associados a uma dada porta do switch. Deve ser possível desabilitar a porta e enviar um trap SNMP caso o número de endereços MAC configurados para a porta seja excedido.

Implementar listas de controle de acesso (ACLs) baseadas em endereço IP de origem e destino, portas TCP e UDP de origem e destino.

Permitir a associação de um endereço MAC específico a uma dada porta do switch, de modo que somente a estação que tenha tal endereço possa usar a referida porta para conexão.

Implementar mecanismos de AAA (Authentication, Authorization e Accounting) com garantia de entrega.

Possuir controle de broadcast, multicast e unicast por porta.

Implementar a criptografia de todos os pacotes enviados ao servidor de controle de acesso e não só os pacotes referentes à senha.

Permitir controlar quais comandos os usuários ou grupos de usuários podem emitir em determinados elementos de rede.

Possuir suporte a mecanismo de proteção da “Root Bridge” do algoritmo “Spanning-Tree” para defesa contra ataques do tipo “Denial of Service” no ambiente nível 2.

Possuir suporte à suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta do switch esteja colocada no modo “Fast Forwarding” (conforme previsto no padrão IEEE 802.1w).

Possuir análise do protocolo DHCP e permitir que se crie uma tabela de associação entre endereços IP atribuídos dinamicamente, MAC da máquina que recebeu o endereço e porta física do switch em que se localiza tal MAC.

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

Possuir análise do protocolo ARP (Address Resolution Protocol) e possuir proteção nativa contra ataques do tipo “ARP Poisoning”.

Os processos de Autenticação, Autorização e Accounting associados a controle de acesso administrativo ao equipamento devem ser completamente independentes dos

processos AAA no contexto IEEE 802.1x.

Implementar controle de acesso por porta, usando o padrão IEEE 802.1x (Port Based Network Access Control). Devem ser atendidos, no mínimo, os seguintes requisitos:

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

A estação não tem cliente IEEE 802.1x (suplicante);

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

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

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

Nome do usuário;

Switch em que o computador do usuário está conectado;

Porta do switch utilizada par acesso;

Endereço MAC da máquina utilizada pelo usuário;

Endereço IP do usuário;

Horários de início e término da conexão;

Bytes transmitidos e recebidos durante a conexão.

Deve ser possível definir, por porta, o intervalo de tempo para obrigar o cliente a se reautenticar (reautenticação periódica).

Deve ser possível forçar manualmente a reautenticação de um usuário conectado a uma porta do switch habilitada para 802.1x.

Suportar a autenticação IEEE 802.1x via endereço MAC em substituição à identificação de usuário, para equipamentos que não disponham de suplicantes.

Implementar suporte ao serviço DHCP Server em múltiplas VLANS simultaneamente, para que possa atribuir endereços IP aos clientes 802.1x autenticados e autorizados.

Deve ser suportada a autenticação de múltiplos usuários em uma mesma porta.

Deve ter tratamento de autenticação IEEE 802.1x diferenciado entre “Voice Vlan” e “Data LAN”, na mesma porta para que um erro de autenticação em uma Vlan não interfira na outra.

Suportar atribuição de autenticação através do navegador (Web Authentication) caso a máquina que esteja utilizando para acesso à Rede não tenha cliente IEEE 802.1x operacional, o portal de autenticação deve utilizar protocolo seguro tal como HTTPS.

Suportar protocolo Radius CoA (Change of Authorization), conforme RFC 5176

PADRÕES IEEE

Implementar padrão IEEE 802.1d (Spanning Tree Protocol) por VLAN.

Implementar padrão IEEE 802.1q (Vlan Frame Tagging).

Implementar padrão IEEE 802.1p (Class of Service) para cada porta.

Implementar padrão IEEE 802.1w (Rapid spanning Tree Protocol).

Implementar padrão IEEE 802.1s (Multi-Instance Spanning-Tree), com suporte a, no mínimo, 16 instâncias simultâneas do protocolo Spanning-Tree.

Implementar padrão IEEE 802.3ad Link Aggregation Control Protocol (LACP).

Implementar padrão IEEE 802.3af (PoE)

Implementar padrão IEEE 802.3at (PoE+)

MULTICAST

Implementar em todas as interfaces do switch o protocolo IGMP Snooping (v1, v2 e v3), não permitindo que o tráfego multicast seja tratado como broadcast no switch.

Implementar em todas as interfaces do switch o protocolo MLD Snooping (v1 e v2), não permitindo que o tráfego multicast IPv6 seja tratado como broadcast no switch.

QUALIDADE DE SERVIÇO (QoS)

Priorização de tráfego através do protocolo IEEE 802.1p.

Suportar fila com prioridade estrita (prioridade absoluta em relação às demais classes dentro do limite de banda que lhe foi atribuído) para tratamento do tráfego “real-time” (voz e vídeo).

Suportar Weighted Round Robin (WRR) ou Shaped Round Robin (SRR).

Classificação e Reclassificação baseadas em endereço IP de origem/destino, portas TCP e UDP de origem e destino, endereços MAC de origem e destino.

Classificação, Marcação e Remarcação baseadas em CoS ("Class of Service" - nivel 2) e DSCP ("Differentiated Services Code Point"- nivel 3), conforme definições do IETF (Internet Engineering Task Force).

Suportar funcionalidades de QoS de “Traffic Shaping” e “Traffic Policing”.

Suportar especificação de banda por classe de serviço.

Para os pacotes que excederem a especificação, deve ser possível configurar ações tais como : transmissão do pacote sem modificação, transmissão com remarcação do valor de DSCP, descarte do pacote.

Suportar mapeamento de prioridades nível 2, definidas pelo padrão IEEE 802.1p, em prioridades nível 3 (IETF DSCP – Differentiated Services Code Point definido pela Internet Engineering Task Force) e vice-versa.

Suportar mecanismos de QoS de prevenção de congestionamento como WRED (Weighted Random Early Detection) ou WTD (Weighted Tail Drop)

Suportar pelo menos quatro filas de prioridade por porta de saída (egress port)

Suportar diferenciação de QoS por VLAN

Internet Protocol versão 6 (IPv6)

Implementar IPv6.

Permitir a configuração de endereços IPv6 para gerenciamento.

Implementar protocolos de gerenciamento Ping, Traceroute, Telnet, SSH, TFTP, FTP, SNMP, SYSLOG, HTTP, HTTPS e DNS sobre IPv6.

Implementar mecanismo de Dual Stack (IPv4 e IPv6), para permitir migração de IPv4 para IPv6.

ROTEAMENTO

Suportar roteamento inter-VLAN

Suportar roteamento estático com no mínimo 16 rotas.

Implementar o protocolo VRRP ou mecanismo similar de redundância de gateway, para IPv4.

Item:	Quantidade:	Descrição:
09	**5**	**Switch empilhável de 24 PORTAS 10/100/1000 PoE/PoE+ (370W), com uplinks SFP GbE**

Especificações gerais:

DESEMPENHO

Possuir capacidade para pelo menos 16.000 endereços MAC na tabela de comutação.

Deve possuir taxa de encaminhamento de no mínimo 108Gbps full-duplex (216Gbps total).

Implementar , no mínimo, 1023 vlans simultaneamente.

Suportar Jumbo frames de no mínimo 9216 Bytes

Deverá ser fornecido com capacidade instalada para tratar a taxa de, pelo menos, 71 Mpps

PORTAS

Deverá ser fornecido com, no mínimo, 24 portas 10/100/1000 suportando os padrões 802.3af (15,4W PoE) e 802.3at (30W PoE+) em todas as 24 portas com, pelo menos, 370W disponíveis para PoE/PoE+ (15,4 W para 24 portas simultaneamente e 30W em 12 portas simultaneamente).

Deverá possuir para uplink, no mínimo, 4 (quatro) portas SFP GigabitEthernet, além das 24 portas UTP solicitadas anteriormente. Deverá ser fornecido modulo e cabos para empilhamento através de porta dedicada.

Deverá vir acompanhado de 2(dois) GBIC SFP/Giga Multimodo compatível com o equipamento.

Todas as portas RJ-45 devem suportar configuração Full-Duplex, com a opção de negociação automática.

Todas as portas solicitadas devem poder operar simultaneamente, sem característica de combo.

Todas as portas RJ-45 devem suportar auto configuração de crossover (Auto MDIX)

Possuir capacidade de associação das portas, no mínimo, em grupo de oito, formando uma única interface lógica com as mesmas facilidades das interfaces originais, compatível com a norma IEEE 802.3ad (LACP).

Possibilitar a configuração dinâmica de portas por software, permitindo a definição de portas ativas/inativas.

Implementar VLANs por porta.

Implementar VLANs compatíveis com o padrão IEEE 802.1q.

Implementar mecanismo de seleção de quais vlans serão permitidas através de trunk IEEE 802.1q. Deve ser permitida a configuração dessa seleção de forma dinâmica.

Possuir porta de console para ligação, direta e através de modem, de terminal RS-232 para acesso à interface de linha de comando. Poderá ser fornecida porta de console com interface USB.

Deverá ser fornecido cabo de console compatível com a porta de console do equipamento.

FONTE DE ALIMENTAÇÃO

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

Suportar alimentação elétrica redundante externa capaz de alimentar o equipamento com todas as funcionalidades.

Possuir cabo de alimentação para a fonte com, no mínimo, 1,80m (um metro e oitenta centímetros) de comprimento.

DIMENSÕES

Permitir ser montado em rack padrão de 19 (dezenove) polegadas, incluindo todos os acessórios necessários.

SINALIZAÇÃO VISUAL

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

GERENCIAMENTO

Implementar os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps.

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

Sem autenticação e sem privacidade (noAuthNoPriv);

Com autenticação e sem privacidade (authNoPriv);

Com autenticação e com privacidade (authPriv).

Possuir suporte a MIB II, conforme RFC 1213.

Implementar MIB que forneça informações sobre utilização e reserva de energia para PoE.

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

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

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

Possuir armazenamento interno das mensagens de log geradas pelo equipamento de no mínimo 4096 bytes.

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

Permitir o controle da geração de traps por porta, possibilitando restringir a geração de

traps a portas específicas.

Implementar nativamente 4 grupos RMON (History, Statistcs, Alarms e Events) conforme RFC 1757

Implementar os protocolos LLDP (IEEE 802.1ab) e LLDP-MED

Possuir porta out-of-band para gerenciamento.

FACILIDADES

Implementar Telnet para acesso à interface de linha de comando.

Permitir a atualização remota do sistema operacional e arquivos de configuração utilizados no equipamento via interfaces ethernet e serial.

Ser configurável e gerenciável via GUI (graphical user interface), CLI (command line interface), SNMP, Telnet, SSH, FTP, HTTP e HTTPS com, no mínimo, 5 sessões simultâneas e independentes.

Permitir a atualização de sistema operacional através do protocolo TFTP ou FTP.

Permitir a transferência segura de arquivos para o equipamento através do protocolo SCP (Secure Copy) utilizando um cliente padrão ou SFTP (Secure FTP).

Gerenciamento remoto protocolo SSH para, implementando pelo menos o algoritmo de encriptação de dados 3DES.

Possuir SSH client, permitindo acessar servidores SSH.

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

Permitir a gravação de log externo (syslog).

Permitir o armazenamento de sua configuração em memória não volátil, podendo, numa queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior à queda de alimentação.

Possuir ferramentas para depuração e gerenciamento em primeiro nível, tais como debug, trace, log de eventos.

Suportar pelo menos quatro sessões simultâneas de espelhamento.

Permitir o espelhamento da totalidade do tráfego de uma porta, de um grupo de portas e de VLANs para outra porta localizada no mesmo switch e em outro switch do mesmo tipo conectado à mesma rede local. Deve ser possível definir o sentido do tráfego a ser espelhado: somente tráfego de entrada, somente tráfego de saída e ambos simultaneamente.

Permitir a adição manual de endereços MAC multicast na tabela de comutação, sem restrição à quantidade de portas a serem associadas.

Deve ser fornecido com documentação técnica e manuais que contenham informações suficientes para possibilitar a instalação, configuração e operacionalização do equipamento.

Implementar funcionalidade de separação do tráfego de voz e dados em uma mesma porta de acesso (Voice VLAN), sem a necessidade de utilização de IEEE 802.1q.

Permitir a criação de subgrupos dentro de uma mesma VLAN com conceito de portas isoladas e portas compartilhadas (“promíscuas”), onde portas isoladas não se comunicam com outras portas isoladas, mas apenas com as portas compartilhadas (“promíscuas”) de uma dada VLAN.

Suportar estabelecer quais VLANs serão permitidas em cada um dos troncos configurados.

Permitir a criação, remoção, gerenciamento e distribuição de VLANs de forma dinâmica através de portas configuradas como tronco IEEE 802.1q.

Responder a pacotes para teste da implementação dos níveis de serviço especificados (SLA).

Suportar no mínimo as seguintes operações de teste:

ICMP echo;

TCP connect (em qualquer porta TCP do intervalo 1-50000 que o administrador especifique).

UDP echo (em qualquer porta UDP do intervalo 1-50000 que o administrador especifique).

O switch deve suportar pelo menos 5 (cinco) destas operações de testes simultaneamente.

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

Implementar DHCP Relay, DHCP Snooping e DHCP Server em múltiplas VLANS;

Suportar empilhamento físico com cabos de empilhamento dedicados, não podendo ser utilizados portas 10Gbps com SFPs para empilhamento, permitindo empilhamento de até 8 unidades, com velocidade de empilhamento de 40Gbps full-duplex (80Gbps total).

A pilha deverá ser gerenciada através de um único endereço IP, permitir agregação lógica de links utilizando qualquer porta da pilha e permitir espelhamento de portas de qualquer porta para qualquer porta da pilha.

Deverá possuir porta USB ou protocolos TFTP, FTP para armazenamento de arquivos.

Deverá possuir funcionalidade que permita configuração automática de portas de acordo com o equipamento conectado

Suportar sFLOW, IPFIX ou funcionalidade similar.

SEGURANÇA

Implementar mecanismo de autenticação para acesso local ou remoto ao equipamento baseada em um Servidor de Autenticação/Autorização do tipo TACACS+ e RADIUS.

Implementar filtragem de pacotes (ACL - Access Control List).

Proteger a interface de comando do equipamento através de senha.

Implementar o protocolo SSH V2 para acesso à interface de linha de comando.

Permitir a criação de listas de acesso baseadas em endereço IP para limitar o acesso ao switch via Telnet, SSH e SNMP. Deve ser possível definir os endereços IP de origem das sessões Telnet e SSH.

Possibilitar o estabelecimento do número máximo de MACs que podem estar associados a uma dada porta do switch. Deve ser possível desabilitar a porta e enviar um trap SNMP caso o número de endereços MAC configurados para a porta seja excedido.

Implementar listas de controle de acesso (ACLs) baseadas em endereço IP de origem e destino, portas TCP e UDP de origem e destino.

Permitir a associação de um endereço MAC específico a uma dada porta do switch, de modo que somente a estação que tenha tal endereço possa usar a referida porta para conexão.

Implementar mecanismos de AAA (Authentication, Authorization e Accounting) com garantia de entrega.

Possuir controle de broadcast, multicast e unicast por porta.

Implementar a criptografia de todos os pacotes enviados ao servidor de controle de acesso e não só os pacotes referentes à senha.

Permitir controlar quais comandos os usuários ou grupos de usuários podem emitir em determinados elementos de rede.

Possuir suporte a mecanismo de proteção da “Root Bridge” do algoritmo “Spanning-Tree” para defesa contra ataques do tipo “Denial of Service” no ambiente nível 2.

Possuir suporte à suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta do switch esteja colocada no modo “Fast Forwarding” (conforme previsto no padrão IEEE 802.1w).

Possuir análise do protocolo DHCP e permitir que se crie uma tabela de associação entre endereços IP atribuídos dinamicamente, MAC da máquina que recebeu o endereço e porta física do switch em que se localiza tal MAC.

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

Possuir análise do protocolo ARP (Address Resolution Protocol) e possuir proteção nativa contra ataques do tipo “ARP Poisoning”.

Os processos de Autenticação, Autorização e Accounting associados a controle de acesso administrativo ao equipamento devem ser completamente independentes dos processos AAA no contexto IEEE 802.1x.

Implementar controle de acesso por porta, usando o padrão IEEE 802.1x (Port Based Network Access Control). Devem ser atendidos, no mínimo, os seguintes requisitos:

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

A estação não tem cliente IEEE 802.1x (suplicante);

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

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

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

Nome do usuário;

Switch em que o computador do usuário está conectado;

Porta do switch utilizada par acesso;

Endereço MAC da máquina utilizada pelo usuário;

Endereço IP do usuário;

Horários de início e término da conexão;

Bytes transmitidos e recebidos durante a conexão.

Deve ser possível definir, por porta, o intervalo de tempo para obrigar o cliente a se reautenticar (reautenticação periódica).

Deve ser possível forçar manualmente a reautenticação de um usuário conectado a uma porta do switch habilitada para 802.1x.

Suportar a autenticação IEEE 802.1x via endereço MAC em substituição à identificação de usuário, para equipamentos que não disponham de suplicantes.

Implementar suporte ao serviço DHCP Server em múltiplas VLANS simultaneamente, para que possa atribuir endereços IP aos clientes 802.1x autenticados e autorizados.

Deve ser suportada a autenticação de múltiplos usuários em uma mesma porta.

Deve ter tratamento de autenticação IEEE 802.1x diferenciado entre "Voice Vlan" e "Data LAN", na mesma porta para que um erro de autenticação em uma Vlan não interfira na outra.

Suportar atribuição de autenticação através do navegador (Web Authentication) caso a máquina que esteja utilizando para acesso à Rede não tenha cliente IEEE 802.1x

operacional, o portal de autenticação deve utilizar protocolo seguro tal como HTTPS.

Suportar protocolo Radius CoA (Change of Authorization), conforme RFC 5176

PADRÕES IEEE

Implementar padrão IEEE 802.1d (Spanning Tree Protocol) por VLAN.

Implementar padrão IEEE 802.1q (Vlan Frame Tagging).

Implementar padrão IEEE 802.1p (Class of Service) para cada porta.

Implementar padrão IEEE 802.1w (Rapid spanning Tree Protocol).

Implementar padrão IEEE 802.1s (Multi-Instance Spanning-Tree), com suporte a, no mínimo, 16 instâncias simultâneas do protocolo Spanning-Tree.

Implementar padrão IEEE 802.3ad Link Aggregation Control Protocol (LACP).

Implementar padrão IEEE 802.3af (PoE)

Implementar padrão IEEE 802.3at (PoE+)

MULTICAST

Implementar em todas as interfaces do switch o protocolo IGMP Snooping (v1, v2 e v3), não permitindo que o tráfego multicast seja tratado como broadcast no switch.

Implementar em todas as interfaces do switch o protocolo MLD Snooping (v1 e v2), não permitindo que o tráfego multicast IPv6 seja tratado como broadcast no switch.

QUALIDADE DE SERVIÇO (QoS)

Priorização de tráfego através do protocolo IEEE 802.1p.

Suportar fila com prioridade estrita (prioridade absoluta em relação às demais classes dentro do limite de banda que lhe foi atribuído) para tratamento do tráfego “real-time” (voz e vídeo).

Suportar Weighted Round Robin (WRR) ou Shaped Round Robin (SRR).

Classificação e Reclassificação baseadas em endereço IP de origem/destino, portas TCP e UDP de origem e destino, endereços MAC de origem e destino.

Classificação, Marcação e Remarcação baseadas em CoS ("Class of Service" - nivel 2) e DSCP ("Differentiated Services Code Point"- nivel 3), conforme definições do IETF (Internet Engineering Task Force).

Suportar funcionalidades de QoS de “Traffic Shaping” e “Traffic Policing”.

Suportar especificação de banda por classe de serviço.

Para os pacotes que excederem a especificação, deve ser possível configurar ações tais como : transmissão do pacote sem modificação, transmissão com remarcação do valor de DSCP, descarte do pacote.

Suportar mapeamento de prioridades nível 2, definidas pelo padrão IEEE 802.1p, em prioridades nível 3 (IETF DSCP – Differentiated Services Code Point definido pela Internet Engineering Task Force) e vice-versa.

Suportar mecanismos de QoS de prevenção de congestionamento como WRED (Weighted Random Early Detection) ou WTD (Weighted Tail Drop)

Suportar pelo menos quatro filas de prioridade por porta de saída (egress port)

Suportar diferenciação de QoS por VLAN

Internet Protocol versão 6 (IPv6)

Implementar IPv6.

Permitir a configuração de endereços IPv6 para gerenciamento.

Implementar protocolos de gerenciamento Ping, Traceroute, Telnet, SSH, TFTP, FTP, SNMP, SYSLOG, HTTP, HTTPS e DNS sobre IPv6.

Implementar mecanismo de Dual Stack (IPv4 e IPv6), para permitir migração de IPv4 para IPv6.

ROTEAMENTO

Suportar roteamento inter-VLAN

Suportar roteamento estático com no mínimo 16 rotas.

Implementar o protocolo VRRP ou mecanismo similar de redundância de gateway, para IPv4.

Item:	Quantidade:	Descrição:
10	**01**	**Consultoria / Serviços de implementação/ configuração**

Consultoria Projeto

2 (dois) dias de um especialista para consultoria na definição do projeto composto pelos equipamentos dos itens 1 a 9. Definir melhor arquitetura e protocolos que serão utilizados, tendo como pontos principais:

Projeto para o balanceamento de links;

Projeto para segurança utilizando os firewalls redundantes;

Projeto para o Core de Rede, com segmentação através de Vlans.

Projeto para implantar os ramais VOIP, integrando com nosso PABX MD110;

Projeto de wireless.

Implantação

7 (sete) dias para configurar todo o ambiente. Toda a instalação física é por conta da TV Cultura. Essa implementação consiste em configuração na parte logica dos equipamentos como implementar e protocolos e funções nos equipamentos adquiridos de acordo com o projeto definido.

Cursos e Treinamento

Treinamento/curso homologado pelo fabricante dos equipamentos para pelo menos 1 funcionário da TV Cultura.

10.3 Deverá ser fornecida documentação técnica e manuais que contenham informações suficientes para possibilitar a instalação, configuração e operacionalização dos

equipamentos.

10.4 Deverá ser incluída no fornecimento garantia e suporte total pelo período de 12 (doze) meses com atendimento 8 x 5 x NBD realizada pelo fabricante ou representante no Brasil.

ANEXO II

DECLARAÇÃO DE MICRO E PEQUENA EMPRESA

(EM PAPEL TIMBRADO DA LICITANTE)

Referente: Convocação Geral nº 006/2014

A empresa _____,inscrita no CNPJ n° _____, sediada (endereço completo) _____, por intermédio de seu representante legal o (a) Sr. (a) _____, CPF n° _____ e RG n° _____, DECLARA, sob as penas da Lei, que atende os dispositivos da Lei

Complementar n° 123, de 14 de dezembro de 2006, notadamente o art. 3°, tendo direito aos benefícios estendidos pelo referido Diploma.

Cidade – (UF), _____de _____ de 2014.

.

_____

(Assinatura do sócio ou procurador legal)

ANEXO III

DECLARAÇÃO CAUFESP

(EM PAPEL TIMBRADO DA EMPRESA)

Referente a Convocação Geral n° 006/2014.

Eu, (nome completo), representante legal da empresa (nome da pessoa jurídica), CNPJ: _____, interessada em participar no processo de Seleção Convocação Geral n° 006/2014, da Fundação Padre Anchieta – Centro Paulista de Rádio e TV Educativas comprometo-me a providenciar o registro no Cadastro Unificado de Fornecedores do Estado de São Paulo, em sua versão web – CAUFESP ou caso já o tenha, comprometo-me a mantê-lo atualizado, bem como providenciar a abertura de conta corrente no Banco do Brasil, sob pena de decadência do direito à contratação, sem prejuízo da aplicação das sanções cabíveis.

São Paulo, ____ de _____ de 2014.

_____

Sócio ou procurador legal

ANEXO IV

(a que se refere ao artigo 2º, do Decreto nº 42.911, de 06 de Março de 1998)

CONVOCAÇÃO GERAL Nº 006/2014 PROCESSO Nº 0264/2014

(EM PAPEL TIMBRADO DA EMPRESA)

Eu, **(nome completo)**, representante legal da empresa **(nome da pessoa jurídica)**, interessada em participar no processo de Seleção Convocação Geral nº 006/2014, Processo nº 0264/2014 da Fundação Padre Anchieta – Centro Paulista de Rádio e TV Educativas, declaro, sob as penas da lei, que, nos termos do § 6º, do artigo 27, da Lei nº 6.544, de 22 de Novembro de 1989, a **(nome da pessoa jurídica)** encontra-se em situação regular perante o Ministério do Trabalho, no que se refere à observância do disposto no inciso XXXIII, do artigo 7ª, da Constituição Federal.

São Paulo, ____ de _____ de 2014.

_____

Sócio ou procurador legal

Inciso XXXIII, do artigo 7º, da Constituição Federal:

"Proibição de trabalho noturno, perigoso ou insalubre aos menores de dezoito e de qualquer trabalho a menores de quatorze anos, salvo na condição de aprendiz."

ANEXO V

CONVOCAÇÃO GERAL Nº 006/2014 PROCESSO Nº 0264/2014

Declaração de Inexistência de Fato Impeditivo e Superveniente

(Modelo a ser redigido em papel timbrado do Proponente)

NOME DA EMPRESA) _____ CNPJ nº _____, sediada (endereço completo) _____, declara, sob as penas da lei, que até a presente data inexistem fatos impeditivos para sua habilitação no presente processo de Seleção, inclusive em virtude das disposições da Lei estadual nº 10.218, de 12/02/99, ciente da obrigatoriedade de declarar ocorrências posteriores.

São Paulo ..... de ..... de 2014

_____

Sócio ou procurador legal

ANEXO VI

Modelo de Procuração

PROCURAÇÃO (No caso de Empresa Estrangeira)

PROCURAÇÃO

Outorgante: (nome da sociedade), sociedade constituída em (país), representada neste ato por seu (cargo) _____, Sr. _____, atuando consoante os poderes contidos no (contrato social ou estatuto da empresa), de (data). (em caso de S/A deve constar o ato de eleição do detentor do cargo).

Outorgado: (nome, qualificação e domicílio no Brasil),

Pelo presente instrumento, a sociedade (outorgante) acima identificada, através de seu representante legal, nomeia e constitui seu suficiente e bastante Procurador (outorgado), para representá-la junto à Fundação Padre Anchieta – Centro Paulista de Rádio e TV Educativas, com poderes especiais para participar da Convocação Geral n° 006/2014, atuando em todas as fases do processo de Seleção, podendo apresentar ou renunciar a recursos administrativos ou judiciais contra habilitações, classificações, inabilitações e desclassificações, receber citação administrativa ou judicial que envolva qualquer fase da seleção, respondendo pelas mesmas, bem como todo e qualquer ato necessário ao bom e fiel cumprimento do presente instrumento.

(Esta Procuração deverá ser devidamente notariada e consularizada pela Autoridade Consular Brasileira do país de origem do PROPONENTE)

ANEXO VII

RESOLUÇÃO FPA N.º 005/PR/05-10/08/2005

DISPÕE SOBRE APLICAÇÃO DE MULTAS PREVISTAS NOS ARTIGOS 81, 86 E 87, DA LEI FEDERAL 8666/93 E NOS ARTIGOS 79, 80, 81 E 82, DA LEI ESTADUAL 6544/89 NA FUNDAÇÃO PADRE ANCHIETA.

Artigo 1º Estabelecer no âmbito desta Fundação, as seguintes normas:

I - Pela recusa injustificada em assinar, aceitar ou retirar o contrato ou retirar instrumento equivalente dentro do prazo estabelecido pela Administração, multa de 40% do valor do ajuste.

II - Pelo atraso injustificado na execução do contrato ou instrumento equivalente:

Em se tratando de compras e serviços:

1) - atraso até 30 dias, multas de 0,5% sobre o valor da obrigação, por dia de atraso;

2) - atraso superior a 30 dias, multa de 1,0%, sobre o valor da obrigação, por dia de atraso;

Em se tratando de obras e serviços a estas vinculadas, multa de 0,2% sobre o valor da obrigação por dia de atraso.

III -O valor do ajuste a servir de base de cálculo para as multas referidas nos incisos I e II será o valor original reajustado até a data de aplicação da penalidade.

IV -Pela inexecução total ou parcial do ajuste:

a) -multa de 10% a 30% devidamente justificada - calculada sobre o valor das mercadorias, serviços ou obras não entregues, ou da obrigação não cumprida;

b) - multa correspondente à diferença de preço resultante da nova licitação realizada para complementação ou realização da obrigação não cumprida.

§1º Se a multa for superior ao valor da garantia prestada além da perda desta, responderá o contratado pela diferença que será descontada dos pagamentos eventualmente devidos pela Administração ou cobrada judicialmente.

§2º As penalidades mencionadas nas alíneas “a” e “b”, do inciso IV são alternativas, devendo a administração optar a seu critério, por uma delas.

§3º A justificativa, como proposta, para fixação do percentual aplicável de conformidade com a alínea “a” será de responsabilidade do gestor do contrato.

Artigo 2º As multas previstas nesta Resolução serão corrigidas monetariamente, consoante o maior índice oficial, até a data de seu recolhimento.

Artigo 3º Da aplicação das multas previstas na Resolução, caberá recurso no prazo de 05 dias úteis, consoante o disposto no artigo 83, inciso I, alínea "c" e parágrafos 1º e 2º, da Lei 6.544/89 e no artigo 109 da Lei Federal 8.666/93

Artigo 4º As multas são autônomas e a aplicação de uma não exclui à da outra, exceto a mencionada no § 3º, da alínea "b", do inciso IV, da artigo 1º.

Artigo 5º As normas estabelecidas nesta Resolução deverão constar, obrigatoriamente, em todos os instrumentos convocatórios das licitações e nos contratos referentes a fornecimento de bens ou serviços.

Artigo 6º As disposições dos itens anteriores aplicam-se, também, às aquisições e serviços que, nos termos da legislação, forem realizadas com dispensa ou inexigibilidade de licitação.

Artigo 7º Esta Resolução entrará em vigor na data de sua publicação.

ANEXO VIII

MINUTA DO CONTRATO

IMPORTANTE: O contrato será devidamente adaptado considerando o tipo de empresa contemplada, em conformidade com os itens 5, 7 ou 9 deste Edital.

CONTRATO Nº _____/2014
PROCESSO Nº 0264/2014

Termo de CONTRATO que entre si celebram a **FUNDAÇÃO PADRE ANCHIETA – CENTRO PAULISTA DE RÁDIO E TV EDUCATIVAS** e a _____, (representada no Brasil pela _____), para fornecimento de equipamentos para reestruturação de rede de dados.

Pelo presente instrumento, de um lado a **FUNDAÇÃO PADRE ANCHIETA –**

CENTRO PAULISTA DE RÁDIO E TV EDUCATIVAS, inscrita no CNPJ/MF sob nº 61.914.891/0001-86, com sede na Rua Cenno Sbrighi, 378, bairro da Água Branca, em São Paulo, Estado de São Paulo, CEP 05036-900, neste ato representada por seus representantes legais, doravante denominada CONTRATANTE, e a empresa _____, sociedade _____, sede _____, representada no Brasil pela _____, inscrita no CNPJ/MF sob n° _____, com sede na _____, neste ato representada por seu representante legal, doravante denominada CONTRATADA, têm, entre si, acordados os termos deste CONTRATO DE FORNECIMENTO, de acordo com o constante no Processo n° 0264/2014, em observância à legislação que rege a espécie e ao Regulamento de Compras e Contratos da Fundação Padre Anchieta, mediante as seguintes Cláusulas e condições:

CLÁUSULA PRIMEIRA - DO OBJETO

O objeto deste CONTRATO é o fornecimento de 1 (um) conjunto de equipamentos para reestruturação da rede de dados da Fundação Padre Anchieta, incluindo consultoria de projeto, implantação, curso e treinamento, demais especificações e condições conforme Memorial Descritivo (Anexo I) deste CONTRATO.

O prazo de entrega será de até 45 (quarenta e cinco) dias.

O fornecimento inclui garantia e suporte total pelo período de 12 (doze) meses com atendimento 8 x 5 x NBD realizada pelo fabricante ou representante no Brasil.

CLÁUSULA SEGUNDA - DA VINCULAÇÃO

Este Contrato guarda consonância com a legislação pertinente, com o Regulamento de Compras e Contratos da Fundação Padre Anchieta, vinculando-se, ainda ao Edital e seus anexos, e à Proposta de Preço da CONTRATADA n° _____ datada de ___/___/2014 e demais documentos que compõem o Processo n° 0264/2014, independentemente de transcrição, que fazem parte integrante e complementar deste instrumento.

CLÁUSULA TERCEIRA – DO FORNECIMENTO

O objeto deste Contrato será fornecido, pela CONTRATADA, em conformidade com as especificações e condições descritas na proposta.

PARÁGRAFO ÚNICO. Para garantir a agilidade, a CONTRATADA disponibilizará Preposto, que será responsável pela interlocução com os setores afins da CONTRATANTE, inclusive para orientação no que se refere à engenharia de suporte e manutenção.

CLÁUSULA QUARTA - DAS OBRIGAÇÕES E RESPONSABILIDADES

I – São obrigações da CONTRATADA:

1. A CONTRATADA obriga-se a cumprir as obrigações constantes deste

CONTRATO e de seus anexos, utilizando normas técnicas oficiais, e cumprir o que segue:

Submeter à apreciação e aprovação prévia da CONTRATANTE quaisquer eventuais alterações nas especificações do equipamento;

Solucionar todos os eventuais problemas pertinentes ou relacionados com o fornecimento objeto deste CONTRATO;

Disponibilizar profissionais devidamente habilitados, capacitados para acompanhar o fornecimento;

Cumprir rigorosamente com todas as programações e atividades inerentes ao objeto deste Contrato;

Manter suporte técnico inerente ao equipamento fornecido;

Assumir a responsabilidade por todos e quaisquer impostos, taxas e contribuições fiscais e parafiscais, inclusive os de natureza previdenciária, social e trabalhista, bem como emolumentos, ônus ou encargos de qualquer natureza, decorrentes da celebração deste CONTRATO ou de sua execução;

Manter, durante toda a execução do Contrato, as condições de habilitação e qualificação exigidas no Edital de Seleção, neste CONTRATO e seus Anexos;

Ceder à Fundação Padre Anchieta, documentação técnica referente ao equipamento fornecido;

Prestar garantia e suporte total pelo período de 12 (doze) meses com atendimento 8 x 5 x NBD realizada pelo fabricante ou representante no Brasil.

II- São obrigações da CONTRATANTE:

1. A CONTRATANTE obriga-se a cumprir as obrigações constantes deste CONTRATO, e ainda:

Efetuar o pagamento pelo fornecimento conforme condições estabelecidas neste CONTRATO;

Responsabilizar-se pelo Termo de Aceite do equipamento entregue ou recusá-los, motivada e fundamentadamente;

Prestar as informações e os esclarecimentos que venham a ser solicitados pela CONTRATADA;

Gerenciar e supervisionar o fornecimento, por intermédio do Gestor do Contrato;

Advertir a CONTRATADA por escrito pelo não cumprimento das obrigações assumidas;

CLÁUSULA QUINTA - DA ALTERAÇÃO DA QUANTIDADE DO OBJETO

1. A CONTRATADA fica obrigada a aceitar, nas mesmas condições contratadas, os acréscimos ou supressões que se fizerem necessários ao objeto, a critério exclusivo da CONTRATANTE, até o limite de 25% (vinte e

cinco inteiros percentuais) do valor atualizado do CONTRATO.

2. Eventual alteração será obrigatoriamente formalizada por meio de Termo Aditivo ao presente CONTRATO.

CLÁUSULA SEXTA - DO PRAZO DE VIGÊNCIA

O presente CONTRATO vigerá pelo prazo de 6 (seis) meses contados da data de sua assinatura.

CLÁUSULA SÉTIMA - NOVAÇÃO

A não utilização, por parte da FUNDAÇÃO PADRE ANCHIETA, de quaisquer direitos a ela assegurados neste CONTRATO ou na legislação em geral, ou a não aplicação de quaisquer sanções neles previstas, não importa em novação quanto a seus termos, não devendo, portanto, ser interpretada como renúncia ou desistência de aplicação de sanções ou de ações futuras. Todos os recursos postos à disposição da FUNDAÇÃO PADRE ANCHIETA, neste CONTRATO, serão considerados como cumulativos e não alternativos, inclusive em relação a dispositivos legais.

CLÁUSULA OITAVA - PRAZO DE ENTREGA

O prazo de entrega será de até 45 (quarenta e cinco) dias.

CLÁUSULA NONA - DO VALOR DO CONTRATO

1. O valor total do presente CONTRATO é de USD _____,___.__ (_____) sendo que o valor total estimativo deste CONTRATO é de R$ ____.____,__ (_____), considerando a taxa de R$ _,___ correspondente ao fechamento do câmbio na data de __/__/2014.

A importação será efetuada na modalidade **EWX (Ex Works – INCOTERMS 2010)**, e os equipamentos serão colocados à disposição da Fundação Padre Anchieta em _____ (local a ser definido pela proponente comtemplada).

2. O preço acordado, em dólares, será fixo e irreajustável, durante a vigência deste Contrato.

CLÁUSULA DÉCIMA – MODALIDADE DE IMPORTAÇÃO

"Incoterms 2010": **EWX (Ex Works), o**s equipamentos deverão ser devidamente embalados para o transporte. A CONTRATANTE assume todos os custos relativos ao embarque internacional, bem como a contratação de frete internacional, seguro e demais despesas relativas ao transporte dos equipamentos.

CLÁUSULA DÉCIMA PRIMEIRA – DAS CONDIÇÕES DE PAGAMENTO

1. Os pagamentos serão efetuados, mediante a apresentação da Commercial Invoice que deverá ser encaminhada ao Setor de Compras/ Importação da Fundação Padre Anchieta, A/C do Sr. Cássio Jorge, telefone

(5511) 2182.3458 – e-mail: HYPERLINK "mailto:cassiojorge@tvcultura.com.br" cassiojorge@tvcultura.com.br, efetuado ao exportador, em reais, através do Banco do Brasil, mediante ordem de pagamento bancária no exterior, na seguinte forma:
_____;
_____;

1.1 Os pagamentos correspondentes ao valor total de USD ____,____.__ (_____), serão convertidos pela taxa de câmbio para moeda estrangeira segundo o valor para venda comercial vigente no dia útil imediatamente anterior à data do efetivo pagamento, e disponibilizado pelo Sistema de informação do Banco Central do Brasil – SISBACEN, Boletim de Fechamento.

1.2 O pagamento será efetuado em Reais (R$) de acordo com o disposto no Regulamento do Mercado de Câmbio e Capitais Internacionais, devendo a Contratada adotar o cumprimento dos ditames legais e regulamentares previstos para as providências condicionais de recebimento.

1.2.1O pagamento será efetuado através de transferência financeira para o exterior, a ser realizada para banco indicado pela Contratada.

CLÁUSULA DÉCIMA SEGUNDA – DA FISCALIZAÇÃO E GESTÃO

1. O fornecimento do objeto desta contratação terá acompanhamento, controle, fiscalização e avaliação pela Gerência de Engenharia da CONTRATANTE.

2. As exigências da fiscalização fundamentar-se-ão na proposta da CONTRATADA, nas legislações próprias, e nas regras de boa técnica.

3. Caberá ao Gestor do Contrato:

a) Fazer cumprir todas as disposições deste contrato;

b) Manifestar-se sobre as divergências quanto ao fornecimento propriamente dito.

c) Advertir a CONTRATADA por escrito pelo não cumprimento das obrigações assumidas.

CLÁUSULA DÉCIMA TERCEIRA – DA ACEITAÇÃO

1. A CONTRATANTE se reserva o direito de rejeitar no todo ou em parte o objeto contratado, se em desacordo com os termos do presente CONTRATO.

2. Quaisquer exigências da fiscalização inerentes ao objeto da presente contratação, deverão ser prontamente atendidas pela CONTRATADA**,** sem qualquer ônus para a CONTRATANTE.

CLÁUSULA DÉCIMA QUARTA - DA INEXECUÇÃO E DA RESCISÃO DO CONTRATO

A inexecução total ou parcial do Contrato poderá, a critério da CONTRATANTE, ensejar a sua rescisão unilateral, com as consequências contratuais, inclusive a suspensão do direito de licitar ou contratar com a CONTRATANTE por prazo de até 2 (dois) anos e o registro do fato no Cadastro de Fornecedores do Estado da São Paulo – CAUFESP, quando for o caso.

2. Constituem motivo para a rescisão do Contrato:

a) o não cumprimento, total ou parcial, ou o cumprimento irregular ou insatisfatório de cláusulas deste CONTRATO;

b) o atraso injustificado no prazo de entrega;

e) a associação com terceiros, a cessão ou transferência total ou parcial do CONTRATO;

f) a fusão, incorporação, cisão ou dissolução da CONTRATADA ou qualquer alteração social que possa, a critério da CONTRATANTE, prejudicar a execução do CONTRATO;

g) o não atendimento das determinações regulares da CONTRATANTE;

h) o requerimento de recuperação judicial ou extrajudicial ou a decretação de falência da CONTRATADA, ou o protesto de títulos, ou emissão de cheques sem a devida provisão de fundos caracterizadores de sua insolvência;

i) a ocorrência de caso fortuito ou de força maior, devidamente comprovados, que possa impedir a execução do CONTRATO.

3. O fato que motivar a rescisão contratual deverá ser formalmente caracterizado, sendo assegurados o contraditório e a ampla defesa da outra parte.

4. Ocorrendo a rescisão do CONTRATO por culpa da CONTRATADA, esta não terá direito a nenhuma indenização;

5. O presente CONTRATO admite rescisão amigável, por acordo entre as partes.

CLÁUSULA DÉCIMA QUINTA - DAS MULTAS

1. Se a CONTRATADA inadimplir, no todo ou em parte, este contrato, a CONTRATANTE poderá, a seu critério, sem prejuízo das penalidades previstas na cláusula anterior, aplicar as multas previstas na Resolução nº. 005/PR/05 de 10/08/2005 (ANEXO VII), do Edital.

2. As multas são independentes e a aplicação de uma não exclui a das outras.

3. O pagamento das multas previstas neste CONTRATO não exime a CONTRATADA do fiel cumprimento das obrigações e responsabilidades contraídas, nem da reparação de eventuais danos, perdas ou prejuízos que o seu ato venha acarretar à CONTRATANTE.

CLÁUSULA DÉCIMA SEXTA - DO FORO

Fica eleito o foro da Comarca da Capital do Estado de São Paulo, como sendo único competente para dirimir dúvidas ou questões do presente CONTRATO, com a expressa renúncia de qualquer outro, por mais privilegiado que seja.

E, por estarem assim justas e contratadas, assinam, as partes, juntamente com as testemunhas, o presente CONTRATO em 02 (duas) vias de igual teor, forma e idêntico valor jurídico, para um só efeito, para que produza os efeitos de direito.

São Paulo, __ de _____ de 2014.

_____

FUNDAÇÃO PADRE ANCHIETA – CENTRO PAULISTA DE RÁDIO E TV EDUCATIVAS

CONTRATANTE

_____

CONTRATADA

TESTEMUNHAS

1ª_____

2ª_____

Nome
RG nº

Nome
RG n°

TERMO DE CIÊNCIA E DE NOTIFICAÇÃO

CONTRATANTE: FUNDAÇÃO PADRE ANCHIETA – CENTRO PAULISTA DE RÁDIO E TV EDUCATIVAS

CONTRATADA: _____, sociedade empresária _____, representada no Brasil pela _____ **,** inscrita no CNPJ/MF sob n° _____ , com sede na _____ , neste ato por seu representante legal.

CONTRATO Nº _____/2014:

OBJETO: FORNECIMENTO DE 1 (UM) CONJUNTO DE EQUIPAMENTOS PARA REESTRUTURAÇÃO DA REDE DE DADOS DA FUNDAÇÃO PADRE ANCHIETA, INCLUINDO CONSULTORIA DE PROJETO, IMPLANTAÇÃO, CURSO E TREINAMENTO, DEMAIS ESPECIFICAÇÕES E CONDIÇÕES CONFORME MEMORIAL DESCRITIVO (ANEXO I). O FORNECIMENTO INCLUI GARANTIA E SUPORTE TOTAL PELO PERÍODO DE 12 (DOZE) MESES COM ATENDIMENTO 8 X 5 X NBD REALIZADA PELO FABRICANTE OU REPRESENTANTE NO BRASIL.

Na qualidade de Contratante e Contratado, respectivamente, do Termo acima identificado, e, cientes do seu encaminhamento ao TRIBUNAL DE CONTAS DO ESTADO DE SÃO PAULO, para fins de instrução de julgamento, damo-nos por CIENTES e NOTIFICADOS para acompanhar todos os atos da tramitação processual, até julgamento final e sua publicação e, se for o caso e de nosso interesse, para, nos prazos e nas formas legais e regimentais, exercer o direito da defesa, interpor recursos e o mais que couber.

Outrossim, estamos CIENTES, doravante, de que todos os despachos e decisões que vierem a ser tomados relativamente ao aludido processo serão publicados no Diário Oficial do Estado, Caderno do Poder Legislativo, parte do Tribunal de Contas do Estado de São Paulo, de conformidade com o artigo 90, da Lei Complementar Estadual nº 709, de 14 de janeiro de 1993, iniciando-se, a partir de então, a contagem dos prazos processuais.

São Paulo, __ de _____ de 2014.

_____

FUNDAÇÃO PADRE ANCHIETA – CENTRO PAULISTA DE RÁDIO E TV EDUCATIVAS
CONTRATANTE

_____

CONTRATADA

FUNDAÇÃO PADRE ANCHIETA – CENTRO PAULISTA DE RÁDIO E TV EDUCATIVAS
Rua Cenno Sbrighi, 378 – Água Branca – CEP 05036-900 – São Paulo – Capital
Tel : 2182-3156 – Fax : 3611-1518
licitacao@tvcultura.com.br
CNPJ 61.914.891/0001-86