MINISTÉRIO DA DEFESA
EXÉRCITOBRASILEIRO
DEPARTAMENTO DE ENGENHARIA E CONSTRUÇÃO
(Departamento Técnico e de Produção do Exército / 1946)

EDITAL DE PREGÃO ELETRÔNICO Nr17/2013-DEC-SRP

(CONTRATAÇÃO DE SOLUÇÃO DE TI)

OBSERVAÇÕES IMPORTANTES:

1) O PRESENTE EDITAL E OS ANEXOS PODEM SER OBTIDOS DAS SEGUINTES FORMAS:

a) POR MEIO DO E-MAIL: CPL@DEC.EB.MIL.BR

b) DIRETAMENTO NO DEC, MEDIANTE APRESENTAÇÃO DE CD-R, CD-RW, PEN DRIVE OU OUTRO DISPOSITIVO QUE PERMITA CÓPIA DOS ARQUIVOS;

c) POR MEIO DO SITE: www.comprasnet.gov.br **e** www.dec.eb.mil.br

2) INFORMAÇÕES COMPLEMENTARES SOBRE O PRESENTE EDITAL E SEUS ANEXOS PODERÃO SER OBTIDAS JUNTO À SEÇÃO DE LICITAÇÕES (CPL) DO DEPARTAMENTO DE ENGENHARIA E CONSTRUÇÃO, SITUADO NO QGEX, BLOCO B, 3º PISO, SETOR MILITAR URBANO, BRASÍLIA DF, PELOS TELEFONES (061) 3415-5091 E 3415-4862 E E-MAIL - CPL@DEC.EB.MIL.BR, NO HORÁRIO DAS 09:30 H ÀS 11:30 HORAS E DAS 13:30 ÀS 16:30 HORAS, DE 2ª A 5ª E NO HORÁRIO DE 08:30 ÀS 11:30 HORAS NA SEXTA-FEIRA;**

3) TRATAMENTO DIFERENCIADO PARA ME/EPP/COOPERATIVA.

Processo Administrativo Nr118/2013 – DEC - SRP
Modalidade de Licitação: PREGÃO ELETRÔNICO
Tipo de Licitação: MENOR PREÇO GLOBAL
Data de abertura da sessão pública: 10/12/2013
Horário: 10:00 horas (horário de Brasília)
Local: www.comprasnet.gov.br

A UNIÃO, PESSOA JURÍDICA DE DIREITO PÚBLICO INTERNO, por intermédio do Ministério da Defesa/Comando do Exército/**DEPARTAMENTO DE ENGENHARIA E CONSTRUÇÃO (DEC**), Organização Militar do Exército Brasileiro, inscrito no CNPJ nº 07.521.315/0001-23, torna público por meio de seus Pregoeiros, designados pelos Boletins Interno Nº 106,e 178 de 06 de junho de 2011e 21 de setembro de 2011, respectivamente, que fará realizar licitação, na modalidade **PREGÃO ELETRÔNICO**, do tipo **menor preço global, com a finalidade de escolher a proposta mais vantajosa para a União e realizar o Registro de Preços para a contratação de uma solução de segurança e comunicação unificada na**

infraestrutura de tecnologia da Informação do DEC. O procedimento licitatório obedecerá a Lei nº 10.520, de 17 de julho de 2002, ao Decreto n.º 5.450, de 31 de maio de 2005, que regulamenta a modalidade do Pregão Eletrônico, o Decreto nº 3.555, de 08 de agosto de 2000 e suas alterações, a Lei Complementar nº 123, de 14 de dezembro de 2006, Decreto nº 6204, de 05 de setembro de 2007, ao Decreto n° 7.892, de 23 de janeiro de 2013, que regulamenta o Sistema de Registro de Preços previsto no art. 15 da Lei nº 8.666/93, a Instrução Normativa nº 01 de 19 de janeiro de 2010, aplicando-se, subsidiariamente, as normas da Lei nº 8.666/93, de 21 de junho de 1993 e suas alterações, a IG 12-02 (Instruções Gerais sobre Licitações e Contratos no âmbito do Comando do Exército), demais diplomas legais vigentes, bem como as condições estabelecidas no presente Edital e seus anexos.

1. DO OBJETO

Aquisição de solução de segurança e comunicação unificada na infraestrutura de tecnologia da informação do Departamento de Engenharia e Construção (DEC) e Diretorias Subordinadas, visando à adequação da tecnologia existente para uma infraestrutura com controles e administração efetiva, bem como a implantação de meios não existentes, como enlace externo próprio e infraestrutura de segurança interna e externa para atender a demanda do DEC.

2. ESCLARECIMENTOS INICIAIS E CONDIÇÕES DE PARTICIPAÇÃO

2.1. PODERÃO PARTICIPAR DESTE PREGÃO AS EMPRESAS QUE:

2.1.1.atendam às condições deste edital e apresentem os documentos nele exigidos, em original ou por qualquer processo de cópia autenticada por Cartório de Notas e Ofício competente, ou por servidor da Equipe de Apoio do Pregão, à vista dos originais;

2.1.2.estejam cadastradas no Sistema de Cadastramento Unificado de Fornecedores – SICAF, nos termos do Decreto 4.485, de 25 de novembro de 2002;

2.1.3.as empresas não cadastradas no SICAF e que tiverem interesse em participar do presente pregão deverão providenciar o seu cadastramento e sua habilitação junto a qualquer Unidade Cadastradora dos órgãos da Administração Pública, até o terceiro dia útil anterior à data do recebimento das propostas;

2.1.4.não estejam sob falência, dissoluções, liquidações, consórcios de empresas, e não sejam controladoras, coligadas ou subsidiárias entre si; e

2.1.5.não tenham sido declaradas inidôneas por qualquer órgão da Administração Pública, direta ou indireta, federal, estadual, municipal ou do Distrito Federal.

2.2. No campo "descrição detalhada do objeto ofertado", de preenchimento obrigatório do fornecedor, as licitantes deverão lançar o detalhamento completo da solução ofertada, identificando a marca e o modelo dos equipamentos e dos softwares ofertados, bem como as descrições sucintas dos treinamentos, conforme modelo de proposta comercial constante do Anexo II a este Edital.

2.3. Os licitantes deverão observar os critérios de sustentabilidade previstos no Art 6º da Instrução Normativa nº 01, de 19 de janeiro de 2010, quando couber.

2.4. A linha de fornecimento do licitante vencedor será consultada no SICAF, ocasião em que será verificado se o mesmo está autorizado a comercializar serviços e equipamentos de TI que atendam as especificações constantes do Termo de Referência – Anexo I, deste Edital. Se houver necessidade de maiores esclarecimentos, será realizada uma consulta ao Cadastro Nacional de Pessoas Jurídicas(CNPJ) e, poderá ser solicitado ao licitante da proposta analisada que envie o Contrato Social da empresa que foi registrado na Junta Comercial do respectivo estado da federação. Se o licitante não possuir a autorização para comercializar os serviços e/ou equipamentos objeto deste certame, terá sua proposta recusada.

3. UNIDADE GERENCIADORA

3.1. DEPARTAMENTO DE ENGENHARIA E CONSTRUÇÃO-160067- Órgão Gerenciador;

4. DA REPRESENTAÇÃO E DO CREDENCIAMENTO

4.1.O Credenciamento dar-se-á pela atribuição de chave de identificação e de senha, pessoal e intransferível, para acesso ao sistema eletrônico. (§ 1º, Art. 3º do Decreto 5.450/2005), no site: http://www.comprasnet.gov.br

4.2.O Credenciamento do Licitante dependerá do registro cadastral atualizado no Sistema de Cadastramento Unificado de Fornecedores – **SICAF**, que também será requisito obrigatório para fins de habilitação.

4.3.O Credenciamento junto ao provedor do sistema implica a responsabilidade legal do licitante ou seu representante legal e a presunção de sua capacidade técnica para realização das transações referentes ao pregão eletrônico (§ 6º, do Art. 3º, do Decreto 5.450/2005).

4.4.O uso da senha de acesso pelo licitante é de sua responsabilidade exclusiva, incluindo qualquer transação efetuada diretamente ou por seu representante, não cabendo ao provedor do sistema e nem ao DEC, promotor da licitação, a responsabilidade por eventuais danos decorrentes de uso indevido da senha, ainda que por terceiros (§ 5º, do Art.3º, do Decreto 5.450/2005).

5. DO ENVIO DA PROPOSTA DE PREÇOS

5.1. O licitante será responsável por todas as transações que forem efetuadas em seu nome no sistema eletrônico **http://www.comprasnet.gov.br**, assumindo como firmes e verdadeiras suas propostas e lances. (inc III, do Art. 13, do Decreto 5.450/2005).

5.2. O licitante deverá acompanhar as operações no sistema eletrônico durante a sessão pública do pregão, ficando responsável pelo ônus decorrente da perda de negócios diante da inobservância de quaisquer mensagens emitidas pelo sistema ou de sua desconexão. (inc IV, Art. 13, do Decreto 5.450/2005).

5.3.A participação no pregão dar-se-á por meio da digitação da senha privativa do licitante e subseqüente encaminhamento da proposta de preços, no valor global ofertado,**das 10:00 horas do dia 27 de novembro de 2013 às 10:00 horas do dia 10 de dezembro de 2013,** exclusivamente por meio do sistema eletrônico. (§ 1°, Art. 21, do Decreto 5.450/2005).

5.4. Como requisito para a participação no pregão, o licitante deverá manifestar, em campo próprio do sistema eletrônico, o pleno conhecimento e atendimento às exigências de habilitação previstas no Edital.

5.5. A Proposta Comercial vencedora, contendo as especificações técnicas detalhadas do objeto ofertado deverá ser enviada em formulário específico, de acordo com Anexo II deste Edital, bem como os demais documentos previstos para habilitação, nos 90 (noventa) minutos seguintes ao encerramento da fase de lances,

pelos seguintes meios: digitalizado e assinado via sistema do comprasnet, ou por e-mail cpl@dec.eb.mil.br(o(s) arquivo(s) não poderão ser superiores a 3(três) MB**), ou via fax (061) 3415-5091. Após a homologação do certame os documentos originais** ou cópias, autenticadas por cartório competente, deverão ser apresentados no prazo de até 05 (dois) dias úteis, **contendo os seguintes detalhes:**

5.5.1.a proposta comercial deverá ser apresentada de acordo com o modelo descrito no Anexo II deste Edital, em original, em papel timbrado da licitante ou identificado com nome/razão social (com o CNPJ), em uma via, sem emendas, rasuras ou entrelinhas, com todos os valores propostos expressos, obrigatoriamente, em Real;

5.5.2.a oferta deverá ser firme e precisa, limitada, rigorosamente, ao objeto desta licitação, sem conter alternativas de preço ou qualquer outra condição que induza o julgamento a ter mais de um resultado, sob pena de desclassificação;

5.5.3.a oferta deverá descrever individualmente **marca, modelo, código de identificação (partnumber) e outras informações necessárias à perfeita caracterização dos equipamentos ofertados**, bem como de todos os componentes fornecidos que sejam opcionais ou que possam oferecer variação de configuração, a fim de permitir a correta identificação dos mesmos na documentação técnica apresentada. Os serviços deverão ser descritos e relacionados com os equipamentos e/ou softwares. As descrições dos serviços de operação assistida e as descrições dos serviços deverão ser o mais detalhada possível, possibilitando uma melhor análise por parte da equipe de apoio ao pregoeiro, a qual emitirá um parecer a respeito da aceitabilidade da proposta para decisão do pregoeiro quanto a aceitação ou não da aludida proposta.

5.5.4.consignar a assinatura do responsável pela elaboração da proposta comercial, bem como a identificação do mesmo abaixo da assinatura, informando o CPJ e a função que o mesmo exerce na organização. A não identificação do nome do responsável abaixo da assinatura não constitui motivo de desclassificação da licitante, contudo esta informação deverá ser fornecida ainda na fase de julgamento da proposta;

5.5.5.não serão admitidas propostas de licitantes que apresentarem as unidades de fornecimento de materiais e serviços diferentes das estabelecidas neste edital;

5.5.6.a proposta não poderá ter validade inferior a **60 (sessenta)** dias corridos, a contar da data de sua apresentação;

5.5.7.deverá constar preço unitário por item e total por grupo. **Como critério de aceitabilidade das propostas de preços será adotado o menor preço por item e menor preço por grupo, nunca sendo superiores ao valores estipulados nesse EDITAL.** Em caso de divergência entre o valor unitário e o valor total será considerado o primeiro, e, entre o valor expresso em algarismo e o valor expresso por extenso, será considerado o valor por extenso. O preenchimento incorreto dos itens necessários para o julgamento implicará na desclassificação da Proposta Comercial da licitante;

5.5.8.declaração expressa de que nos preços estão incluídos todos os impostos, taxas, fretes, seguros, bem como quaisquer outras despesas, diretas e indiretas, incidentes até a efetiva entrega, instalação e treinamentos constantes da proposta comercial ofertada;

5.5.9.conter os seguintes dados do licitante: Razão Social, endereço, telefone/Fax, número do CNPJ/MF, Banco, agência, número da conta corrente e praça de pagamento; e

5.5.10.declaração de conhecimento e concordância com os termos deste Pregão.

5.6. Após apresentação da proposta, não caberá desistência, salvo por motivo justo decorrente de fato superveniente e aceito pelo Pregoeiro.

5.7. Serão desclassificadas as propostas que não atendam às exigências do presente Edital e/ou seus anexos, ou que sejam omissas ou apresentem irregularidades, ou defeitos capazes de dificultar o julgamento da proposta comercial.

5.8. A apresentação da proposta implicará na plena aceitação, por parte do proponente, das condições estabelecidas neste Edital e seus anexos.

5.9.A licitante que não encaminhar os documentos conforme as orientações constantes do item 5.5 deste Edital, será desclassificado.

6. DA ABERTURA DAS PROPOSTAS

A sessão pública deste Pregão Eletrônico será aberta às 10:00h do dia 10 de dezembro de 2013. (horário de Brasília-DF).

7. DA FORMULAÇÃO DOS LANCES

7.1. Aberta a etapa competitiva, os licitantes poderão encaminhar lances exclusivamente por meio do sistema eletrônico, sendo o licitante imediatamente informado do seu recebimento e respectivo horário de registro e valor.

7.2. Os licitantes poderão oferecer lances sucessivos, observados o horário fixado e as regras de aceitação dos mesmos.

7.3.Só serão aceitos os lances cujos valores forem inferiores ao último lance que tenha sido anteriormente registrado no sistema.

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

7.5. Durante o transcurso da sessão pública, os licitantes serão informados, em tempo real, do valor do menor lance registrado que tenha sido apresentado pelos demais licitantes, vedada a identificação do detentor do lance.

7.6.A etapa de lances da sessão pública será encerrada mediante aviso de fechamento, emitido pelo sistema eletrônico aos licitantes. Findo o prazo, automaticamente, será encerrada a recepção de lances.

7.7. Após o fechamento da etapa de lances, o pregoeiro poderá encaminhar, pelo sistema eletrônico, contraproposta diretamente ao licitante que tenha apresentado o lance de menor valor, para que seja iniciada a negociação na busca de um preço justo

8. DO JULGAMENTO DAS PROPOSTAS

8.1.O Pregoeiro efetuará o julgamento das propostas de preços e poderá encaminhar, pelo sistema eletrônico, contraproposta ao licitante que tenha apresentado o lance de menor valor, com o objetivo de obter o preço justo para a solução apresentada, bem como decidir sobre sua aceitação.

8.2. Após a sessão de lances, analisando a aceitabilidade ou não, o Pregoeiro anunciará o licitante vencedor imediatamente após o encerramento da etapa de lances da sessão pública ou, quando for o caso, após negociação e decisão pelo pregoeiro acerca da aceitação do lance de menor valor. **Como critério de aceitabilidade das propostas de preços será adotado o menor preço por item e menor preço por grupo, nunca sendo superiores ao valores estipulados nesse EDITAL. Em caso de verificação de valores superiores estabelecidos será desclassificado o licitante.**

8.3. Se a proposta ou o lance de menor valor não for aceitável, ou se o licitante não atender às exigências de habilitação, o pregoeiro examinará a proposta ou o lance subseqüente, verificando a sua aceitabilidade e procedendo à sua habilitação, na ordem

de classificação, e assim sucessivamente, até a apuração de uma proposta ou lance que atenda ao edital por um preço justo.

8.4. No caso de desconexão com o pregoeiro, no decorrer da etapa competitiva do pregão, o sistema eletrônico poderá permanecer acessível aos licitantes para a recepção dos lances, retornando o pregoeiro, quando possível, sua atuação no certame, sem prejuízo dos atos realizados. Quando a desconexão persistir por tempo superior a **10 (dez) minutos**, a sessão do pregão será suspensa e terá reinício somente após comunicação expressa aos participantes.

8.5. O pregoeiro poderá, caso julgue necessário, solicitar maiores esclarecimentos sobre a composição dos preços unitários propostos, e/ou suspender o certame e fazer uma diligência técnica, na qual será verificada infraestrutura da licitante, bem como o sistema de logística que a mesma empregará para cumprir as cláusulas contratuais, serão dirimidas dúvidas quanto às marcas e aos modelos ofertados, e será visitada uma das instituições que atestou a capacidade técnica para a licitante vencedora, para checar a correlação dos serviços e equipamentos prestados com os ofertados.

9. DA MICRO EMPRESA E EPP

9.1. Caso as propostas apresentadas por microempresas e empresas de pequeno porte sejam iguais ou até 5% (cinco por cento) superiores à proposta detentora do melhor lance ou valor negociado, será assegurada preferência de contratação, respeitado o seguinte:

9.2.a microempresa ou empresa de pequeno porte mais bem classificada poderá apresentar proposta de preço inferior àquela detentora do melhor lance ou valor negociado, situação em que será adjudicado em seu favor o objeto deste Pregão;

9.3.não ocorrendo a contratação da microempresa ou empresa de pequeno porte, na forma do subitem anterior, serão convocadas as **licitantes** remanescentes que porventura se enquadrem na hipótese desta condição, na ordem classificatória, para o exercício do mesmo direito;

9.4.no caso de equivalência dos valores apresentados pelas microempresas e empresas de pequeno porte que se encontrem nos intervalos estabelecidos nesta condição, será realizado sorteio entre elas para que se identifique aquela que primeiro poderá apresentar melhor oferta;

9.5.a microempresa ou empresa de pequeno porte mais bem classificada será convocada para apresentar nova proposta no prazo máximo de 30 (trinta) minutos após a solicitação do Pregoeiro, sob pena de preclusão;
9.6.na hipótese da não-contratação nos termos previstos nesta condição, o objeto será adjudicado em favor da proposta originalmente vencedora do certame;
9.7.o disposto nesta Condição somente se aplicará quando a melhor oferta inicial não tiver sido apresentada por microempresa ou empresa de pequeno porte;

9.8.o Pregoeiro solicitará documentos que comprovem o enquadramento da licitante na categoria de microempresa ou empresa de pequeno porte, de acordo com o anexo VI.
9.9.tratamento diferenciado para ME/EPP/Cooperativa para este edital.

10. DA HABILITAÇÃO

10.1.A Habilitação das licitantes será verificada **"On-Line",** no Sistema de Cadastro Unificado de Fornecedores – **SICAF**, após o exame da aceitabilidade da proposta, devendo, ainda, a licitante apresentar:

10.1.1. Declaração de Fatos Impeditivos, conforme regulamentação constante da IN nº. 02-SLTI, de 11 Out 10, nos termos do modelo constante do Anexo V deste Edital, assinada por sócio, dirigente, proprietário ou procurador da licitante, com o número da identidade do declarante;

10.1.2. Declaração de que a empresa não utiliza mão-de-obra direta ou indireta de menores de idade, Lei Nº 9.854, de 27 de outubro de 1999, nos termos do modelo constante do Anexo IV deste Edital;

10.1.3. Atestados de Boa e Regular Execução do Objeto (Capacidade Técnica), que deverá ser fornecido por pessoa jurídica de direito público ou privado, em que conste que a licitante tenha executado, a contento, o objeto da presente licitação, nos termos do modelo constante do Anexo III deste Edital;

10.1.4. Documento do fabricante dos equipamentos ou de distribuidor autorizado, atestando a origem dos equipamentos ofertados;

10.1.5. Documento do(s) fabricante(s), comprovando que a licitante é credenciada para realizar suporte nos equipamentos e softwares ofertados, objeto deste Edital;

10.1.6. Declaração de Elaboração Independente da Proposta;

10.1.7. Declaração para ME/EPP, quando for o caso(Anexo XI);

10.1.8. Declaração de Preferência de Contratação, quando for o caso(Anexo X);

10.1.9. Certidão Negativa de Débitos Trabalhistas – CNDT(Lei 12.440, de 07 Jul 11);

10.1.10 A boa situação financeira do licitante será avaliada pelos Índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), maiores ou igual a 1 (um), resultantes da aplicação das fórmulas abaixo, com os valores extraídos de seu balanço patrimonial ou apurados mediante consulta on-line, no caso de empresas inscritas no SICAF:

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

$$SG=\frac{\text{Ativo Total}}{\text{Passivo Circulante +Exigível a Longo Prazo}}$$

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

10.1.11. O licitante que apresentar índices econômicos inferiores a 1 (um) em qualquer dos índices de Liquidez Geral, Solvência Geral e Liquidez Corrente deverá comprovar que possui (capital mínimo ou patrimônio líquido) equivalente a 10 % (dez por cento) do valor total estimado da contratação, devendo a comprovação ser feita relativamente à data da apresentação da proposta, na forma da lei, admitida a atualização para esta data através de índices oficiais.

10.2. Em hipótese alguma será concedido prazo para a apresentação de documentos de habilitação que não tiverem sido entregues na sessão própria, de modo que a falta de quaisquer documentos implicará a inabilitação da licitante.

10.3. DISPOSIÇÕES GERAIS DA HABILITAÇÃO

10.3.1. Os documentos necessários à habilitação poderão ser apresentados em original, ou em cópia autenticada por cartório competente, ou publicação em órgão da imprensa oficial ou em cópias simples, desde que acompanhadas dos originais para conferência pelo Pregoeiro e sua equipe de apoio.

10.3.2. A Empresa ou sociedade estrangeira em funcionamento no país deverá apresentar, também, o decreto de autorização ou o ato de registro ou autorização para funcionamento expedido pelo órgão competente, quando a atividade assim o exigir.

11. DA IMPUGNAÇÃO DO ATO CONVOCATÓRIO

11.1. Qualquer pessoa poderá solicitar impugnação do ato convocatório deste Pregão, até 02 (dois) dias úteis antes do término da data fixada para recebimento das propostas. Decairá do direito de impugnar os termos deste Edital, perante a Administração, os licitantes que não o fizerem até o prazo estipulado.

11.2. Qualquer pessoa poderá solicitar esclarecimentos ou providências do ato convocatório deste Pregão, até 03 (três) dias úteis antes do término da data fixada para recebimento das propostas. Decairá do direito de esclarecimentos dos termos deste Edital, perante a Administração, os licitantes que não o fizerem até o prazo estipulado.

11.3. Caberá ao Pregoeiro decidir sobre a petição no prazo de vinte e quatro horas.

11.4. Acolhida à petição contra o ato convocatório, será designada nova data para a realização do certame.

12. DOS RECURSOS

12.1. É admissível impugnação, recurso, representação e pedido de reconsideração dentro das razões e condições definidas nos Art. 41 e 109 da Lei nº 8.666/93 e suas alterações posteriores.

12.2. Os recursos serão dirigidos ao Ordenador de Despesas, por intermédio do Pregoeiro e realizados exclusivamente no âmbito do sistema eletrônico, em formulários próprios. O licitante deverá atentar-se à abertura do prazo para intenção de recursos, comandado no SISTEMA pelo pregoeiro. Não serão considerados recursos interpostos após o fechamento do prazo.

12.3. O recurso contra decisão do Pregoeiro não terá efeito suspensivo.

12.4. O acolhimento do recurso importará a invalidação apenas dos atos insuscetíveis de aproveitamento.

12.5. Os autos permanecerão com vista franqueada aos interessados, na Seção de Licitações do DEC, situada no QGEx, Bloco "B", 3º Piso, SMU – BRASÍLIA-DF.

13. DAS CONDIÇÕES DE ENTREGA E RECEBIMENTO DO OBJETO

13.1. Os Serviços e materiais deverão ser entregues no Departamento de Engenharia e Construção, localizado à Av. do Exército, Quartel General do Exército - QGEX, Bloco "B" – 3º Piso, SMU, Brasília – DF e no IBGE Rua General Canabarro, 706 – CPD – Bloco B – Macaranã – Rio de Janeiro – RJ.

13.2. O recebimento dos materiais e serviços far-se-á da seguinte forma:

13.2.1.provisoriamente, quantitativamente, para posterior comprovação da conformidade do bem com as especificações constantes do Anexo I (Termo de Referência) deste Edital;

13.2.2.definitivamente, pela Comissão de Recebimento e Exame, a ser designada pela Fiscalização, após comprovação da compatibilidade do bem com as especificações constantes do Anexo I (Termo de Referência) do Edital e o seu funcionamento, após a instalação;

13.2.3.rejeitado, quando os materiais estiverem em desacordo com o estabelecido no Anexo I (Termo de Referência) do Edital ou se os materiais apresentarem falhas de funcionamento e de uso.

13.3.A contratante convocará a licitante vencedora, durante a validade da ATA, para, no prazo máximo de 5 (cinco) dias, aceitar e retirar a nota de empenho (NE), sob pena de decair o direito ao fornecimento, sem prejuízo das sanções previstas no art. 81, da Lei 8.666/93. O prazo de convocação poderá ser prorrogado uma vez, por igual período, quando solicitado pela licitante vencedora durante o seu transcurso, desde que ocorra motivo justificado e aceito pela contratante.

13.4.O prazo de entrega dos materiais deverá ser de no máximo 60 (sessenta) dias corridos, após o recebimento do empenho, pela contratada, e o início da prestação dos serviços deverão ocorrer até 20 (vinte) dias corridos, após o recebimento da ordem de serviço que será fornecida pelo gestor do contrato.

13.5 Os treinamentos serão realizados quando das instalações dos equipamentos e softwares, em datas propostas pela contratada e aprovadas pela contratante.

14. DOTAÇÃO ORÇAMENTÁRIA

As despesas decorrentes da aquisição do objeto desta Licitação correrão à conta dos recursos consignados no Orçamento Geral da União, pelo TESOURO NACIONAL, ao Exército Brasileiro – Departamento de Engenharia e Construção, no exercício financeiro de 2013, programa trabalho 05122075020000001, PTRES 52121, Planos Interno (PI) I3DAFUNADOM, além das Ações Orçamentárias geridas pelo DEC: , cujo montante esteja previsto nos recursos destinados para a Administração Central. Neste contexto, também poderão ser utilizados os recursos provenientes de Destaques Orçamentários e de Convênios, desde que previstos como despesa da Administração Central do DEC.Poderão ser empregadas as seguintes naturezas de despesas: 44.90.52; 44.90.39 e 33.90.39.

15. DO PAGAMENTO

15.1. O pagamento será efetuado em até 30 (trinta dias) dias corridos, contados da data da aceitação dos itens constantes das notas fiscais, observada a aceitabilidade pela equipe de fiscalização do contrato.

15.2. A liberação do pagamento ficará condicionada à consulta prévia ao SICAF (via ON LINE), devendo a contratada estar com sua documentação obrigatória válida.

15.3. No caso de incorreção nos documentos apresentados, inclusive na Nota Fiscal/Fatura, serão os mesmos restituídos à adjudicatária para as correções necessárias, não respondendo o DEC por quaisquer encargos resultantes de atrasos nos pagamentos correspondentes.

15.4. A contratada só poderá emitir a nota fiscal após autorização prévia, por escrito, do gestor do contrato.

16. DAS SANÇÕES ADMINISTRATIVAS E PENALIDADES

16.1. Nos termos do art. 7º da Lei nº 10.520/2002 e art. 28 do Decreto nº 5.450/2005, ficará impedida de licitar e contratar com a União, Estados, Distrito Federal ou Municípios e será descredenciada do SICAF ou dos sistemas de cadastramento de fornecedores a que se refere o inciso XIV do art. 4º da mesma Lei, pelo prazo de até 5 (cinco) anos, sem prejuízo das multas previstas no Edital e das demais penalidades legais, a licitante que:

a. não retirar a Nota de Empenho, quando convocada dentro do prazo de validade de sua proposta;

b. apresentar documentação falsa;

c. deixar de entregar os documentos exigidos para o certame;

d. retardar, falhar ou fraudar a execução da obrigação assumida;

e. não mantiver a proposta; e

f. comportar-se de modo inidôneo ou cometer fraude fiscal.

16.2. Com fundamento nos artigos 86 e 87 da Lei nº 8.666/93 e no Decreto n° 3.555/2000, a adjudicatária ficará sujeita, no caso de atraso injustificado, assim considerado pela Administração, execução parcial ou inexecução da obrigação, sem prejuízo das responsabilidades civil e criminal, assegurada a prévia e ampla defesa, às seguintes penalidades:

a. advertência;

b. multa, nas condições estabelecidas neste edital.

16.3.O valor dos juros de mora serão calculados por dia de atraso, contados dia a dia, e aplicados cumulativamente com as multas moratórias e compensatórias, limitada a incidência a 30 (trinta) dias. Após o trigésimo dia e a critério da Administração, poderá ocorrer a não aceitação do objeto, de forma a configurar, nessa hipótese, inexecução total da obrigação assumida, sem prejuízo da rescisão unilateral da avença. Para a inexecução total do contrato será aplicada a multa de 60% do valor deste contrato;

16.4.O descumprimento total ou parcial das obrigações assumidas pelo licitante, sem justificativa aceita pelo DEC, resguardados os procedimentos legais pertinentes, poderá acarretar:

I. Multa de 0,33% (trinta e três centésimos por cento) por dia de atraso, na entrega de material ou execução de serviços, calculado sobre o valor correspondente à parte inadimplente, até o limite de 9,9%, que corresponde a até 30 (trinta) dias de atraso.

II. Após 30 (trinta) dias de atraso, a critério da contratante, será aplicada a Multa de 0,66 % (sessenta e seis centésimos por cento) por dia de atraso, na entrega de material ou execução de serviços, calculado, desde o trigésimo primeiro dia de atraso, sobre o valor

correspondente à parte inadimplente, em caráter excepcional, podendo chegar até 30 (trinta) dias de atraso. Findo este novo prazo, a critério da contratante, o contrato poderá ser rescindido unilateralmente, sem eximir a contratada das penalidades previstas neste edital.

III. Multa de 15% (quinze por cento) em caso de recusa injustificada do adjudicatário em assinar o contrato ou retirar o instrumento equivalente, dentro do prazo estabelecido neste Edital;

IV. 10% (dez por cento) sobre o valor do contrato, pelo descumprimento de qualquer cláusula do contrato, exceto prazo de entrega;

V. Advertência;

VI. Suspensão do direito de contratar com o Contratante por até 2 (dois) anos;

VII. Declaração de inidoneidade para licitar com a Administração Pública

16.5. A multa será formalizada por simples apostilamento contratual, na forma do art. 65, § 8º, da Lei nº 8.666/93 e será executada após regular processo administrativo, oferecido à contratada a oportunidade de defesa prévia, no prazo de 05 (cinco) dias úteis, a contar do recebimento da notificação, nos termos do § 3º do art. 86 da Lei nº 8.666/93, observada a seguinte ordem:

I - mediante desconto no valor da garantia depositada do respectivo contrato;
II - mediante desconto no valor das parcelas devidas à contratada; e
III - mediante procedimento administrativo ou judicial de execução.

16.6. Se a multa aplicada for superior ao valor da garantia prestada, além da perda desta, responderá à contratada pela sua diferença, devidamente atualizada pelo Índice Geral de Preços de Mercado (IGP-M) ou equivalente, que será descontada dos pagamentos eventualmente devidos pela Administração ou cobrados judicialmente. A contratada terá o prazo de 15 (quinze) dias para apresentar nova garantia contratual.

16.7. O atraso, para efeito de cálculo de multa, será contado em dias corridos, a partir do dia seguinte ao do vencimento do prazo de entrega ou execução do contrato, se dia de

expediente normal no Departamento de Engenharia e Construção, ou no primeiro dia útil seguinte.

16.8. Em despacho, com fundamentação sumária, poderá ser relevado:

> I - o atraso não superior a 5 (cinco) dias; e
> II - a execução de multa cujo montante seja inferior ao dos respectivos custos decobrança.

16.9.A multa poderá ser aplicada cumulativamente com outras sanções, segundo a natureza e a gravidade da falta cometida, observado o princípio da proporcionalidade.

16.10. A aplicação das sanções previstas não exclui a possibilidade da responsabilidade civil do Contratado por eventuais perdas e danos causados à Administração Pública. Nos casos em que houver perdas e danos para a Administração, poderá incidir multa compensatória em favor da Contratante, nos termos do art. 408 do CCB e seguintes, no valor de 100%(cem por cento) do valor do contrato por inexecução total deste.

16.11. A multa aplicada deverá ser recolhida ao Tesouro Nacional por meio de GRU (Guia de Recolhimento da União), no prazo máximo de 10 (dez) dias corridos, a contar da data do recebimento da notificação enviada pelo Contratante.

16.12. O valor da multa, no caso de não recolhimento, poderá ser descontado dos pagamentos eventualmente devidos pela Administração ou cobrada judicialmente.

16.13. A licitante convocada dentro do prazo de validade de sua proposta, que deixar de entregar ou apresentar documentação falsa exigida para o certame, ensejar o retardamento da execução de seu objeto, não mantiver a proposta, falhar ou fraudar a execução dos serviços e/ou materiais, comportar-se de modo inidôneo ou cometer fraude fiscal, poderá sofrer sanção de impedimento de licitar com a Administração Pública. Poderá ser descredenciada junto ao SICAF, pelo prazo de 5 (cinco) anos, sem prejuízo das multas previstas neste Edital e das demais cominações legais, garantido o direito do contraditório e da ampla defesa.

16.14. Decorridos 60 (trinta) dias de atraso, a nota de empenho e/ou contrato deverão ser cancelados e/ou rescindidos, exceto se houver justificado interesse da Administração em admitir atraso superior a 60 (sessenta) dias.Neste caso, o atraso não poderá ultrapassar de 15 (quinze) dias corridos, cujo valor da multa diária será igual a multa prevista no nº II do subitem 17.4 deste Edital.

17. DO TERMO DE CONTRATO

17.1. O licitante vencedor será convocado para assinar o respectivo termo de contrato, dentro do prazo de 5 (cinco) dias contados da notificação pelo DEC, considerado o prazo de validade da ATA. Este prazo poderá ser prorrogado, desde que a justificativa apresentada pela licitante vencedora seja aceita pelo DEC.

17.2. O prazo de vigência do presente contrato será a contar de sua assinatura até 12meses, podendo ser prorrogado para os serviços de manutenção e suporte, por iguais e sucessivos períodos, em conformidade com o art. nº 57 da Lei nº 8.666/93, observado o limite máximo de 48 (quarenta e oito) meses e terá sua eficácia iniciada na data da publicação do extrato do contrato no DOU.

17.3. Antes da celebração do contrato, o DEC realizará consulta "ON LINE" ao Sistema de Cadastramento Único de Fornecedores – SICAF, e ao Cadastro Informativo de Créditos não Quitados – CADIN, cujos resultados serão anexados aos autos do processo.

17.4. Após a assinatura, o extrato do contrato será publicado na imprensa oficial, de acordo com o previsto no § único do art. 61 da Lei 8.666/93.

17.5.A contratada deverá emitir um Termo de Confidencialidade de Sigilo, se comprometendo a não divulgar quaisquer informações ou conceder entrevistas, sem a devida autorização prévia. Também deverá entregar um Termo de Confidencialidade de Sigilo assinado pelos funcionários que estiverem envolvidos na elaboração do objeto contratado. O modelo do Termo de Compromisso de Sigilo será constantes dos Anexos XI e XII a este Edital.

17.6. Todos os produtos fornecidos como resultado da execução do projeto serão de propriedade do DEC, aplicando-se as restrições relativas aos direitos de propriedade intelectual e direitos autorais da solução de tecnologia da informação, conforme regula a lei nº 9.610/98.

17.7. Procedimentos e Critérios de Aceitação:

- Após a execução dos serviços, o Contratante deverá atestar a conclusão dos mesmos e avaliar a qualidade do serviço realizado. Tal aprovação não eximirá a Contratada de suas responsabilidades técnicas, administrativas e fiscais perante a Contratante.

- Em caso de defeitos identificados após o encerramento da Ordem de serviço, a Contratadadeverá iniciar as correções no prazo de 5 (cinco) horas após a notificação formal pelo Contratante.
- As prioridades de atendimento serão definidas a partir de orientação do Contratante, levando-se em conta a criticidade de cada demanda.

18. DA ATA DE REGISTRO DE PREÇOS

18.1. Após a proclamação do resultado da licitação e adjudicação do objeto da licitação pelo Pregoeiro, será efetuado o registro de preços e confeccionado a respectiva **Ata de Registro de Preços**, compromisso a ser firmado entre a licitante vencedora e o Órgão Gerenciador, sendo homologada pela autoridade competente.

18.2. O Fornecedor será convocado para, no prazo de 10 (dez) dias úteis, contados da data de recebimento da convocação, assinar a **Ata de Registro de Preços**.

18.3. O prazo para assinatura da **Ata de Registro de Preços** poderá ser prorrogado por igual período, desde que solicitado por escrito e mediante motivo justificado e aceito pela Administração.

18.4. Com a assinatura da **Ata de Registro de Preços**, a empresa que teve o seu preço registrado assume o compromisso de atender durante o prazo de sua vigência, os pedidos realizados.

18.5. A **Ata de Registro de Preços** deverá ser assinada pelo representante legal da empresa vencedora (classificada em primeiro lugar).

18.6. A **Ata de Registro de Preços** é um compromisso de fornecimento firmado pelo licitante vencedor e destina-se a subsidiar o acompanhamento dos preços.

18.7. No caso do fornecedor primeiro classificado, depois de convocado, não comparecer ou se recusar a assinar a **Ata de Registro de Preços**, sem prejuízo das sanções a ele previstas neste Edital, o DEC, registrará os demais licitantes, na ordem de classificação, mantido o preço do primeiro classificado na licitação.

18.8. Em qualquer das hipóteses acima, concluído o processo, o DEC, fará o devido apostilamento na **Ata de Registro de Preços** e informará aos demais fornecedores a nova ordem de registro.

18.9. As licitantes classificadas a partir do 2° lugar poderão aderir ao preço do 1° colocado através de manifestação de vontade por escrito para convocação pelo Inadimplemento do 1° colocado.

18.10. Fica vedada a transferência ou cessão da **Ata de Registro de Preços**.

19. DOS ÓRGÃOS GERENCIADOR E PARTICIPANTES

19.1. O órgão gerenciador será o **Departamento de Engenharia e Construção**.

19.2. Participante o seguinte órgão:

a) **IBGE** – Fun. Inst. Bras. Geografia e Estatística – Rio de Janeiro. Uasg 114601.

19.3.A ata de registro de preços, durante sua vigência, poderá ser utilizada por qualquer órgão ou entidade da administração pública que não tenha participado do certame licitatório, mediante anuência do órgão gerenciador, desde que devidamente justificada a vantagem e respeitadas, no que couber, as condições e as regras estabelecidas no Decreto nº 7.892/13, e na Lei nº 8.666/93.

19.4. Os órgãos e entidades que não tenham participado do registro de preços, quando desejarem fazer uso da ata de registro de preços, deverão consultar o órgão gerenciador da ata para manifestação sobre a possibilidade de adesão.

19.5. Caberá ao fornecedor beneficiário da Ata de Registro de Preços, observadas as condições nela estabelecidas, optar pela aceitação ou não do fornecimento, desde que este fornecimento não prejudique as obrigações anteriormente assumidas com o órgão gerenciador e órgãos participantes.

19.6. As aquisições ou contratações adicionais a que se refere este item não poderão exceder, por órgão ou entidade, a cem por cento dos quantitativos dos itens do instrumento convocatório e registrados na ata de registro de preços para o órgão gerenciador e órgãos participantes.

19.7. As adesões à ata de registro de preços serão limitadas, na totalidade, ao quíntuplo do quantitativo de cada item registrado na ata de registro de preços para o órgão gerenciador e órgãos participantes, independente do número de órgãos não participantes que eventualmente aderirem.

19.8. Ao órgão não participante que aderir à presente ata, compete os atos relativos à cobrança do cumprimento pelo fornecedor das obrigações contratualmente assumidas e a aplicação, observada a ampla defesa e o contraditório, de eventuais penalidades decorrentes do descumprimento de cláusulas contratuais, em relação às suas próprias contratações, informando as ocorrências ao órgão gerenciador.

19.9. Conforme previsto no art.22, §5º do Decreto 7.892/2013, o órgão gerenciador somente autorizará adesão à ata após a primeira aquisição por órgão integrante da ata.

19.10. Após a autorização do órgão gerenciador, o órgão não participante deverá efetivar a aquisição solicitada em até 90 (noventa) dias, devendo observar o prazo de vigência da ata.

20. DO CANCELAMENTO DA ATA DE REGISTRO DE PREÇOS

A Ata de Registro de Preços será cancelada:

20.1.automaticamente, por decurso de prazo de vigência;

20.2.quando não restarem fornecedores registrados; ou

20.3.pelo DEC, quando caracterizado o interesse público.

21. DO CANCELAMENTO DO REGISTRO DO FORNECEDOR

O fornecedor terá seu registro na Ata cancelado, por intermédio de processo administrativo específico, assegurado o contraditório e a ampla defesa.

21.1.A pedido, quando:

21.1.1.comprovar estar impossibilitado de cumprir as exigências da Ata, por ocorrência de casos fortuitos ou de força maior;

21.1.2.o seu preço registrado se tornar, comprovadamente, inexeqüível em função da elevação dos preços de mercado dos insumos que compõem o custo do produto.

21.2. Pela Administração, unilateralmente, quando:

21.2.1.a licitante não aceitar reduzir o preço registrado, na hipótese deste se tornar superior àqueles praticados no mercado;

21.2.2.o fornecedor perder qualquer condição de habilitação e qualificação técnica exigida no procedimento licitatório;

21.2.3.por razões de interesse público, devidamente, motivado e justificado;

21.2.4.o fornecedor não cumprir as obrigações decorrentes da Ata de Registro de Preços;

21.2.5.o fornecedor não comparecer ou se recusar a retirar, no prazo estabelecido, os pedidos de compra decorrentes da **Ata de Registro de Preços**; e

21.2.6.caracterizada qualquer hipótese de inexecução total ou parcial das condições estabelecidas na **Ata de Registro de Preços** ou nos pedidos de compra dela decorrentes.

22. DA VALIDADE DA ATA DE REGISTRO DE PREÇOS

A Ata de Registro de preços terá a validade de 12(doze) meses, contados a partir da homologação do certame pela Autoridade Competente.

23. DAS OBRIGAÇÕES

23.1. Da Contratada:

23.1.2.executar os serviços conforme especificado no Termo de Referência, Anexo II a este Edital;

23.1.3.prestar os esclarecimentos solicitados pelo Contratante;

23.1.4.guardar sigilo sobre as informações a que tiver acesso em razão dos serviços prestados, respondendo pela inobservância deste item, inclusive após o término do contrato;

23.1.5.providenciar a assinatura do Termo de Confidencialidade e Sigilo pelos técnicos da Contratada;

23.1.6.manter durante a vigência contratual as condições de habilitação exigidas neste Edital;

23.1.7.dar ciência ao Contratante, por escrito, de qualquer anormalidade que verificar na execução dos serviços;

23.1.8.corrigir, sem ônus para o Contratante, os defeitos, omissões ou quaisquer irregularidades dos serviços executados, ainda que identificados após o ateste dos serviços pelo Contratante;

23.1.9.apresentar a relação dos funcionários que irão prestar os serviços para a execução contratual perante o contratante, entre eles um responsável técnico e o preposto, estas duas funções poderão ser acumuladas;

23.1.10.responder pelas despesas relativas a encargos trabalhistas, seguro de acidentes, impostos, contribuições previdenciárias, deslocamentos de técnicos, postagem de software e quaisquer outras despesas que forem devidas e referentes aos serviços executados por seus funcionários, visto que os mesmos não possuem nenhum vinculo empregatício com o Contratante;

23.1.12. prestar suporte “on site”, caso o chamado não possa ser resolvido por meio eletrônico;

23.1.13.fornecer documentação técnica detalhada sobre as atualizações do produto;

23.1.14.prestar informações e orientações necessárias à utilização e ao perfeito funcionamento dos softwares e hardwares instalados;

23.1.15.refazer serviços quando apresentarem padrões de qualidade inferiores aos definidos neste edital, sem ônus adicionais para o Contratante, nos prazos estabelecidos em contrato, contados a partir da notificação;

23.1.16.prestar os serviços conforme a quantidade, a qualidade e a pontualidade exigidas neste Edital;

23.1.17.não transferir a outrem, no todo ou em parte, os serviços contratados;

23.1.18. enquanto durar o contrato, a contratada terá que disponibilizar atendimento para abertura de chamados de assistência técnica através de discagem direta local para o município de Brasília/DF, 24 horas e 7 dias por semana, ou disponibilizar um serviço de chamada gratuita para chamadas interurbanas, caso a Contratada não disponha de instalação no município de Brasília/DF;

23.1.19.comprovar a especialização e certificação dos técnicos envolvidos na instalação, com certificados emitidos pelo fabricante da solução ou por entidades credenciadas pelos fabricantes dos equipamentos e/ou softwares propostos;

23.1.20.possuir atestados de capacidade técnica, em seu nome emitido por Pessoa Jurídica de Direito Publico ou Privado, comprovando que realizou serviços de instalação e manutenção de hardware do equipamento ofertado;

23.1.21.comprovar que existe em seu quadro de funcionários, na data da assinatura do contrato, profissional detentor de certificado emitido pelo fabricante da ferramenta ofertada, ou por entidades credenciadas pelos fabricantes (sejam hardwares ou softwares);

23.1.22.enquanto durar o contrato, atender ao pedido de assistência técnica no local dos sistemas e equipamentos instalados na sede do Contratante, 24 (vinte quatro) horas por dia, 7 (sete) dias por semana e dar encaminhamento ao problema em até 24 (vinte e quatro) horas do dia seguinte ao da abertura do chamado;

23.1.23.atender ao pedido de assistência técnica por telefone, fax ou e-mail dos sistemas e equipamentos instalados nas cidades de Brasília durante todo o período de garantia, nos dias úteis (segunda a sexta-feira), no horário comercial (8 às 18 horas) e dar encaminhamento ao problema em até 24 (vinte e quatro) horas do dia seguinte ao da abertura do chamado;

23.1.24.providenciar, durante o período de vigência de contrato e suas possíveis renovações, atualização e “upgrade” de versão, bem como, patches corretivos para todos os sistemas fornecidos;

23.1.25.fornecer senha de acesso ao site do fabricante do software, com permissão para o Contratante efetuar download de novas versões e patches.

23.1.26.indenizar às suas expensas, quaisquer danos causados a terceiros em decorrência do cumprimento do presente edital;

23.2. Da Contratante:

23.2.1.efetuar o pagamento do objeto deste contrato nas condições estabelecidas por este instrumento e, após a conferência realizada pela equipe de fiscalização do Contratante, bem como realizar a retenção dos tributos e impostos, em conformidade com a legislação pertinente;

23.2.2.efetuar as requisições, de conformidade com a discriminação constante deste edital;

23.2.3.proporcionar condições necessárias ao fornecimento dos produtos solicitados;

23.2.4.prestar informações e esclarecimentos que venham a ser solicitados pela Contratada com relação ao objeto desta licitação;

23.2.5.fiscalizar e acompanhar a execução e a entrega do objeto desta licitação; e

23.2.6.comunicar à Contratada toda e qualquer ocorrência relacionada com a entrega do objeto, diligenciando nos casos que exigem providências corretivas.

24 – DA VIGÊNCIA DO CONTRATO

24.1.O prazo de vigência do contrato a ser celebrado em virtude do Edital(Anexo VII do edital)será de 12 (doze) meses a contar de sua assinatura, podendo ser prorrogado para os serviços de manutenção e suporte, por iguais e sucessivos períodos, em conformidade com o art. nº 57 da Lei nº 8.666/93, observado o limite máximo de 48 (quarenta e oito) meses e terá sua eficácia iniciada na data da publicação do extrato do contrato noDOU.

25. DA GARANTIA CONTRATUAL

25.1.A contratada deverá prestar garantia de execução do Contrato de 5% (cinco por cento) até o 5º (quinto) dia útil após a assinatura do contrato , conforme o art nº56 da Lei 8.666/93, de seu valor total, em moeda brasileira, com prazo de validade de até 02(dois) meses após o encerramento do contrato, por uma das seguintes modalidades:

25.1.1.caução em dinheiro, ou título da dívida pública;

25.1.2.seguro garantia;

25.1.3.fiança bancária.

25.2. A licitante vencedora deverá apresentar a garantia ao DEC, no ato da assinatura do contrato.

26. DA PUBLICIDADE

O Contratante providenciará a publicação do extrato do contrato no Diário Oficial da União, de acordo com a prescrição contida no art. 61 da Lei 8.666/93 e art. 13 da Instrução Normativa Nr 08, de 4 de dezembro de 1998-MARE.

27. DO FORO

As questões decorrentes da execução deste Edital, que não possam ser dirimidas administrativamente, serão processadas e julgadas na Justiça Federal, no Foro da cidade de Brasília/DF, Seção Judiciária do Distrito Federal, com exclusão de qualquer outro.

28. DAS DISPOSIÇÕES FINAIS

28.1. Esta licitação poderá ser revogada por interesse do DEC, em decorrência de fato superveniente devidamente comprovado, pertinente e suficiente para justificar o ato, ou anulada por vício ou ilegalidade, a modo próprio ou por provocação de terceiros, sem que os licitantes tenham direitos a qualquer indenização, obedecendo ao disposto no Art. 18 do Decreto 3.555/2000.

28.2. Qualquer modificação no presente EDITAL será divulgada pela mesma forma que se divulgou o texto original, reabrindo-se o prazo, inicialmente, estabelecido, exceto quando, inquestionavelmente, a alteração não afetar a formulação da proposta.

28.3. Os proponentes são responsáveis pela fidelidade e legitimidade das informações e dos documentos apresentados em qualquer fase da licitação.

28.4. Após apresentação da proposta não caberá desistência, salvo por motivo justo decorrente de fato superveniente e aceito pelo Pregoeiro.

28.5. Na contagem dos prazos estabelecidos neste Edital e seus anexos, excluir-se-á o dia do início e incluir-se-á o do vencimento, vencendo-se os prazos somente em dias de expediente normais.

28.6. O desatendimento de exigências formais não essenciais não importará no afastamento do licitante, desde que sejam possíveis as aferições das suas qualificações e as exatas compreensões da sua proposta, durante a realização da sessão pública do

pregão.

28.7. Integram este Edital os seguintes anexos:

ANEXO I – Termo de Referência;

ANEXO II – Modelo de Proposta de Preços;

ANEXO III – Modelo de Atestado de Boa e Regular Execução do Objeto (Capacidade Técnica);

ANEXO IV – Modelo de Declaração de Trabalho de Empregados em Condições Excepcionais e de Menor (Lei nº 9.854, de 27 de outubro de 1999,);

ANEXO V – Modelo de Declaração de Fatos Impeditivos;

ANEXO VI – Modelo de declaração para micro empresa e Empresa de Pequeno Porte de micro e pequena empresa

ANEXO VII – Modelo da Minuta do Contrato

ANEXO VIII – Modelo da Minuta da Ata de Registro de Preços

ANEXO IX – Modelo de Declaração de Elaboração Independente da Proposta.

ANEXO X – Declaração de Preferência de Contratação.

ANEXO X I – Modelo do Termo de Confidencialidade de Sigilo

Brasília-DF, 16 de setembro de 2013.

_____

ROBSON **COCINO** DA COSTA- Cel

Ordenador de Despesas do DEC

MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
DEPARTAMENTO DE ENGENHARIA E CONSTRUÇÃO
(Departamento Técnico e de Produção do Exército/1946)
DEPARTAMENTO REAL CORPO DE ENGENHEIROS

ANEXO I

TERMO DE REFERÊNCIA

1. OBJETO

Constitui objeto do presente Pregão Eletrônico a obtenção da proposta mais vantajosa, com a finalidade de se proceder ao Registro de Preços para aquisição de solução de segurança e comunicação unificada na infraestrutura de tecnologia da informação do Departamento de Engenharia e Construção (DEC) e Diretorias Subordinadas, visando à adequação da tecnologia existente para uma infraestrutura com controles e administração efetiva, bem como a implantação de meios não existentes, como enlace externo próprio e infraestrutura de segurança interna e externa para atender a demanda do DEC, descrita, quantificada e especificada neste Termo.

2. JUSTIFICATIVA

Conforme prescreve o Planejamento Estratégico Organizacional do Departamento de Engenharia e Construção (DEC) para o quadriênio 2013-2016, faz-se necessária a existência de uma infraestrutura de tecnologia da informação que suporte e apoie os objetivos estratégicos do DEC, bem como o seu gerenciamento. Necessidades essas evidenciadas nos itens “6. Fatores Críticos de Sucesso do DEC” (no Item “d.”) e “7. Estratégias” (no Item “c.”), e no “Anexo A – Diretrizes do Chefe do DEC 2013-2016” (no Item “f.”), todos do “Planejamento Estratégico Organizacional do DEC para o quadriênio 2013-2016.

Esta contratação está alinhada ao Plano Diretor de Tecnologia da Informação –

PDTI 2013-2016 do DEC, o qual determina as ações a serem realizadas no âmbito da Tecnologia da Informação no Departamento, visando ao apoio aos objetivos estratégicos do DEC. A implantação de uma Solução de Segurança e Comunicação Unificada visa a atender a ação "8.01 Unificação do Gerenciamento da Infraestrutura de TI (Rede e Meios)" incluída do PDTI 2013-2016 do DEC.

A adequação da infraestrutura de tecnologia da informação existente no DEC depende de aquisição de equipamentos e softwares que permitam a segmentação da rede, a administração centralizada e a segurança do ambiente. Nos últimos anos, as atribuições do Departamento de Engenharia e Construção e as demandas externas recebidas têm aumentado consideravelmente. No entanto, a equipe da Seção de Tecnologia da Informação (SG3) teve seu quadro de pessoal mantido, não acompanhando o crescimento de demandas. Especificamente, a equipe da Subseção de Infraestrutura de TI (SG3.2) tem enfrentado dificuldades na execução de seus trabalhos em função do quadro reduzido de pessoal e da grande quantidade de demandas existentes. A SG3.2 executa suas atividades sem nenhum software de gerenciamento de redes ou controle de segurança do ambiente computacional do DEC, utilizando-se apenas de scripts, análises de logs, e comandos manuais. Os equipamentos de rede existentes não permitem a implantação de um adequado ambiente de redes, com alta disponibilidade, confiabilidade e segurança.

A indisponibilidade da infraestrutura de redes do DEC atualmente gera alto impacto nas atividades do Departamento, comprometendo, inclusive, o cumprimento de sua missão. Tendo em vista a relevância das informações, este Departamento tem realizado diversas atividades que visam à modernização da infraestrutura existente, automatização de processos internos, e otimização dos investimentos em tecnologia da informação, de modo a garantir maior qualidade às informações, além de agilidade no processo de coleta, processamento e disseminação de dados. A infraestrutura de comunicação atual do DEC não está preparada para receber novas facilidades e tão pouco se encontra em condições de manter os serviços com qualidade, segurança e com garantia de disponibilidade, devido a diversas questões, dentre elas:

- Os equipamentos já estão com a vida útil expirada;
- Equipamentos sem garantia;
- Equipamentos sem suporte;

- Equipamentos sem gerência;
- Equipamentos com o firmware desatualizado;
- Modelos descontinuados;
- Falta de redundância;
- Dificuldade de gerência;
- Problemas de autenticação;
- Equipamentos de diversos fabricantes;
- Equipamentos trabalhando no limite;
- Arquitetura não hierárquica; e
- Equipamentos que carecem de atualização tecnológica, necessitando de novas funcionalidades, tais como: Power over Ethernet - PoE, 802.1x, 802.1ag, Ipv6 Route Protocol, dentre outras.

No limiar do desenho do atual cenário, percebe-se que o DEC corre muitos riscos, como ter usuários sem acesso a sistemas críticos, rede indisponível, acessos indevidos, acessos não autorizados entre outros. Por esta razão, urge a necessidade da modernização da rede através de aquisição de Solução de Segurança e Comunicação Unificada em substituição aos equipamentos de rede atuais.

A adequação da infraestrutura necessita ocorrer no formato de uma solução unificada e centralizada, envolvendo software, hardware e serviços. Os hardwares e softwares adquiridos para a solução devem ser do mesmo fabricante ou homologados por seus fabricantes como perfeitamente compatíveis entre si. Por tratar-se de uma solução com características técnicas bem definidas e específicas, a heterogeneidade de equipamentos de diversos fabricantes provocaria instabilidade e dificultaria a implantação e o gerenciamento da solução. Equipamentos de fabricantes distintos possuem especificações técnicas e utilizam tecnologias diversas para atender aos mesmos requisitos, havendo assim ausência de plena compatibilidade entre eles, apesar de serem utilizados com os mesmos fins. A solução está sendo adquirida a fim de tornar mais ágil o gerenciamento e permitir a adequação da infraestrutura de comunicação do Departamento para atender aos requisitos de segurança e estabilidade desejáveis e necessários às atividades desenvolvidas. A implantação de uma solução com equipamentos e softwares de

diversos fabricantes contrapõe-se à finalidade da aquisição. Sendo assim, a aquisição deve ser realizada como uma solução única, dividida em grupos com hardware, software e serviços compatíveis, e disponibilizada por fornecedores especializados e capacitados nas tecnologias ofertadas de modo a prover os resultados desejados.

3. FUNDAMENTO LEGAL

3.1. O fundamento legal encontra-se na Lei nº. 10.520, de 17 de julho de 2002, no Decreto nº 5.450, de 31 de maio de 2005, utilizando subsidiariamente as cominações legais da Lei nº 8.666/93 e suas alterações.

3.2. A utilização do Sistema de Registro de Preços é adotado, em virtude que as compras poderão ser realizadas parceladamente.

4. DA FORMA DE COTAÇÃO E CRITÉRIO DE ACEITABILIDADE DE PREÇOS

- Para efeito de cotação, será levado em conta o MENOR PREÇO POR ITEM E POR GRUPO.

- **Como critério de aceitabilidade das propostas de preços será adotado o menor preço por item e menor preço por grupo, nunca sendo superiores ao valores estipulados nesse EDITAL.**

5. MATERIAIS:

5.1. Os quantitativos do nº 5.2 abaixo, poderão ser adquirido sem forma parcelada dentro da vigência de validade da Ata de Registro de Preços, conforme a demanda do consumo, ficando à administração desobrigada a contratar todo o material homologado.

5.2. DESCRIÇÃO E ESPECIFICAÇÃO TÉCNICA DOS SERVIÇOS E BENS

GRUPO	ITEM	DESCRIÇÃO	Unidade	Qtde	Valor Unitário Máximo que a ADM pode pagar (R$)	Valor Total Máximo (R$)
		SERVIÇOS PARA SOLUÇÃO DE SEGURANÇA E COMUNICAÇÃO UNIFICADA				
Grupo 1 Solução WIFI	1	CONTROLADOR WIFI	UN	4	*58.528,60*	*234.114,40*
	2	Serviço de Instalação do Item 1	UN	4	*14.409,98*	*57.639,92*
	3	Serviço de Manutenção e Suporte do Item 1	UN	4	*15.317,01*	*61.268,04*
	4	CONTROLADOR WIFI REDUNDANTE	UN	4	*112.059,08*	*448.236,32*
	5	Serviço de Instalação do Item 4	UN	4	*16.059,62*	*64.238,48*

GRUPO	ITEM	DESCRIÇÃO	Unidade	Qtde	Valor Unitário Máximo que a ADM pode pagar (R$)	Valor Total Máximo (R$)
		SERVIÇOS PARA SOLUÇÃO DE SEGURANÇA E COMUNICAÇÃO UNIFICADA				
	6	Serviço de Manutenção e Suporte do Item 4	UN	4	26.773,93	107.095,72
	7	PACOTE DE EXPANSÃO PARA CONTROLADOR WIFI	UN	8	35.212,12	281.696,96
	8	Serviço de Instalação do Item 7	UN	8	5.335,73	42.685,84
	9	Serviço de Manutenção e Suporte do Item 7	UN	8	7.951,62	63.612,96
	10	SOFTWARE DE GERENCIAMENTO DA REDE WIFI	UN	4	15.423,45	61.693,80
	11	Serviço de Instalação do Item 10	UN	4	9.338,23	37.352,92
	12	Serviço de Manutenção e Suporte do Item 10	UN	4	7.269,11	29.076,44
	13	PACOTE DE EXPANSÃO PARA SOFTWARE DE GERENCIAMENTO DA REDE WIFI	UN	10	9.858,52	98.585,20
	14	Serviço de Instalação do Item 13	UN	10	3.518,62	35.186,20
	15	Serviço de Manutenção e Suporte do Item 13	UN	10	4.037,03	40.370,30
	16	PONTO DE ACESSO WIFI INTERNO	UN	100	4.124,57	412.457,00
	17	Serviço de Instalação do Item 16	UN	100	732,90	73.290,00
	18	Serviço de Manutenção e Suporte do Item 16	UN	100	584,78	58.478,00
	19	PONTO DE ACESSO WIFI EXTERNO	UN	12	28.569,64	342.835,68
	20	Serviço de Instalação do Item 19	UN	12	3.544,75	42.537,00
	21	Serviço de Manutenção e Suporte do Item 19	UN	12	2.627,64	31.531,68
	22	SITE SURVEY	UN	20	2.647,84	52.956,80
	23	OPERAÇÃO ASSISTIDA	DIA	50	1.343,53	67.176,50
	24	TREINAMENTO DO TIPO I PARA A SOLUÇÃO DE SEGURANÇA E COMUNICAÇÃO UNIFICADA (WIFI)	UN	6	43.761,50	262.569,00
Grupo 2 Solução de Controle de Acesso	25	SOLUÇÃO CENTRALIZADA DE CONTROLE DE ACESSO DE USUÁRIOS E DISPOSITIVOS	UN	2	102.281,11	204.562,22
	26	Serviço de Instalação do Item 25	UN	2	34.170,47	68.340,94
	27	Serviçode Manutenção e Suporte do Item 25	UN	2	24.291,97	48.583,94
	28	PACOTE DE EXPANSÃO PARA SOLUÇÃO CENTRALIZADA DE CONTROLE DE ACESSO DE USUÁRIOS E DISPOSITIVOS	UN	4	31.671,17	126.684,68
	29	Serviço de Instalação do Item 28	UN	4	15.811,39	63.245,56
	30	Serviçode Manutenção e Suporte do Item 28	UN	4	1.535,57	6.142,28
	31	OPERAÇÃO ASSISTIDA	DIA	20	1.343,53	26.870,60
Grupo 3 Switching	32	SWITCH DE ACESSO TIPO I	UN	15	27.083,44	406.251,60
	33	Serviço de Instalação do Item 32	UN	15	2.778,77	41.681,55
	34	Serviçode Manutenção e Suporte do Item 32	UN	15	3.295,74	49.436,10
	35	SWITCH DE ACESSO TIPO II	UN	15	32.631,79	489.476,85
	36	Serviço de Instalação do Item 35	UN	15	3.260,90	48.913,50
	37	Serviçode Manutenção e Suporte do Item 35	UN	15	4.172,29	62.584,35
	38	SWITCH DE ACESSO TIPO III	UN	15	36.430,14	546.452,10
	39	Serviço de Instalação do Item 38	UN	15	3.668,24	55.023,60
	40	Serviçode Manutenção e Suporte do Item 38	UN	15	4.844,77	72.671,55
	41	SWITCH CORE	UN	4	781.522,85	3.126.091,40
	42	Serviço de Instalação do Item 41	UN	4	85.892,90	343.571,60
	43	Serviçode Manutenção e Suporte do Item 41	UN	4	116.302,35	465.209,40

GRUPO	ITEM	DESCRIÇÃO	Unidade	Qtde	Valor Unitário Máximo que a ADM pode pagar (R$)	Valor Total Máximo (R$)
		SERVIÇOS PARA SOLUÇÃO DE SEGURANÇA E COMUNICAÇÃO UNIFICADA				
	44	CONECTOR ÓPTICO TIPO I	UN	80	5.966,72	477.337,60
	45	Serviço de Instalação do Item 44	UN	80	626,26	50.100,80
	46	CONECTOR ÓPTICO TIPO II	UN	12	17.912,76	214.953,12
	47	Serviço de Instalação do Item 46	UN	12	1.541,73	18.500,76
	48	CONECTOR ÓPTICO TIPO III	UN	80	8.654,43	692.354,40
	49	Serviço de Instalação do Item 48	UN	80	775,86	62.068,80
	50	CONECTOR ÓPTICO TIPO IV	UN	12	18.166,40	217.996,80
	51	Serviço de Instalação do Item 50	UN	12	1.616,53	19.398,36
	52	CONECTOR ÓPTICO TIPO V	UN	96	2.364,50	226.992,00
	53	Serviço de Instalação do Item 52	UN	96	230,52	22.129,92
	54	MÓDULO DE FIREWALL PARA SWITCH CORE	UN	2	551.169,64	1.102.339,28
	55	Serviço de Instalação do Item 54	UN	2	66.420,10	132.840,20
	56	Serviço de Manutenção e Suporte do Item 54	UN	2	164.449,27	328.898,54
	57	OPERAÇÃO ASSISTIDA	DIA	20	1.343,53	26.870,60
	58	TREINAMENTO DO TIPO II PARA A SOLUÇÃO DE SEGURANÇA E COMUNICAÇÃO UNIFICADA (SWITCHING)	UN	3	43.994,84	131.984,52
Grupo 4 Segurança	59	SOLUÇÃO DE FIREWALL E IPS	UN	2	72.849,56	145.699,13
	60	Serviço de Instalação do Item 59	UN	2	19.194,41	38.388,82
	61	Serviço de Manutenção e Suporte do Item 59	UN	2	31.188,03	62.376,06
	62	SOFTWARE DE GERENCIAMENTO CENTRALIZADO DE FIREWALL	UN	1	81.264,39	81.264,39
	63	Serviço de Instalação do Item 62	UN	1	14.001,29	14.001,29
	64	Serviço de Manutenção e Suporte do Item 62	UN	1	25.359,19	25.359,19
	65	SOLUÇÃO DE SEGURANÇA WEB	UN	1	171.859,72	171.859,72
	66	Serviço de Instalação do Item 65	UN	1	42.713,52	42.713,52
	67	Serviço de Manutenção e Suporte do Item 65	UN	1	20.344,60	20.344,60
	68	PACOTE DE EXPANSÃO PARA SOLUÇÃO DE SEGURANÇA WEB	UN	5	45.371,33	226.856,65
	69	Serviço de Instalação do Item 68	UN	5	6.985,73	34.928,65
	70	Serviço de Manutenção e Suporte do Item 68	UN	5	35.120,93	175.604,65
	71	OPERAÇÃO ASSISTIDA	DIA	25	1.343,53	33.588,25
	72	TREINAMENTO DO TIPO III PARA A SOLUÇÃO DE SEGURANÇA E COMUNICAÇÃO UNIFICADA (Segurança)	UN	3	43.561,50	130.684,50
Grupo 5	73	RACK TIPO I	UN	3	6.429,43	19.288,29
	74	Instalação RACK TIPO I	UN	3	1.308,93	3.926,79
Grupo 6	75	RACK TIPO II	UN	2	7.229,42	14.458,84
	76	Instalação RACK TIPO II	UN	2	1.549,14	3.098,28
		VALOR TOTAL GLOBAL				14.227.686,29

OBSERVAÇÃO:

* **O preço global máximo admitido para o objeto a ser contratado será de R$ 14.227.686,29 (quatorze milhões, duzentos e vinte e sete mil, seiscentos e oitenta e seis reais e vinte e nove centavos).**

*** Como critério de aceitabilidade, as propostas de preços das licitantes não poderão ser superiores aos valores unitários (POR ITEM e POR GRUPO), nem ao valor global estimado para esta licitação e apresentados na tabela acima. Os Grupos são independentes e poderão ser cotados por outros licitantes.**

*** Todos os itens devem ser compatíveis entre si tanto dentro dos grupos específicos quanto na solução como um todo. Assim sendo, antes da habilitação, será verificado *in loco* se os itens ofertados atendem às compatibilidades exigidas.**

*** O somatório dos valores e dos itens da tabela acima referem-se aos da UG Gerenciadora (DEC) e UG participante (IBGE).**

5.3. DESCRIÇÃO DETALHADA DOS OBJETOS A SEREM ADQUIRIDOS

5.3.1. Solução de Segurança e Comunicação Unificada

GRUPO 1 - Solução WIFI (itens 1 a 24)

Item 1. -Controlador WiFi

1) Fornecimento de Controlador WiFi 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.

2) O equipamento deve ter capacidade máxima de gerenciar simultaneamente pelo menos 500 (quinhentos) equipamentos dostipos“Ponto de Acesso WiFi” descritos neste Termo de Referência. Deve ter capacidade máxima de suportar no mínimo 7.000 (sete mil) clientes conectados à rede WiFi.

3) O equipamento deve ser entregue com capacidade inicial para gerenciar e controlar, no mínimo e simultaneamente, 12 (doze) equipamentosdostipos“Ponto de Acesso WiFi” descritos neste Termo de Referência.

4) O equipamento deve permitir o crescimento modular da sua capacidade através de um “Pacote de Expansão para Controlador WiFi” (de hardware e/ou software) de forma a aumentar gradativamente o número de pontos de acesso WiFi controlados até a capacidade máxima do equipamento.

5) O equipamento deverá suportar alta disponibilidade através de equipamento redundante.

6) No caso de falha de um equipamento controlador WiFi “ativo”, todos os pontos de acesso WiFi associados e controlados pelo mesmo deverão suportar associação de forma automática ao equipamento controlador WiFi “redundante” e passar a ser controlados por este. O controlador WiFi “redundante” poderá estar fisicamente em outro local ou em uma rede IP diferente do controlador WiFi “Ativo”.

7) Cada equipamento deve possuir, no mínimo, capacidade para 08 (oito) interfaces Gigabit Ethernet UTP RJ-45 de 1Gbps, fixas ou do tipo que utilize módulos SFP (smallform-factorpluggable).

8) Caso as interfaces sejam do tipo SFP (smallform-factorpluggable),deverão ser fornecidas, no mínimo, 08 (oito) interfaces 1000Base-T de 1Gbps, full-duplex, UTP RJ-45, operacionais e não compartilhadas com outras interfaces

do equipamento, por chassis controlador WiFi.

9) Possuir, para redundância, no mínimo, 2 (duas) fontes de alimentação de energia, com seleção automática de tensão (100-240 VAC) 60Hz. Deverão ser fornecidos os cabos de alimentação.

10) Permitir a troca de fonte de alimentação sem que seja necessária a parada do equipamento.

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

12) Possuir LEDs para a indicação no mínimo do estado de operação e atividade das portas.

13) Permitir ser montado em rack padrão de 19 (dezenove) polegadas, incluindo o fornecimento de todos os acessórios necessários para fixação.

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

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

16) O controlador WiFi deve ser capaz de controlar pontos de acesso WiFi do tipo indoor (uso futuro) e outdoor, simultaneamente, nos padrões 802.11a, 802.11b/g e 802.11n.

17) O controlador WiFi deve ser capaz de controlar pontos de acesso WiFi operando em modo mesh e ponto local (não-mesh), simultaneamente, nos padrões 802.11a, 802.11b/g e 802.11n.

18) O controlador WiFi deve ser capaz de operar em modo de “tráfego centralizado” (mesh) e de “chaveamento de tráfego local” (não-mesh), simultaneamente, nos padrões 802.11a, 802.11b/g e 802.11n.

19) No modo de operação de “tráfego centralizado” (mesh), o tráfego de dados gerado pelos usuários associados aos pontos de acesso WiFi deve passar através do controlador WiFi (“ativo” ou “redundante”). O tráfego de controle dos pontos de acesso WiFi deve ser enviado para o controlador WiFi.

20) Deve ser capaz de, no futuro, operar de modo a controlar pontos de acesso do mesmo fabricante operando em “chaveamento de tráfego local” (não-mesh).

21) No modo de operação de “chaveamento de tráfego local” (não-mesh), deve permitir a configuração de pontos de acesso WiFi de forma que os mesmos realizem o chaveamento (switching) local do tráfego de dados gerado pelos usuários a eles associados, evitando que o tráfego de dados destes usuários passem através do controlador WiFi (“ativo” ou “redundante”). O tráfego de controle dos pontos de acesso WiFi deve ser enviado para o controlador WiFi.

22) Operando no modo de “chaveamento de tráfego local” (não-mesh), o controlador WiFi deve:

- No caso de falha na comunicação lógica entre os pontos de acesso WiFi da localidade com o controlador WiFi, ou com o Sistema de Autenticação Centralizado dos usuários, ou em caso de falha no link WAN (ou LAN) que realize a conexão lógica dos pontos de acesso WiFi com o controlador WiFi, os usuários já associados aos pontos de acesso da localidade devem continuar a ter acesso à rede local. Também deve ser possível fazer com que novos usuários se autentiquem se associem de forma alternativa à rede local sem qualquer prejuízo de acesso local. Os usuários também devem continuar realizando roaming entre os pontos de acesso WiFi locais.

- A rede WiFi local não pode se tornar inoperante devido a ocorrência de qualquer uma das 03 (três) falhas isoladas ou simultâneas apresentadas anteriormente: falha no controlador WiFi, falha no Sistema de Autenticação Centralizado ou falha no link de comunicação entre os pontos de acesso e o controlador (WAN ou LAN).

- Caso a solução proposta não atenda os itens anteriores, a CONTRATADA deverá fornecer uma solução alternativa de redundância e autenticação para pontos de acesso operando com “chaveamento de tráfego local”. A solução alternativa deverá ter capacidade de controlar, no mínimo e simultaneamente, 12 (doze) pontos de acesso do mesmo fabricante operando com “chaveamento de tráfego local” e seus custos deverão ser inseridos no Item “Controlador WiFi” (Item 1).

23) O controlador WiFi deve possuir pelo menos uma porta de console local para gerenciamento.

24) O controlador WiFi deve ajustar automaticamente os canais 802.11 para a otimizar a cobertura de rede e mudar as condições de RF baseado em performance.

25) Possibilitar a implementação de criptografia do tráfego de dados e controle, na comunicação entre Pontos de acesso e Controlador WiFi.

26) Implementar WEP (WiredEquivalentPrivacy), chaves estáticas e dinâmicas (40 bits e 128 bits).

27) Implementar WPA (Wi-Fi Protected Access com algoritmo de criptografia TKIP).

28) Implementar WPA-2 (Wi-Fi Protected Access com algoritmo de criptografia AES).

29) Possuir suporte a autenticação IEEE 802.1X, com pelo menos os seguintes métodos:

- EAP-FAST;
- EAP-TLS;
- PEAPv0/EAP-MSCHAPv2;
- PEAPv1/EAP-GTC.

30) Possuir suporte a 802.1x e Change of Authorization (RFC3573) da solução "Centralizada de Autenticação para Usuários" para troca de VLAN e comunicação do estado das interfaces quando estas ficam "up" ou "down".

31) Possuir segurança IEEE 802.11i.

32) Suportar a criptografia centralizada com os seguintes protocolos: AES-CCMP, TKIP e WEP.

33) Deve implementar mecanismo de autenticação através de portal Web para os usuários visitantes ou temporários, de forma integrada com o Item “Solução Centralizada de Autenticação para Usuários” descrito neste Termo de Referência.

34) Estes usuários autenticados através do portal Web devem se autenticar e ser desviados para segmentos específicos da rede LAN (VLANs).

35) O controlador WiFi deve permitir a criação de um usuário especial para gerenciamento de usuários visitantes ou temporários.

36) Deve implementar o bloqueio da comunicação entre usuários em um mesmo SSID permitindo o isolamento dos usuários.

37) Deve ser fornecido com recursos e licenças instaladas para implementar mecanismo de detecção, localização e contenção de pontos de acesso invasor do tipo “Rogue AP”.

38) Deve ser fornecido com recursos e licenças instaladas para implementar mecanismo de detecção, localização e contenção de clientes invasores do tipo “Clientes Rogue”.

39) Deve ser fornecido com recursos e licenças instaladas para implementar mecanismo de detecção, localização e contenção de “Redes Ad-Hoc”.

40) Deve ser fornecido com recursos e licenças instaladas para implementar detecção de ataques “Denialof Service (DoS)” no mínimo dos seguintes tipos:

- “Associationfloodorstorm”;

- “Authenticationfloodorstorm”;
- “EAPOL Start”;
- “EAPOL Logoff”;
- “Deauthenticationfloodorstorm”;
- “Disassociationfloodorstorm”.

41) Deve ser fornecido com recursos e licenças instaladas para implementar detecção de ataques “Security PenetrationAttacks” no mínimo dos seguintes tipos:

- Detecção de “NetStumbler”;
- Detecção de “Wellenreiter”;
- Detecção de “FakeAPs”.

42) Deve implementar detecção de interferência e reajuste dos parâmetros de RF evitando problemas de cobertura e performance.

43) Deve implementar balanceamento de carga de usuários de modo automático através de múltiplos pontos de acesso para otimizar a performance durante elevada utilização da rede.

44) Deve possuir recursos instalados para implementar mecanismos automáticos de gerenciamento de recursos de rádio, detectando áreas sem cobertura, indisponibilidades de pontos de acesso, e executando auto configuração, auto-correção e auto-otimização.

45) No modo de operação de “mesh”, deve possuir recursos instalados para implementar mecanismo que ajusta dinamicamente o caminho de “Rádio Frequência” através dos quais os pontos de acesso WiFi se conectarão entre si, incluindo a readequação destes caminhos em caso de falha em um ponto de acesso WiFi que faça parte da topologia “mesh”.

46) Deve possuir recursos instalados para implementar mecanismo que no evento de falha de um ponto de acesso WiFi, o controlador WiFi ajuste automaticamente a potência dos pontos de acesso adjacentes para realizar a cobertura da área onde o ponto de acesso WiFi que falhou estava provendo o sinal.

47) Deve possuir recursos instalados para implementar mecanismo que ajusta dinamicamente a saída de potência dos pontos de acesso individualmente para acomodar as condições de alterações da rede, garantindo a performance e escalabilidade.

48) Ajustar, dinamicamente, o nível de potência e canal dos rádios dos pontos de acesso WiFi de modo a otimizar o tamanho da célula de RF, garantido a performance e escalabilidade.

49) Permitir a realização de “roaming” dos usuários entre pontos de acesso WiFi distintos que atendam a uma mesma localidade.

Item 2.Serviço de Instalação do Item 1

São de responsabilidade da contratada para a execução dos Serviços de Instalação, a instalação física e a configuração lógica do equipamento conforme os requisitos, localidades e condições descritas no item “2.3)Serviços de Instalação” deste documento.

Item 3.Serviço de Manutenção e Suporte do Item 1

1) Os serviços de Suporte e Manutenção do equipamento deverão ser em regime de 24x7x4 (24 horas x 7 dias da semana com prazo para inicio da resolução do problema até 04 horas subseqüentes à abertura do chamado técnico) pelo prazo mínimo de 12 (doze) meses que deverá ser considerado na planilha de preços como valor unitário por unidade de equipamento.

2) A CONTRATANTE poderá abrir chamados de manutenção diretamente no Fabricante do Item sem necessidade de prévia consulta e/ou qualquer liberação por parte da CONTRATADA.

3) Deverá ser garantido à CONTRATANTE o pleno acesso ao site do Fabricante dos equipamentos e softwares. Esse acesso deve permitir consultas a quaisquer bases de dados disponíveis para usuários relacionadas aos equipamentos e softwares especificados, além de permitir downloads de quaisquer atualizações de software ou documentação deste produto.

Item 4.Controlador WiFi Redundante

1) Fornecimento de Controlador WiFi 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.

2) O modelo ofertado deve ser do mesmo fabricante do Item “Controlador WiFi” descrito neste Termo de Referência.

3) O equipamento deve ter capacidade máxima de gerenciar simultaneamente pelo menos 500 (quinhentos) equipamentos dos tipos“Ponto de Acesso WiFi” descritos neste Termo de Referência. Deve ter capacidade máxima de suportar, no mínimo, 7.000 (sete mil) clientes conectados à rede WiFi.

4) O equipamento deverá suportar alta disponibilidade.Caso necessário, o equipamento deverá ser fornecido com o licenciamento para a mesma quantidade de Pontos de Acesso WiFi do equipamento ativo, bem como permitir o crescimento modular de sua capacidade através de um “Pacote de Expansão para Controlador WiFi”.

5) No caso de falha de um equipamento controlador WiFi “ativo”, todos os pontos de acesso WiFi associados e controlados pelo mesmo deverão suportar associação de forma automática ao equipamento controlador WiFi “redundante” e passar a ser controlados por este. O controlador WiFi “redundante” poderá estar fisicamente em outro local ou em uma rede IP diferente do controlador WiFi “Ativo”.

6) Cada equipamento deve possuir, no mínimo, capacidade para 08 (oito) interfaces Gigabit Ethernet UTP RJ-45 de 1Gbps, fixas ou do tipo que utilize módulos SFP (smallform-factorpluggable).

7) Caso as interfaces sejam do tipo SFP (smallform-factorpluggable),deverão ser fornecidas, no mínimo, 08 (oito) interfaces 1000Base-T de 1Gbps, full-duplex, UTP RJ-45, operacionais e não compartilhadas com outras interfaces do equipamento, por chassis controlador WiFi.

8) Possuir, para redundância, no mínimo, 2 (duas) fontes de alimentação de energia, com seleção automática de tensão (100-240 VAC) 60Hz. Deverão ser fornecidos os cabos de alimentação.

9) Permitir a troca de fonte de alimentação sem que seja necessária a parada do equipamento.

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

11) Possuir LEDs para a indicação no mínimo do estado de operação e atividade das portas.

12) Permitir ser montado em rack padrão de 19 (dezenove) polegadas, incluindo o fornecimento de todos os acessórios necessários para fixação.

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

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

15) O controlador WiFi deve ser capaz de controlar pontos de acesso WiFi do

tipo indoor (uso futuro) e outdoor, simultaneamente, nos padrões 802.11a, 802.11b/g e 802.11n.

16) O controlador WiFi deve ser capaz de controlar pontos de acesso WiFi operando em modo mesh e ponto local (não-mesh), simultaneamente, nos padrões 802.11a, 802.11b/g e 802.11n.

17) O controlador WiFi deve ser capaz de operar em modo de "tráfego centralizado" (mesh) e de "chaveamento de tráfego local" (não-mesh), simultaneamente, nos padrões 802.11a, 802.11b/g e 802.11n.

18) No modo de operação de "tráfego centralizado" (mesh), o tráfego de dados gerado pelos usuários associados aos pontos de acesso WiFi deve passar através do controlador WiFi ("ativo" ou "redundante"). O tráfego de controle dos pontos de acesso WiFi deve ser enviado para o controlador WiFi.

19) Deve ser capaz de, no futuro, operar de modo a controlar pontos de acesso do mesmo fabricante operando em "chaveamento de tráfego local" (não-mesh).

20) No modo de operação de "chaveamento de tráfego local" (não-mesh), deve permitir a configuração de pontos de acesso WiFi de forma que os mesmos realizem o chaveamento (switching) local do tráfego de dados gerado pelos usuários a eles associados, evitando que o tráfego de dados destes usuários passem através do controlador WiFi ("ativo" ou "redundante"). O tráfego de controle dos pontos de acesso WiFi deve ser enviado para o controlador WiFi.

21) Operando no modo de "chaveamento de tráfego local" (não-mesh), o controlador WiFi deve:

- No caso de falha na comunicação lógica entre os pontos de acesso WiFi da localidade com o controlador WiFi, ou com o Sistema de Autenticação Centralizado dos usuários, ou em caso de falha no link WAN (ou LAN) que realize a conexão lógica dos pontos de acesso WiFi com o controlador WiFi, os usuários já associados aos pontos de acesso da localidade devem continuar a ter acesso à rede local. Também deve ser possível fazer com que novos usuários se autentiquem se associem de forma alternativa à rede local sem qualquer prejuízo de acesso local. Os usuários também devem continuar realizando roaming entre os pontos de acesso WiFi locais.

- A rede WiFi local não pode se tornar inoperante devido a ocorrência de qualquer uma das 03 (três) falhas isoladas ou simultâneas apresentadas anteriormente: falha no controlador WiFi, falha no Sistema de Autenticação Centralizado ou falha no link de comunicação entre os pontos de acesso e o controlador (WAN ou LAN).

- Caso a solução proposta não atenda aos itens anteriores, a CONTRATADA deverá fornecer uma solução alternativa de

redundância e autenticação para pontos de acesso operando com “chaveamento de tráfego local”. A solução alternativa deverá ter capacidade de controlar, no mínimo e simultaneamente, 12 (doze) pontos de acesso do mesmo fabricante operando com “chaveamento de tráfego local” e seus custos deverão ser inseridos no Item “Controlador WiFi” (Item 1).

22) O controlador WiFi deve possuir pelo menos uma porta de console local para gerenciamento.

23) O controlador WiFi deve ajustar automaticamente os canais 802.11 para a otimizar a cobertura de rede e mudar as condições de RF baseado em performance.

24) Possibilitar a implementação de criptografia do tráfego de dados e controle, na comunicação entre Pontos de acesso e Controlador WiFi.

25) Implementar WEP (WiredEquivalentPrivacy), chaves estáticas e dinâmicas (40 bits e 128 bits).

26) Implementar WPA (Wi-Fi Protected Access com algoritmo de criptografia TKIP).

27) Implementar WPA-2 (Wi-Fi Protected Access com algoritmo de criptografia AES).

28) Possuir suporte a autenticação IEEE 802.1X, com pelo menos os seguintes métodos:

- EAP-FAST;
- EAP-TLS;
- PEAPv0/EAP-MSCHAPv2;
- PEAPv1/EAP-GTC.

29) Possuir suporte a 802.1x e Change of Authorization (RFC3573) da solução "Centralizada de Autenticação para Usuários" para troca de VLAN e comunicação do estado das interfaces quando estas ficam "up" ou "down".

30) Possuir segurança IEEE 802.11i.

31) Suportar a criptografia centralizada com os seguintes protocolos: AES-CCMP, TKIP e WEP.

32) Deve implementar mecanismo de autenticação através de portal Web para os usuários visitantes ou temporários, de forma integrada com o Item “Solução Centralizada de Autenticação para Usuários” descrito neste Termo de Referência.

33) Estes usuários autenticados através do portal Web devem se autenticar e ser desviados para segmentos específicos da rede LAN (VLANs).

34) O controlador WiFi deve permitir a criação de um usuário especial para gerenciamento de usuários visitantes ou temporários.

35) Deve implementar o bloqueio da comunicação entre usuários em um mesmo SSID permitindo o isolamento dos usuários.

36) Deve suportar mecanismo de detecção, localização e contenção de pontos de acesso invasor do tipo “Rogue AP”.

37) Deve suportar mecanismo de detecção, localização e contenção de clientes invasores do tipo “Clientes Rogue”.

38) Deve suportar mecanismo de detecção, localização e contenção de “Redes Ad-Hoc”.

39) Deve suportar detecção de ataques “Denialof Service (DoS)” no mínimo dos seguintes tipos:

- “Associationfloodorstorm”;
- “Authenticationfloodorstorm”;
- “EAPOL Start”;
- “EAPOL Logoff”;
- “Deauthenticationfloodorstorm”;
- “Disassociationfloodorstorm”.

40) Deve suportar detecção de ataques “Security PenetrationAttacks” no mínimo dos seguintes tipos:

- Detecção de “NetStumbler”;
- Detecção de “Wellenreiter”;
- Detecção de “FakeAPs”.

41) Deve implementar detecção de interferência e reajuste dos parâmetros de RF evitando problemas de cobertura e performance.

42) Deve implementar balanceamento de carga de usuários de modo automático através de múltiplos pontos de acesso para otimizar a performance durante elevada utilização da rede.

43) Deve possuir recursos instalados para implementar mecanismos automáticos de gerenciamento de recursos de rádio, detectando áreas sem cobertura, indisponibilidades de pontos de acesso, e executando auto configuração, auto-correção e auto-otimização.

44) No modo de operação de “mesh”, deve possuir recursos instalados para implementar mecanismo que ajusta dinamicamente o caminho de “Rádio Frequência” através dos quais os pontos de acesso WiFi se conectarão entre si, incluindo a readequação destes caminhos em caso de falha em um ponto de acesso WiFi que faça parte da topologia “mesh”.

45) Deve possuir recursos instalados para implementar mecanismo que no evento de falha de um ponto de acesso WiFi, o controlador WiFi ajuste automaticamente a potência dos pontos de acesso adjacentes para realizar a cobertura da área onde o ponto de acesso WiFi que falhou estava provendo o sinal.

46) Deve possuir recursos instalados para implementar mecanismo que ajusta dinamicamente a saída de potência dos pontos de acesso individualmente para acomodar as condições de alterações da rede, garantindo a performance e escalabilidade.

47) Ajustar, dinamicamente, o nível de potência e canal dos rádios dos pontos de acesso WiFi de modo a otimizar o tamanho da célula de RF, garantido a performance e escalabilidade.

48) Permitir a realização de “roaming” dos usuários entre pontos de acesso WiFi distintos que atendam a uma mesma localidade.

Item 5.<u>Serviço de Instalação do Item 4</u>

São de responsabilidade da contratada para a execução dos Serviços de Instalação, a instalação física e a configuração lógica do equipamento conforme os requisitos, localidades e condições descritas no item “2.3)Serviços de Instalação”deste documento.

Item 6.<u>Serviço de Manutenção e Suporte do Item 4</u>

1) Os serviços de Suporte e Manutenção do equipamento deverão ser em regime de 24x7x4 (24 horas x 7 dias da semana com prazo para inicio da resolução do problema até 04 horas subseqüentes à abertura do chamado técnico) pelo prazo mínimo de 12 (doze) meses que deverá ser considerado na planilha de preços como valor unitário por unidade de equipamento;

2) A CONTRATANTE poderá abrir chamados de manutenção diretamente no Fabricante do Item sem necessidade de prévia consulta e/ou qualquer liberação por parte da CONTRATADA.

3) Deverá ser garantido à CONTRATANTE o pleno acesso ao site do Fabricante dos equipamentos e softwares. Esse acesso deve permitir consultas a quaisquer bases de dados disponíveis para usuários relacionadas aos equipamentos e softwares especificados, além de permitir downloads de quaisquer atualizações de software ou documentação deste produto.

Item 7.Pacote de Expansão para Controlador WiFi

1) Fornecimento de um Pacote de Expansão para Controlador 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.

2) O modelo ofertado deve ser do mesmo fabricante do Item "Controlador WiFi" (Item 1),descrito neste Termo de Referência.

3) O Pacote de Expansão deve ser totalmente compatível com o "Controlador WiFi descrito neste documento. Pode ser oferecido em forma de hardware ou licença de software.

4) Deve, operando em conjunto com o controlador WiFi, atender a todas características, especificações e requisitos descritas no Item "Controlador WiFi".

5) Permitir a expansão da capacidade do Item "Controlador WiFi" em gerenciar e controlar 25 (Vinte e cinco) equipamentos dos tipos "Ponto de Acesso WiFi" adicionais descritos neste Termo de Referência.

6) Ser acompanhado de todos os acessórios necessários para operacionalização da expansão, tais como: licenças de softwares, documentação técnica e manuais que contenham informações suficientes para possibilitar a instalação, configuração e operacionalização do módulo de expansão.

Item 8.Serviço de Instalação do Item 7

São de responsabilidade da contratada para a execução dos Serviços de Instalação, a instalação física e a configuração lógica do pacote de expansão conforme os requisitos, localidades e condições descritas no item "2.3)Serviços de Instalação"deste documento.

Item 9.Serviço de Manutenção e Suporte do Item 7

1) Os serviços de Suporte e Manutenção do equipamento deverão ser em regime de 24x7x4 (24 horas x 7 dias da semana com prazo para inicio da resolução do problema até 04 horas subseqüentes à abertura do chamado técnico) pelo prazo mínimo de 36 (trinta e seis) meses que deverá ser considerado na planilha de preços como valor unitário por unidade de equipamento.

2) A CONTRATANTE poderá abrir chamados de manutenção diretamente no

Fabricante do Item sem necessidade de prévia consulta e/ou qualquer liberação por parte da CONTRATADA.

3) Deverá ser garantido à CONTRATANTE o pleno acesso ao site do Fabricante dos equipamentos e softwares. Esse acesso deve permitir consultas a quaisquer bases de dados disponíveis para usuários relacionadas aos equipamentos e softwares especificados, além de permitir downloads de quaisquer atualizações de software ou documentação deste produto.

Item 10. Software de Gerenciamento da Rede WiFi

1) Fornecimento de Software de Gerenciamento de Rede WiFi capaz de gerenciar o Item "Controlador WiFi" e os itens "Ponto de Acesso WiFi Internos" e "Ponto de Acesso WiFi Externos" descritos neste Termo de Referência.

2) O modelo ofertado deverá estar em linha de produção, sem previsão de encerramento, na data de entrega da proposta.

3) O modelo ofertado deve ser do mesmo fabricante do Item "Controlador WiFi" (Item 1) descrito neste Termo de Referência.

4) O software deve ter capacidade máxima de gerenciar simultaneamente pelo menos 10.000 (dez mil) equipamentos dos tipos "Ponto de Acesso WiFi" descritos neste Termo de Referência.

5) O software deve ser entregue com capacidade inicial para gerenciar, no mínimo e simultaneamente, um total de 50 (cinqüenta) equipamentos que formam a solução: equipamentos dos tipos "Ponto de Acesso WiFi Externos", "Ponto de Acesso WiFi Internos", "Controladores WiFi" e outros descritos neste Termo de Referência.

6) O software deve permitir o crescimento modular da sua capacidade através de um "Pacote de Expansão para software de gerenciamento da Rede WiFi" (software ou licença de software) de forma a aumentar gradativamente o número de pontos de acesso WiFi controlados e gerenciados até a capacidade máxima do software de gerenciamento.

7) Deve ser capaz de gerenciar pontos de acesso WiFi operando em modo mesh e ponto local (não-mesh), simultaneamente, nos padrões 802.11a, 802.11b/g e 802.11n.

8) Deve possuir capacidade de gerenciamento hierárquico com possibilidade de definição de grupos de equipamentos e alteração das características de configuração do Grupo sem a necessidade de configuração individual de cada equipamento.

9) O software de gerência deve ser acessado através de qualquer browser via HTTP ou HTTPS, permitindo o acesso à plataforma de gerência a qualquer

momento de qualquer local.

10) Deve suportar alta disponibilidade, ativo/standby, trabalhando com no mínimo dois servidores físicos.

11) Deve permitir ao administrador importar a planta dos andares e assinalar as características de RF dos Pontos de acesso aumentando a precisão do projeto.

12) Permitir a organização hierárquica de equipamentos em plantas, de plantas em prédios e de prédios em projetos.

13) Possuir descoberta automática dos dispositivos individuais da infraestrutura wireless.

14) Visualização do mapa lógico da rede, com a representação gráfica dos equipamentos e sinalização por cor de seu estado operacional.

15) Visualização de alertas da rede em tempo real, com indicação de severidade por cor, para pontos de acesso WiFi operando em modo mesh e ponto local (não-mesh), de forma simultânea.

16) Visualização de alertas da rede em tempo real, com indicação de severidade por cor, para os controladores WiFi.

17) Possuir ferramentas para permitir ao administrador visualizar em um único console o layout da rede WiFi e monitorar o desempenho desta rede - incluindo mapa detalhado que exibe a cobertura de RF sobre os mapas com layout real dos andares.

18) Deve permitir o rastreamento em tempo real dos dispositivos móveis conectados na infraestrutura da rede WiFi.

19) Deve possibilitar a visualização rápida de eventuais buracos de cobertura de RF, alarmes e estatísticas de utilização para fácil e rápido monitoramento e troubleshooting.

20) Possuir ferramentas integradas para prever os requerimentos de RF para projeto da rede WiFi, incluindo qual o melhor local para os pontos de acesso na planta do prédio/andar, configuração e estimar o desempenho e a cobertura.

21) Deve possuir mecanismos para consolidar informações de rede, tais como: níveis de ruído, relação sinal/ruído, interferência, potência de sinal e topologia de rede, permitindo ao administrador isolar e resolver problemas nos vários níveis da rede.

22) Possuir capacidade de listagem on-line da relação sinal-ruído de cada usuário, sua localização (tracking), endereço IP, endereço MAC, nível de potência de recepção e dados de associação e de autenticação 802.1x.

23) Capacidade de identificação e listagem dos rádios vizinhos e respectivos SSID/BSSID que podem ser percebidos por cada ponto de acesso.

24) Deve ser possível configurar alarmes automáticos caso o índice relacionado ao alarme ultrapasse um determinado limiar.

25) Deve fornecer gráficos com análise espectral realtime. Caso o software de gerenciamento não possua esta capacidade, deverá ser fornecido software adicional para que este item seja atendido.

26) Implementar monitoração das inferências não WiFi (telefones sem fio, dispositivos Bluetooth, câmeras sem fio, etc), com classificação das fontes de interferência.

27) Deve correlacionar alarmes de dois ou mais pontos de acesso WiFi sobre a mesma fonte de interferência e reportar ao administrador como um só dispositivo.

28) Permitir que sejam configurados pelo menos 8 grupos diferentes de usuários e administradores, com níveis de privilégios de acesso e configuração distintos.

29) Deve permitir a criação de “Domínios Virtuais” para os administradores da rede que contenham, no mínimo, equipamentos. Deve ser possível que determinados usuários e administradores sejam associados a estes “Domínios Virtuais” de forma que apenas tenham acesso ao gerenciamento e visualização dos elementos pertencentes ao “Domínio Virtual”.

30) Permitir a atualização de software dos pontos de acesso de modo centralizado via interface web.

31) Deve descobrir automaticamente os equipamentos individuais na infraestrutura de rede WiFi, eliminando a necessidade de configuração e manutenção, e provendo informação para fins de planejamento da capacidade e troubleshooting.

32) Possuir suporte para gerenciamento de falhas via SNMP (Simple Network Management Protocol) versão 3 (além do SNMP versão 2 e 1) para gerenciamento seguro entre a plataforma de gerenciamento e os Controladores WiFi.

33) Implementar modelos de configuração (templates) de forma a possibilitar a replicação de configuração entre equipamentos.

34) Possuir capacidade de gerência de configuração com armazenamento de diferentes versões e suporte a "rollback”.

35) Possuir a capacidade de gerar alarmes se um ataque for detectado.

36) Implementar a detecção, localização e contenção de Rogue APs e AD-

HOC networks.

37) Implementar a detecção de clientes autorizados conectados a pontos de acesso não autorizados (Rogue APs) e de clientes não autorizados em pontos de acesso oficiais (clientes Rogues).

38) Implementar assinaturas de ataques de RF e prevenção de intrusão para ajudar ao administrador a detectar rapidamente ataques de RF "Denialof Service (DoS)" no mínimo dos seguintes tipos: "Associationfloodorstorm"; "Authenticationfloodorstorm"; "EAPOL Start"; "EAPOL Logoff"; "Deauthenticationfloodorstorm" e "Disassociationfloodorstorm".

39) Deve ser fornecido com recursos e licenças instaladas para implementar detecção de ataques "Security PenetrationAttacks" no mínimo dos seguintes tipos: detecção de "NetStumbler"; detecção de "Wellenreiter" e detecção de "FakeAPs".

40) Deve fornecer a capacidade de geração de relatórios customizáveis para os administradores de rede.

41) Deve fornecer no mínimo, os seguintes tipos de relatórios: listagem de clientes wireless, inventário da rede wireless, informações de configuração dos controladores WiFi e dos pontos de acesso, utilização da rede wireless e da rádio frequência.

42) Deve suportar a geração de relatórios para Auditoria de Rede (ou "ComplianceReports"). No mínimo deve ser gerado e entregue relatório no padrão "PCI Data Security Standard (DSS)" versão 1.1 apresentando informações de segurança importantes sobre a rede WiFi.

43) Deve suportar a geração de relatórios contendo ameaças de segurança recorrentes antes que estes causem danos para a infraestrutura wireless e de LAN. Deve fornecer geração de relatórios de segurança, como por exemplo, pontos de acesso estranhos detectados na rede (Rogue AP e Adhoc Rogue).

44) Suporte a criação e aplicação de políticas que permitam ao administrador gerir/criar: VLAN, RF, qualidade de serviço (QoS) e política de segurança, SSIDs múltiplos e únicos com parâmetros individuais de segurança.

45) Deve implementar ferramentas de troubleshooting de clientes com dificuldade de se conectarem à rede WiFi.

46) Deve ser capaz de, no mínimo, monitorar o funcionamento de switches de rede no software de gerenciamento.

47) As informações de toda a rede – tais como alarmes gerais, alarmes de wireless IPS, interferências de RF, localização de pontos de acesso rogues e clientes rogue, localização de usuários, monitoração de switches de rede - devem ser apresentadas em um console único e não devem ser separadas em consoles distintos.

48) O software e a documentação (manuais) deverão ser fornecidos em CD/DVD ou ser disponibilizada senha para que seja realizado o “download” da página Internet do fabricante. Devem conter informações suficientes para possibilitar a instalação, configuração e operacionalização do software.

49) Deve ser fornecido em forma de appliance virtual (solução que permite ser instalado diretamente na plataforma de virtualização sem a necessidade de sistema operacional adicional)ou instalável na forma virtualizada (solução de que permite ser instalado sobre um sistema operacional licenciado e virtualizado).No caso de ser fornecido de forma virtualizada, deverão ser fornecidos os softwares e licenças necessárias para o pleno funcionamento da solução.

Item 11.Serviço de Instalação do Item 10

São de responsabilidade da contratada para a execução dos Serviços de Instalação, a instalação física e a configuração lógica do software conforme os requisitos, localidades e condições descritas no item “2.3)Serviços de Instalação” deste documento.

Item 12.Serviço de Manutenção e Suporte do Item 10

1) Os serviços de Suporte e Manutenção do equipamento deverão ser em regime de 24x7x4 (24 horas x 7 dias da semana com prazo para inicio da resolução do problema até 04 horas subseqüentes à abertura do chamado técnico) pelo prazo mínimo de 12 (doze) meses que deverá ser considerado na planilha de preços como valor unitário por unidade de equipamento.

2) A CONTRATANTE poderá abrir chamados de manutenção diretamente no Fabricante do Item sem necessidade de prévia consulta e/ou qualquer liberação por parte da CONTRATADA.

3) Deverá ser garantido à CONTRATANTE o pleno acesso ao site do Fabricante dos equipamentos e softwares. Esse acesso deve permitir consultas a quaisquer bases de dados disponíveis para usuários relacionadas aos equipamentos e softwares especificados, além de permitir downloads de quaisquer atualizações de software ou documentação deste produto.

Item 13.Pacote de Expansão para software de gerenciamento da Rede WIFI

1) Fornecimento de Pacote de Expansão para aumento de capacidade do Item “Software de Gerenciamento da Rede WiFi” (Item 10).

2) O modelo ofertado deverá estar em linha de produção, sem previsão de encerramento, na data de entrega da proposta.

3) Deve ser totalmente compatível com o Item “Software de gerenciamento da Rede WiFi” de forma a aumentar gradativamente o número de pontos de acesso WiFi controlados e gerenciados até a capacidade máxima do software de gerenciamento.

4) Deve, operando em conjunto com o “Software de gerenciamento da Rede WiFi”, atender a todas características, especificações e requisitos descritas no Item “Software de gerenciamento da Rede WiFi”.

5) Permitir a expansão da capacidade do Item “Software de gerenciamento para Rede WiFi” em gerenciar 25 (vinte e cinco) equipamentos adicionais que formam a solução: equipamentos dos tipos “Ponto de Acesso WiFi”, “Controladores WiFi” e outros descritos neste Termo de Referência.

6) O pacote de expansão e a documentação (manuais) deverão ser fornecidos em CD/DVD ou ser disponibilizada senha para que seja realizado o “download” da página Internet do fabricante. Devem conter informações suficientes para possibilitar a instalação, configuração e operacionalização do módulo de expansão.

Item 14. Serviço de Instalação do Item 13

São de responsabilidade da contratada para a execução dos Serviços de Instalação, a instalação física e a configuração lógica do pacote de expansão conforme os requisitos, localidades e condições descritas no item “2.3)Serviços de Instalação”deste documento.

Item 15. Serviço de Manutenção e Suporte do Item 13

1) Os serviços de Suporte e Manutenção do equipamento deverão ser em regime de 24x7x4 (24 horas x 7 dias da semana com prazo para inicio da resolução do problema até 04 horas subseqüentes à abertura do chamado técnico) pelo prazo mínimo de 12 (doze) meses que deverá ser considerado na planilha de preços como valor unitário por unidade de equipamento.

2) A CONTRATANTE poderá abrir chamados de manutenção diretamente no Fabricante do Item sem necessidade de prévia consulta e/ou qualquer liberação por parte da CONTRATADA.

3) Deverá ser garantido à CONTRATANTE o pleno acesso ao site do Fabricante dos equipamentos e softwares. Esse acesso deve permitir consultas a quaisquer bases de dados disponíveis para usuários relacionadas aos equipamentos e softwares especificados, além de permitir downloads de quaisquer atualizações de software ou documentação deste produto.

Item 16.Ponto de Acesso WiFi Interno

1) Fornecimento de Ponto de Acesso WiFi Interno, 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.

2) O modelo ofertado deve ser do mesmo fabricante do Item “Controlador WiFi” descrito neste Termo de Referência.

3) Equipamento de Ponto de Acesso (Access Point) para rede local sem fio

(Sem fio LAN) atendendo aos padrões IEEE 802.11a, 802.11b, 802.11g e 802.11n, com configuração via software.

4) Deve implementar funcionamento em modo gerenciável por "Controlador WiFi", para configuração de seus parâmetros sem fio, gerenciamento das políticas de segurança, QoS e monitoramento de RF(rádio frequência).

5) O ponto de acesso poderá estar diretamente ou remotamente conectado ao Módulo de Controle de Rede sem fio, inclusive via roteamento nível 3 da camada OSI.

6) Implementar Protocolo de comunicação CAPWAP.

7) Caso ocorra a falha de um "Controlador WiFi", os Pontos de Acesso relacionados deverão se associar automaticamente a outro "Controlador WiFi", podendo se escolher a prioridade de um determinado ponto de acesso sobre outro, a fim de selecionar quais pontos de acesso devem permanecer em funcionamento na ocasião de falha de múltiplos Módulos de Controle.

8) Deve permitir simultaneamente usuários configurados nos padrões 802.11b, 802.11g, 802.11a e 802.11n, através de rádios independentes (Ponto de Acesso Dual Radio).

9) Implementar as seguintes taxas de transmissão e com fallback automático:

- 802.11 a/g: 54,48,36,24,18,12, 9, e 6 Mbps.
- 802.11 b: 11, 5,5,2 e 1 Mbps.
- 802.11n: 300, 270, 240, 180, 150, 135, 120, 90, 60, 45, 30 e 15 Mbps.

10) Implementar o protocolo de enlace CSMA/CA (Carrier SenseMultiple Access/CollisionAvoidance) para acesso ao meio de transmissão.

11) Operar nas modulações DSSS e OFDM.

12) Possuir capacidade de selecionar automaticamente o canal de transmissão.

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

14) Possuir suporte a pelo menos 16 SSIDs.

15) Permitir habilitar e desabilitar a divulgação do SSID.

16) Implementar mecanismo de minimização do tempo de roaming (deslocamento) de clientes autenticados via 802.1x(FastSecure Roaming) entre dois Pontos de Acesso no mesmo segmento de rede ou em segmentos de rede distintos. A reassociação de um cliente de um Ponto de Acesso para outro deve

ser inferior a 100 ms (milissegundos).

17) Implementar padrão IEEE 802.11e (WMM – Wi-fiMultimedia) para priorização de tráfego, suportando aplicações em tempo real, tais como, VoIP, WebCasting, videoconferência, dentre outras.

18) Possibilitar controlar as respostas de requisições Wi-Fi com a finalidade de selecionar faixas de frequências diferentes (2.4Ghz e 5Ghz) para que clientes Wi-Fi se associem ao Ponto de Acesso a faixa de frequência menos congestionada.

19) Implementar em conjunto com o "Controlador WiFi" a capacidade de usar sinais de recepção para ajuste dos múltiplos sinais de transmissão, por usuário, com a finalidade de melhorar a relação sinal ruído (SNR) e taxa de transmissão de clientes que não implementem a tecnologia MIMO (Multiple Inputs Multiple Outputs). Essa funcionalidade não deve exigir o feedback do cliente sem fio.

20) Deve possuir hardware interno dedicado para análise de espectro em 2.4GHz e 5GHz, de alta resolução (melhor que 5MHz), sem que ocorra impacto no tráfego dos clientes.

21) Deve possuir modo de operação de analisador de espectro, acessível remotamente, para análise e captura de dados da condição do espectro quando necessário.

22) Deve detectar interferências WiFi (provenientes de dispositivos 802.11) e detectar e classificar interferências não-WiFi, tais como (Bluetooth, DECT, Câmeras de Vídeo sem fio, Micro-ondas e outros)

23) Deve ter a capacidade de mudar de canal caso seja detectada alguma das interferências listadas acima no canal de operação atual e devem permanecer no novo canal caso a interferência seja persistente.

24) Deve detectar no mínimo 5 (cinco) interferências simultâneas.

25) Deve fazer tanto a transmissão de dados WiFi quanto a análise de espectro simultaneamente, com processamento separado e sem impactar no desempenho da transmissão de dados.

26) Não deve haver licença restringindo o número de usuários por ponto de acesso.

27) Os equipamentos ponto de acesso devem ser homologados pela ANATEL.

28) Deve possibilitar o seu gerenciamento através doSoftware de Gerenciamento da Rede WiFi.

29) Deve permitir associação de clientes em IPv6 com no mínimo os

seguintes requisitos:

- Clientes com endereços IPv6 somente.
- Clientes com endereços IPv4 e IPv6, dual-stack
- Suportar atribuição dinâmica de endereços IPv6 tais como, IPv6 StatelessAutoConfiguration (SLAAC), Stateless DHCPv6, Statefull DHCPv6 e configuração manual de endereços IPv6.
- Permitir, no mínimo, 2 (dois) endereços IPv6 por cliente sem fio.
- Permitir associação de clientes IPv4 e IPv6 no mesmo SSID.
- Permitir roaming transparente sem troca de endereçamento IPv6 para clientes móveis.

30) Requisitos de Irradiação:

- Possuir 04 (quatro) antenas, independentes, compatíveis com os padrões 802.11a/b/g/n com ganho de, no mínimo, 4dBi e padrão de irradiação omnidirecional.
- Possuir antenas dual-mode internas.
- Possuir potência máxima de transmissão de, no mínimo,20dBm(802.11a e 802.11n) e 100mW.

Possuir potência máxima de transmissão de, no mínimo,22dBm(802.11b/g e 802.11n) e 160mW.

- Possuir sensibilidade de recepção de, no mínimo, -92dBm(802.11b), -91dBm(802.11g), –92dBm(802.11a) e -91dBm(802.11n).
- Possuir MIMO 3x4.

31) Requisitos de Rede

- Suportar a pilha de protocolos TCP/IP.
- Implementar Virtual LANs (VLANs) conforme padrão IEEE 802.1q.
- Implementar a criação de, no mínimo, 16 VLANs.
- Possuir, uma interface Gigabit Ethernet 10/100/1000, autosensing, com conector RJ-45, para conexão à rede local fixa.

32) Requisitos de Gerenciamento

- Implementar o protocolo NTP com autenticação entre peers.

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

- Permitir a configuração e gerenciamento através de browser padrão (http, https), SSH, e porta serial.

- Possuir porta de console para gerenciamento e configuração via linha de comando (CLI – comandline interface) com conector RJ-45 ou USB, diferente da porta de rede solicitada anteriormente.

- Permitir a gravação de log externo (syslog).

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

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

- Possuir suporte a MIB II, conforme RFC 1213.

- 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.

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

- O hardware do ponto de acesso deve permitir a conversão de um ponto de acesso autônomo para um ponto de acesso gerenciável e vice-versa.

- Possibilitar a configuração de um ponto de acesso como um “Sniffer” da rede sem fio, com a finalidade de “troubleshooting” de uma determinada região.

33) Facilidades e Acessórios:

- Implementar cliente DHCP, para configuração automática de rede.

- Funcionar em modo plug-and-play, permitindo a sua configuração automática.

- Possuir LED's indicativos do estado de operação e atividade de RF (Rádio Frequência).

- Possibilitar alimentação elétrica local e via padrão Power over Ethernet (802.3af ou 802.3at) através de uma única interface de rede, utilizando a mesma interface de rede já utilizada para comunicação com a rede.

- Suportar fonte de alimentação com seleção automática de tensão (100-240 VAC).

- Não há necessidade de fornecimento da fonte de alimentação para os Access Points.

- Possuir estrutura que permita fixação do equipamento em teto e parede.

- Possuir sistema antifurto embutido na carcaça do ponto de acesso, do tipo Kensington ou similar.

- Deve ser acompanhado de todos os acessórios necessários para operacionalização do equipamento, tais como: softwares, cabos de energia elétrica, estrutura para fixação em paredes e teto, documentação técnica e manuais que contenham informações suficientes para possibilitar a instalação, configuração e operacionalização do equipamento.

34) Requisitos de Segurança

- Implementar varredura de RF nas bandas 802.11a, 802.11b, 802.11g e 802.11n, para a identificação de Pontos de Acesso não autorizados (rogues) e interferências.

- O sistema de monitoração e controle de RF deve possuir mecanismos de detecção/bloqueio de intrusos no ambiente sem fio.

- Permitir o bloqueio de comunicação entre clientes sem fio diretamente (comunicação ad-hoc não é permitida).

- Permitir o bloqueio da configuração do Ponto de Acesso via rede sem fio.

- Implementarvlanguest, para que usuários não autenticados ganhem acesso restrito na condição de visitante.

- Implementar filtros baseado em protocolos e em endereços MAC.

- Implementar IEEE 802.1X, com pelo menos os seguintes métodos EAP:

- EAP-Flexible Authentication via Secure Tunneling (EAP-FAST),
- Protected EAP- Generic Token Card (PEAP-GTC),
- PEAP-Microsoft Challenge Authentication Protocol Version 2 (PEAP-MSCHAPv2),
- EAP-Transport Layer Security (EAP-TLS).

- Integração com Radius Server e Tacacs Server que suporte os métodos EAP citados.

- Possuir suporte a 802.1x e Change of Authorization (RFC3573) da solução "Centralizada de Autenticação para Usuários" para troca de VLAN e comunicação do estado das interfaces quando estas ficam "up" ou "down".

- Implementar associação dinâmica de usuário a VLAN, com base nos parâmetros da etapa de autenticação.

- Implementar protocolo de autenticação para controle do acesso administrativo e auditoria de comandos ao equipamento com mecanismos de AAA (Authentication, Authorization e Accounting).

- Implementar criptografia do tráfego de controle entre Ponto de Acesso e o “Controlador WiFi”.

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

- Implementar WEP (WiredEquivalentPrivacy), chaves estáticas e dinâmicas (40 bits e 128 bits).

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

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

- Implementar o padrão IEEE 802.11i.

- Possibilitar a configuração de um ponto de acesso como um “Sensor wIPS” da rede sem fio, com a finalidade de monitorar ataques à rede Sem fio uma determinada região. O Ponto de Acesso deve permitir ser configurado como sensor em tempo integral e ser configurado como sensor em modo compartilhado com atendimento de tráfego de cliente sem fio.

- Deve ser capaz de realizar o switching local do tráfego gerado entre

os clientes a ele associados, sem a necessidade de conectividade com o Módulo de Controle para o tráfego dos clientes de cada ponto de acesso. Caso haja falha de comunicação com o Módulo de Controle, os clientes associados devem continuar tendo acesso à rede, sem a necessidade de reautenticação.

- Deve ser possível se conectar no Ponto de Acesso para verificação de níveis de sinal, ruído e ocupação do canal, através de um software de análise de RF.

Item 17.Serviço de Instalação do Item 16

São de responsabilidade da contratada para a execução dos Serviços de Instalação, a instalação física e a configuração lógica do equipamento conforme os requisitos, localidades e condições descritas no item "2.3)Serviços de Instalação"deste documento.

Item 18.Serviço de Manutenção e Suporte do Item 16

1) Os serviços de Suporte e Manutenção deste Item deverão ser realizados em regime 8x5xNBD (8 horas x 5 dias da semana com prazo para inicio da resolução do problema até o dia útil subsequente à abertura do chamado técnico) pelo prazo mínimo de 12 (doze) meses que deverá ser considerado na planilha de preços como valor unitário por unidade de equipamento.

2) A CONTRATANTE poderá abrir chamados de manutenção diretamente no Fabricante do Item sem necessidade de prévia consulta e/ou qualquer liberação por parte da CONTRATADA.

3) Deverá ser garantido à CONTRATANTE o pleno acesso ao site do Fabricante dos equipamentos e softwares. Esse acesso deve permitir consultas a quaisquer bases de dados disponíveis para usuários relacionadas aos equipamentos e softwares especificados, além de permitir downloads de quaisquer atualizações de software ou documentação deste produto.

Item 19.Ponto de Acesso WiFi Externo

1) 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.

2) O modelo ofertado deve ser do mesmo fabricante do Item "Controlador WiFi" descrito neste Termo de Referência.

3) Deve ser um equipamento ponto de acesso WiFi, para rede local sem fio, com possibilidade de instalação de antenas externas, 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.

4) Deve ser do tipo outdoor (externo) atendendo no mínimo a norma IP-67.

5) Deve operar em modo “mesh”, com tráfego centralizado no controlador WiFi e possuir capacidade de análise espectral em Rádio Frequência.

6) Deve funcionar em modo gerenciado pela Controladora WiFi para configuração de seus parâmetros, gerenciamento das políticas de segurança, e QoS.

7) Deverá operar logicamente conectado à controladora WiFi, inclusive via roteamento de camada 3 do modelo OSI, seja através de rede de comunicação pública ou rede de comunicação privada.

8) Em caso de falha do controlador WiFi ao qual o ponto de acesso está associado, o ponto de acesso deverá se associar automaticamente a um controlador WiFi redundante, não permitindo que a rede sem fio se torne inoperante por este motivo.

9) O ponto de acesso deve ter capacidade de operar de forma que realize o encaminhamento do tráfego dos usuários através do(s) Controlador(es) WiFi.

10) Deve suportar usuários WiFi configurados nos padrões IEEE 802.11b/g/n e 802.11a/n simultaneamente.

11) Deve operar, no mínimo, com temperaturas de -30 a +55°C (graus Celsius).

12) Deve suportar, no mínimo, umidade do ar de 5% a 95% sem condensação.

13) Deve operar em condições ambientais respeitando, no mínimo, a normaIEC 60529 nível IP-67 (International Protection Rating).

14) Deve sobreviver a rajadas de ventos de até 265 Km/h ou 165 MPH.

15) Deve possuir 2x3 multiple-input multiple-output (MIMO) em 802.11n (faixas de 2,4GHz e 5GHz).

16) Deverá operar em canais de 20 e 40 MHz em 802.11n.

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

18) Possuir pelo menos as seguintes taxas de transmissão e com fallback automático para 802.11n: MSC0 - MSC15 (6.5Mbps - 300Mbps).

19) Deve ser capaz de selecionar automaticamente o canal de transmissão.

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

21) Deve suportar pelo menos modulação OFDM.

22) Deve permitir o ajuste dinâmico de nível de potência e canal de rádio de modo a otimizar o tamanho da célula de RF.

23) Deve possuir funcionalidade de permitir ou bloquear a divulgação do SSID.

24) Deve possuir padrão WMM (Wi-Fi Multimedia) da Wi-Fi Alliance para priorização de tráfego.

25) A quantidade de usuários por ponto de acesso WiFi não deve ser restringida por licenças.

26) Deve implementar tecnologia MRC - With maximum ratio combining (MRC) technology.

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

28) O ponto de acesso deve possuir no mínimo 03 (três) conexões dual-band (2,4GHz e 5GHz) para instalação de pelo menos 03 (três) antenas externas. As antenas devem operar, no mínimo, nas faixas de frequência entre 2,400 e 2,480 MHz e entre 5.725 e 5.850 MHz, simultaneamente, na mesma antena. Estas antenas devem ser do tipo para instalação em ambientes externos e do mesmo fabricante do ponto de acesso.

29) Devem ser fornecidas 03 (três antenas), que serão conectadas diretamente ao rádio, sem cabo externo. A antena pode ser de fabricante diferente do ponto de acesso.

30) As antenas devem prover ganho de, no mínimo, 4.0 dBi na faixa de frequência de 2,4GHz e de 7.0 dBi na faixa de frequência de 5GHz, simultaneamente. As antenas devem operar com padrão de irradiação omnidirecional, provendo cobertura em 360º (trezentos e sessenta graus).

31) Caso o ponto de acesso não possua 03 (três) conexões para antenas dual-band (2,4GHz e 5GHz), deverão ser fornecidos no mínimo 02 (dois) pontos de acesso com as seguintes configurações:

- Um ponto de acesso deverá ser fornecido com 02 antenas com ganho de no mínimo 4.0 dBi operando nas faixas de frequência entre 2,400 e 2,480 GHz e com 02 antenas com ganho de no mínimo 7.0 dBi operando nas faixas entre 5,725 e 5,850 GHz.

- O outro ponto de acesso deverá ser fornecido com 01 antena com ganho de no mínimo 4.0 dBi operando nas faixas de frequência entre 2,400 e 2,480 GHz e com 01 antena com ganho de no mínimo 7.0 dBi operando nas faixas entre 5,725 e 5,850 GHz.

- Os custos dos dois pontos de acesso deverão ser inseridos no Item “Ponto de Acesso WiFi Externo”.

32) Todas as antenas devem operar com padrão de irradiação omnidirecional, provendo cobertura em 360º (trezentos e sessenta graus). As antenas devem ser do tipo para instalação em ambientes externos e do mesmo fabricante do ponto de acesso.

33) Deve possuir sensibilidade de recepção de valor menor ou igual:

- -92dBm em 802.11a a 6Mbps;
- -92dBm em 802.11b a 5.5Mbps;
- -92dBm em 802.11g a 6Mbps;
- -93dBm em 802.11n (HT20) a MC0 em 2,4GHz;
- -89dBm em 802.11n (HT40) a MC0 em 5GHz.

34) Deve possuir, no mínimo, 01 (uma) interface padrão IEEE 802.3ab 10/100/1000BaseT, auto-sensing, auto MDI/MDIX, com conectores RJ-45, OU 01 (uma) interface GigabitEthernet em fibra óptica monomodo padrão IEEE 802.3z 1000BaseLX 1310nm para conexão à rede local.

35) O ponto de acesso deve possuir estrutura que permita fixação em poste e mastros. Todos os acessórios para que possa ser feita a fixação deverão ser fornecidos com o equipamento.

36) Deve permitir a atualização remota ou local do sistema operacional e arquivos de configurações utilizados nos equipamentos, via interfaces ethernet ou serial.

37) Possuir no mínimo 01 LED indicativo do estado de operação.

38) O equipamento deve vir acompanhado de manuais que contenham informações suficientes para possibilitar a instalação, configuração e operacionalização do equipamento.

39) Ser acompanhado de todos os acessórios necessários para operacionalização, tais como: licenças de softwares, documentação técnica e manuais que contenham informações suficientes para possibilitar a instalação, configuração e operacionalização.

40) Possuir varredura de RF nas bandas 802.11a, 802.11b, 802.11g e 802.11n para identificação de pontos de acesso intrusos não autorizados (rogues) e interferências no canal habilitado ao ponto de acesso e nos demais canais configurados na rede WiFi, sem impacto no seu desempenho;

41) Possuir IEEE 802.1x, com pelo menos os seguintes métodos EAP:

- EAP-PEAP.
- EAP-TLS.
- EAP-TTLS.

42) Possuir criptografia do tráfego local.

43) Deve implementar 802.11i.

44) Deve possuir Wi-Fi Protected Access: WPA2 e WPA.

45) Deve detectar e gerar alarmes de interferências WiFi (provenientes de dispositivos padrão IEEE802.11) e detectar, classificar e gerar alarmes de interferências não-WiFi, tais como bluetooth, telefones sem fio, câmeras de vídeo sem fio e outros.

46) 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;

47) Todos os rádios do equipamento devem processar os dados WiFi dos usuários enquanto a análise de espectro é realizada pelo ponto de acesso de forma simultânea, sem prejuízo de performance.

48) O ponto de acesso deve fornecer informações em tempo real ao controlador WiFi ao qual está associado referentes à qualidade do espectro de RF para o canal de operação atual e para todos os canais de operação nas faixas de 2,4GHz e 5GHz, ao mesmo tempo que processa dados 802.11 dos usuários da rede WiFi.

49) Caso o ponto de acesso ofertado não possua capacidade para realizar simultaneamente a monitoração de espectro e o atendimento dos usuários da rede WiFi por todos os rádios do equipamento, sem prejuízo de desempenho, a proponente deverá ofertar 02 (dois) pontos de acesso WiFi para atender o requerimento técnico:

- O primeiro ponto de acesso será utilizado para realizar a monitoração de espectro de Rádio Frequência.
- O segundo ponto de acesso será utilizado para atender os usuários respeitando os requisitos de modularidade descritos nos requisitos do Item 16.
- Os custos dos dois pontos de acesso deverão ser inseridos no Item “Ponto de Acesso WiFi Externo”.

50) O ponto de acesso WiFi deverá ser alimentado diretamente por ponto de energia elétrica de 100-240VAC e 60Hz. Caso seja fornecido com fonte de alimentação externa ou power injector externo, os mesmos devem respeitar:

51) Deve operar, no mínimo, com temperaturas de -20 a +55°C (graus Celsius).

52) Deve suportar, no mínimo, umidade do ar de 5% a 95% sem condensação.

53) A alimentação elétrica dos componentes da solução deverá ser feita pela CONTRATADA somente a partir de ponto de energia elétrica de 100-240VAC-60Hz a ser disponibilizado pela CONTRATANTE próximo da ponto de acesso. Deverá ser fornecido pela CONTRATADA o cabo de alimentação elétrica com pelo menos 10 metros de comprimento.

54) O equipamento ponto de acesso WiFi deve ser homologado pela ANATEL.

Item 20.Serviço de Instalação do Item 19

São de responsabilidade da contratada para a execução dos Serviços de Instalação, a instalação física e a configuração lógica do equipamento conforme os requisitos, localidades e condições descritas no item “2.3)Serviços de Instalação”deste documento.

Item 21.Serviço de Manutenção e Suporte do Item 19

1) Os serviços de Suporte e Manutenção deste Item deverão ser realizados em regime 8x5xNBD (8 horas x 5 dias da semana com prazo para inicio da resolução do problema até o dia útil subsequente à abertura do chamado técnico) pelo prazo mínimo de 12 (doze) meses que deverá ser considerado na planilha de preços como valor unitário por unidade de equipamento.

2) A CONTRATANTE poderá abrir chamados de manutenção diretamente no Fabricante do Item sem necessidade de prévia consulta e/ou qualquer liberação por parte da CONTRATADA.

3) Deverá ser garantido à CONTRATANTE o pleno acesso ao site do Fabricante dos equipamentos e softwares. Esse acesso deve permitir consultas a quaisquer bases de dados disponíveis para usuários relacionadas aos equipamentos e softwares especificados, além de permitir downloads de quaisquer atualizações de software ou documentação deste produto.

Item 22. Site Survey

1) A CONTRATADA deverá realizar o serviço de Site Survey dos pontos de implantação dos "Pontos de Acesso WiFi" por Andar de Bloco de Edificação ou Área Externa, incluindo o trabalho de levantamento de campo.

2) Após a formalização da quantidade de usuários e locais onde a solução será implantada pela CONTRATANTE, a CONTRATADA terá um prazo de 20 (vinte) dias corridos para apresentação do relatório do site survey contendo as seguintes informações:

- Quantidade de "Pontos de Acesso WiFi" (considerando serem estes os especificados nos subitens 16 e 19 desta solução) necessários para cobertura da localidade indicada e quantidade de usuários;

- A CONTRATADA deverá apresentar relatório contendo o mapeamento e distribuição dos "Pontos de Acesso WiFi" distribuídos no mapa da localidade.

Item 23.Operação Assistida

1) A aquisição dos equipamentos e softwares relacionados no Grupo 1 ensejará a execução da fase de operação assistida descrita neste item.

2) Por operação assistida entende-se o acompanhamento presencial do funcionamento dos equipamentos e softwares instalados, com pronta intervenção no caso de qualquer problema detectado, bem como o esclarecimento de quaisquer dúvidas levantadas pela equipe técnica da CONTRATANTE.

3) A Unidade referente à "Operação Assistida" é por Dia Útil de trabalho, sendo que a quantidade mínima contratada não deverá ser menor que 5 (cinco) dias.

4) Após o atesto relativo à etapa de instalação e configuração dos equipamentos e softwares, a CONTRATADA deverá prover o serviço de operação assistida durante o período contratado.

5) Durante o período contratado de operação assistida, a CONTRATADA deverá manter nas dependências do CONTRATANTE, nos dias úteis, das 8h às 12h e das 13h às 17h, um profissional com certificação de nível profissional do mesmo fabricante da solução ofertada que tenha participado da etapa de instalação e configuração dos equipamentos.

6) Concluído o período contratado referente à etapa de operação assistida, e não havendo problemas técnicos, operacionais, de performance e/ou dúvidas sobre a gerência e funcionamento da solução implementada, o CONTRATANTE, por comissão especialmente constituída para este fim, subsidiada por sua equipe de gerência de redes, atestará o serviço em até 5 (cinco) dias úteis.

Item 24.Treinamento do Tipo I para a Solução de Segurança e Comunicação Unificada (WIFI)

1) A CONTRATADA deverá prover um serviço de transferência de conhecimento, denominado simplesmente como "Treinamento do Tipo I para a

Solução de Segurança e Comunicação Unificada" com base em material do fabricante da solução ofertada.

2) Caso a solução ofertada seja composta por mais de um fabricante, deverá ser ofertado "Treinamento do Tipo I para a Solução de Segurança e Comunicação Unificada" apenas para a solução que componha maior parte da solução.

3) O "Treinamento do Tipo I para a Solução de Segurança e Comunicação Unificada" deverá ser ministrado por profissional capacitado e certificado pelo Fabricante com foco na tecnologia de "Rede WiFi" que compõe a Solução de Segurança e Comunicação Unificada.

4) O "Treinamento do Tipo I para a Solução de Segurança e Comunicação Unificada" deverá ser realizado para um grupo de 5 (cinco) técnicos da CONTRANTE.

5) O "Treinamento do Tipo I para a Solução de Segurança e Comunicação Unificada" deverá possuir carga horária mínima de 40 (quarenta) horas e deverá ocorrer em meio período a ser definido pela CONTRATANTE.

6) O "Treinamento do Tipo I para a Solução de Segurança e Comunicação Unificada" deverá ser realizada utilizando conteúdo teórico e prático, através de laboratório preparado com equipamentos equivalentes aos ofertados, onde estarão disponíveis as mesmas funcionalidades solicitadas nas especificações técnicas dos itens referentesà tecnologia de "Rede Wifi".

7) O curso deverá ter conteúdo técnico teórico e prático, onde os alunos deverão ter conhecimentos básicos para instalação, operação e manutenção da tecnologia de "Rede WiFi" que compõea solução de Segurança e Comunicação Unificada.

8) A CONTRATADA deverá disponibilizar instalações na cidade de Brasília/DF bem como todos os materiais necessários aos alunos para a realização do treinamento.

9) A CONTRATADA deverá prover toda a logística e todo o material necessário à execução da capacitação teórica e prática, ou seja, instalações adequadas, equipamentos, manuais e apostilas didáticas. Os manuais e apostilas fornecidos devem ser desenvolvidos com base nos materiais do fabricante.

10) Será permitida a utilização de acesso remoto aos equipamentos destinados ao conteúdo prático do treinamento quando necessário. Os equipamentos deverão ser de mesma marca e semelhante aos equipamentos ofertados.

11) A capacitação técnica deverá ter início em até 30 (trinta) dias após a assinatura do contrato, podendo ser adiada por conveniência daCONTRATANTE, quando então, em comum acordo com a CONTRATADA,

será marcada a data definitiva.

GRUPO 2 - Solução de Controle de Acesso (itens 25 a 31)

Item 25. Solução Centralizada de Controle de Acesso de Usuários e Dispositivos

1) Fornecimento de “Solução Centralizada de Controle de Acesso deUsuários e Dispositivos” nova e sem uso anterior. Deverá estar em linha de produção, sem previsão de encerramento de fabricação na data de entrega da proposta.

2) O modelo ofertado deve ser compatível com o Item “Controlador WiFi” descrito neste Termo de Referência.

3) A solução deverá prover a funcionalidade de autenticação para os usuários da rede wireless, cabo e VPN.

4) A solução deverá ser fornecida com suporte as funções de autenticação, identificação e validação para no mínimo, 500 (quinhentos) dispositivos com capacidade de expansão para pelo menos2.000 (dois mil) dispositivos sem adição de hardware. Caso a solução utilize assinatura para ativação destas funcionalidades, deverá ser fornecida assinatura com cobertura para no mínimo 36 meses;

5) A solução deverá ser fornecida em forma "appliance" através de equipamento dedicado e exclusivo para esta finalidade e com sistema operacional e software especializado. Todas as funcionalidades descritas neste Item deverão ser executadas no mesmo equipamento. Toda a solução de hardware e software deverá ser fornecida pelo mesmo fabricante.

6) Não serão aceitas soluções baseadas em software.

7) Cada equipamento deverá ser fornecido com todos os acessórios, placas, memórias, softwares e licenças para atender a função de autenticação integralmente.

8) A solução deve suportar alta disponibilidade (“high availability”).

9) Deverá possuir mecanismo de replicação de informações entre os dois dispositivos.

10) Implementar o padrão aberto de gerência de rede SNMPv3.

11) Permitir a gravação de log externo (syslog).

12) Todas as configurações devem ser feitas através de interface gráfica utilizando protocolo HTTPS.

13) Deve funcionar em conjunto com a solução de wireless constante no Grupo1 deste Termo de Referência.

14) Requisitos de Identificação e Autenticação de Usuário:

- Deverá permitir que usuários especiais autorizados possam criar contas temporárias para visitantes acessar a rede.

- Deverá permitir criação de contas temporárias com políticas de segurança definidas.

- Deverá permitir que usuários especiais autorizados autentiquem-se em base interna da solução e externa, como no Microsoft "Active Directory", LDAP (LightweightDirectory Access Protocol), InternalDatabase e RADIUS.

- Deverá permitir que as políticas de segurança dos usuários especiais autorizados sejam baseadas no Grupo definido.

- Deverá permitir que os usuários especiais autorizados possam criar contas, editar, suspender e também gerar relatórios.

- Deverá permitir limitar que os usuários especiais autorizados tenham acesso apenas às contas criadas por ele mesmo.

- Deverá permitir que os usuários especiais autorizados tenham acesso à todas as contas criadas.

- Deve possibilitar a configuração para separação do tráfego dos usuários visitantes em uma rede lógica independente.

- Deve possibilitar a configuração de atribuição de nível de serviço e acesso a serviços baseado na autenticação de usuário.

- Deverá ter a capacidade de definir o acesso de usuário visitante dentro de um período pré-determinado.

- A solução deverá atuar como um servidor RADIUS, permitindo autenticar os usuários cadastrados como visitante.

- A autenticação e autorização para acesso de usuários e dispositivos deve utilizar RADIUS como protocolo de controle.

- A solução deve prover autenticação e autorização de acesso à rede baseado na identificação do usuário e do dispositivo utilizado pelo usuário.

- A solução deve permitir o agrupamento de usuários baseado no papel do usuário na organização e em um conjunto de privilégios similares.

- A solução deve controlar o acesso de usuários e dispositivos através de redes com e sem fio (wireless).

- A solução deve suportar CoA (ChangeofAuthorization – RFC3576), que permita o controle dinâmico de todas as sessões RADIUS ativas.

- A solução deve suportar os seguintes protocolos de autenticação: EAP-MSCHAPv2, EAP-MD5, EAP-TLS e PEAP.

- A solução deve permitir que visitantes, contratados e temporários se autentiquem na rede através de um portal HTTP ou HTTPS.

- A solução deve permitir que determinados usuários tenham privilégio para a criação de contas de visitantes.

- A solução deve permitir que o visitante receba as informações de acesso à rede via impressão, email ou SMS.

15) Requisitos de Identificação e Validação de Dispositivo:

- A solução deve possuir capacidade de identificação automáticade tipos de dispositivos conectados a rede com base em valores de atributos associados ao dispositivo.

- A solução deve suportar a coleta de atributos relacionados a dispositivos através do uso de probes HTTP, DHCP, RADIUS, DNS, SNMP.

- Deve suportar atributos dos protocolos DHCP, IP, LLDP, MAC, RADIUS, SNMP para identificação de tipo de dispositivo.

- A solução deve permitir a criação de lista de regras customizadaspara construção de políticas de identificação de tipos de dispositivos.

- A solução deve permitir a construção de políticas de segurança para autorização de acesso com base nas políticasde identificação de tipo de dispositivo.

- Deve ser possível criar políticas de acesso e autorização baseado no tipo de dispositivo identificado.

- A solução deve suportar a classificação de dispositivos identificados no mínimo pelo fabricante, modelo e sistema operacional.

- Deve ser permitido ao usuário se autenticar através de diferentes tipos de dispositivos simultaneamente com políticas de acesso e autorização distintas associadas a cada tipo de dispositivo.

- A solução deve possuir funcionalidade de identificação de tipos de

dispositivos não associados a usuários, como câmeras IP, impressoras e dispositivos de segurança física. Para cada tipo de dispositivo identificado, deve ser possível aplicar de forma automática políticas de acesso e autorização.

- A solução deve implementar política de avaliação de acesso do dispositivo cliente quanto a sua conformidade com as políticas de software de antivírus, antispyware, sistema operacional e software cliente (agente) com base no tipo e versão do sistema operacional, tipo e versão do browser utilizado, bem como nível de acesso do usuário ou grupo, podendo de forma automática promover atualização destes softwares antes que o dispositivo cliente seja autorizado a acessar a rede.

- A solução deve possuir softwares clientes (agente) para avaliação de acesso de dispositivos com suporte aos sistemas operacionais Microsoft Windows e Apple Mac OSX.Deve possuir clientes WEB com suporte a Mozilla Firefox, Google Chrome, Apple Safari e Microsoft Internet Explorer.

- A solução deve possuir funcionalidade de distribuição automática de software cliente (agente) para o dispositivo de usuário por meio de execução de política de avaliação de acesso.

- Devepossuir opçãode customização da tela de login do usuário do software cliente (agente), com inserção de logotipo, instruções de login e mensagem.

16) Requisitos de hardware:

- Possuir, no máximo, 01 (um) RU's de altura e deverá vir acompanhado de todos os acessórios originais do fabricante para a instalação em rack de 19 polegadas.

- Possuir no mínimo 1 (um) Processador Quad-Core de 2.4 GHz.

- Possuir no mínimo 16 (dezesseis) GB de memória RAM.

- Possuir, no mínimo, 01 (um) disco rígido SAS de 600 (seiscentos) Gbytes e 10.000 (dez mil) RPM.

- Possuir, no mínimo, 04 (quatro) interfaces GigabitEthernet 100/1000 elétrica (UTP/RJ45).

- Possuir fonte interna com chaveamento automático de no mínimo 650W de potência que opera em 110V / 220V e 60Hz de frequência.

Item 26.Serviço de Instalação do Item 25

São de responsabilidade da contratada para a execução dos Serviços de Instalação, a instalação física e a configuração lógica da solução conforme os requisitos, localidades e condições descritas no item "2.3)Serviços de Instalação" deste documento.

Item 27.Serviço de Manutenção e Suporte do Item 25

1) Os serviços de Suporte e Manutenção do equipamento deverão ser em regime de 24x7x4 (24 horas x 7 dias da semana com prazo para inicio da resolução do problema até 04 horas subsequentes à abertura do chamado técnico) pelo prazo mínimo de 12 (doze) meses que deverá ser considerado na planilha de preços como valor unitário por unidade de equipamento.

2) A CONTRATANTE poderá abrir chamados de manutenção diretamente no Fabricante do Item sem necessidade de prévia consulta e/ou qualquer liberação por parte da CONTRATADA.

3) Deverá ser garantido à CONTRATANTE o pleno acesso ao site do Fabricante dos equipamentos e softwares. Esse acesso deve permitir consultas a quaisquer bases de dados disponíveis para usuários relacionadas aos equipamentos e softwares especificados, além de permitir downloads de quaisquer atualizações de software ou documentação deste produto.

Item 28. Pacote de Expansão para Solução Centralizada de Controle Acesso de Usuários e Dispositivos

1) Fornecimento de Pacote de Expansão para Solução Centralizada de Controle Acesso de Usuários e Dispositivos 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.

2) O modelo ofertado deve ser do mesmo fabricante do Item "Solução Centralizada Controle Acesso de Usuários e Dispositivos" descrito neste Termo de Referência.

3) Deverá ser fornecido o Pacote de Expansão para Solução Centralizada Controle Acesso de Usuários e Dispositivos para atender, no mínimo, 250 (duzentos e cinqüenta) novos dispositivos.

4) A solução deve atender a todas as características de funcionamento contidas no Item "Solução Centralizada Controle Acesso de Usuários e Dispositivos".

5) A solução poderá ser fornecida baseada em licenças, software e/ou hardware.

Item 29. Serviço de Instalação do Item 28

São de responsabilidade da contratada para a execução dos Serviços de Instalação, a instalação física e a configuração lógica do pacote de expansão conforme os requisitos, localidades e condições descritas no item “2.3)Serviços de Instalação”deste documento.

Item 30.Serviço de Manutenção e Suporte do Item 28

1) Os serviços de Suporte e Manutenção do equipamento deverão ser em regime de 24x7x4 (24 horas x 7 dias da semana com prazo para inicio da resolução do problema até 04 horas subsequentes à abertura do chamado técnico) pelo prazo mínimo de 12 (doze) meses que deverá ser considerado na planilha de preços como valor unitário por unidade de equipamento.

2) A CONTRATANTE poderá abrir chamados de manutenção diretamente no Fabricante do Item sem necessidade de prévia consulta e/ou qualquer liberação por parte da CONTRATADA.

3) Deverá ser garantido à CONTRATANTE o pleno acesso ao site do Fabricante dos equipamentos e softwares. Esse acesso deve permitir consultas a quaisquer bases de dados disponíveis para usuários relacionadas aos equipamentos e softwares especificados, além de permitir downloads de quaisquer atualizações de software ou documentação deste produto.

Item 31.Operação Assistida

1) A aquisição dos equipamentos e softwares relacionados no Grupo 2 ensejará aexecução da fase de operação assistida descrita neste item.

2) Por operação assistida entende-se o acompanhamento presencial do funcionamento dos equipamentos e softwares instalados, com pronta intervenção no caso de qualquer problema detectado, bem como o esclarecimento de quaisquer dúvidas levantadas pela equipe técnica da CONTRATANTE.

3) A Unidade referente à "Operação Assistida" é por Dia Útil de trabalho, sendo que a quantidade mínima contratada não deverá ser menor que 5 (cinco) dias.

4) Após o atesto relativo à etapa de instalação e configuração dos equipamentos e softwares, a CONTRATADA deverá prover o serviço de operação assistida durante o período contratado.

5) Durante o período contratado de operação assistida, a CONTRATADA deverá manter nas dependências do CONTRATANTE, nos dias úteis, das 8h às 12h e das 13h às 17h, um profissional com certificação de nível profissional do mesmo fabricante da solução ofertada que tenha participado da etapa de instalação e configuração dos equipamentos.

6) Concluído o período contratado referente à etapa de operação assistida, e não havendo problemas técnicos, operacionais, de performance e/ou dúvidas

sobre a gerência e funcionamento da solução implementada, o CONTRATANTE, por comissão especialmente constituída para este fim, subsidiada por sua equipe de gerência de redes, atestará o serviço em até 5 (cinco) dias úteis.

GRUPO 3 - Switching (itens 32 a 58)

Item 32.Switch de Acesso Tipo I

1) Fornecimento de Switch de Acesso Tipo I 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.

2) O modelo ofertado deve ser do mesmo fabricante do Item “Switch Core” descrito neste Termo de Referência.

3) Possuir no mínimo um total de 50 (cinquenta) interfaces de rede dedicadas e não compartilhadas, sem uso de interfaces tipo "combo". Estas interfaces devem ser divididas da seguinte forma:

- Possuir, no mínimo, 2 (duas) interfaces ópticas dedicadas e não compartilhadas padrão 10GBaseX 10Gigabit Ethernet, Full-duplex, baseadas em conectores ópticos (transceivers) padrão SFP+. Deverá ter capacidade para aceitar conectores ópticos dos padrões 10GBaseSR, 10GBaseLR e 10GBaseER.

- Possuir, no mínimo, 48 (quarenta e oito) interfaces dedicadas e não compartilhadas padrão Gigabit Ethernet 10/100/1000Base-T de 10/100/1000 Mbps, Full duplex, conector RJ-45 e com autosensing de velocidade. Estas portas não podem ser compartilhadas com slots utilizados para portas de uplink ou de empilhamento.

4) Todas as interfaces Ethernet 10/100/1000Base-T devem obedecer às normas técnicas IEEE802.3 (10BaseT), IEEE802.3u (100BaseTX), 802.3ab (1000BaseT) e IEEE802.3x (FlowControl).

5) Possuir porta de console para gerenciamento e configuração via linha de comando. O conector deve ser RJ-45 ou padrão RS-232 (os cabos e eventuais adaptadores necessários para acesso à porta de console devem ser fornecidos).

6) Possuir fonte de alimentação interna ao equipamento, chaveada, com ajuste automático de tensão 110 e 220 volts e operando na freqüência de 60 Hz.

7) Deve ser instalável em rack padrão de 19”, sendo que deverão ser fornecidos os respectivos Kit’s de fixação.

8) Deve possuir no máximo 1 rack unit (1RU) de altura.

9) Possuir LEDs, por porta, que indiquem a integridade e atividade do link e se a porta está transmitindo ou recebendo tráfego.

10) Possuir interfaces de gerenciamento baseadas em linha de comando (CLI) e WEB browser (HTTP e HTTPS) que permita aos usuários configurar e gerenciar switches através de um browser padrão.

11) Implementar HTTP com criptografia SSL versão 3 (HTTPS) de forma a prover uma conexão segura quando o switch é configurado ou monitorado via WEB Browser.

12) Gerenciável via Telnet (com no mínimo 5 sessões simultâneas) e porta de console.

13) Devem ser implementados, no mínimo, 3 (três) níveis de privilégios de acesso para gerenciamento do switch via Telnet, a saber:

- Nível “Administrador” ou “Super-usuário”: acesso completo e ilimitado, sendo permitidas operações de leitura e escrita sobre todo o sistema.

- Nível “Operador”: acesso com operações leitura e escrita, tendo escopo de atuação limitada a portas específicas.

- Nível “Somente Leitura”: acesso limitado à visualização de configurações, sem direitos de modificações.

14) Deve ser gerenciável via SSH versão 2 (SSHv2).

15) Devem ser implementados, para maior segurança do SSHv2, os algoritmos de criptografia: 3DES (168 bits) e AES (128, 192 e 256 bits).

16) Possuir agente de gerenciamento MIB, MIB SNMP II (RFC 1213), MIB bridging (RFC 1493), que possua descrição completa das MIBimplementadas no equipamento, inclusive as extensões privadas, se existirem.

17) Deve ser gerenciável via SNMP (v1, v2 e v3).

18) Implementar nativamente 4 grupos RMON (History, Statistics, Alarms e Events) conforme RFC 1757.

19) Deve permitir o espelhamento de VLANs ou portas e de um grupo de portas - independentemente de haver ou não política de tráfego aplicadas a estas portas - para pelo menos duas outras portas especificadas, no mesmo switch ou não.

20) O fabricante do equipamento ofertado deve possuir ferramenta que permita gerenciar as configurações física e lógica do mesmo.

21) Implementar o protocolo Syslog para funções de “logging” de eventos.

22) Possibilidade de upgrade de software através do protocolo TFTP.

23) Deve possuir arquitetura que utilize memória Flash-EPROM para armazenamento do sistema operacional.

24) O equipamento deve vir acompanhado de manuais que contenham informações suficientes para possibilitar a instalação, configuração e operacionalização.

25) Implementar Redes Locais Virtuais (VLANs).

26) Implementar LANs Virtuais (VLANs) conforme definições do padrão IEEE 802.1Q.

27) Implementar a criação de no mínimo 255 VLANs ativas baseadas em interfaces.

28) Deve implementarVLANs dinâmicas. Deve implementar a criação, remoção e distribuição de VLANs de forma dinâmica através de interfaces configuradas como tronco IEEE 802.1Q.

29) Implementar "VLAN Trunking" conforme padrão IEEE 802.1Q nas interfaces Gigabit Ethernet. Deve ser possível estabelecer quais VLANs serão permitidas em cada um dos troncos 802.1Q configurados.

30) Implementar a funcionalidade de "PortTrunking" conforme padrão IEEE 802.3ad.

31) Deve implementar a função de Unidirection Link Detection (UDLD) para detecção de problemas no cabeamento da rede.

32) Deve ser possível criar grupos de interfaces contendo pelo menos 08 (oito) interfaces Gigabit Ethernet (em "full duplex").

33) Deve implementar empilhamento (stack). Deve ser acompanhado das interfaces e cabos necessários para empilhamento.

34) O empilhamento deve ser feito através de interfaces e slots dedicados, não compartilhados e não deve consumir interfaces de Rede.

35) A funcionalidade de empilhamento deve possuir pelo menos as seguintes características:

- Deve implementar a criação de pelo menos 06 (seis) grupos de interfaces agregadas por stack (pilha).
- Deve ser possível empilhar pelo menos 04 (quatro) destes switches por pilha.
- O empilhamento deve ser feito em anel ("stackring") para garantir que, na eventual falha de um link, a pilha continue a funcionar.

- A pilha deverá ser gerenciada através de um único endereço IP, implementar agregação lógica de links utilizando qualquer porta da pilha além de implementar espelhamento de interfaces de qualquer porta para qualquer porta da pilha.

- Em caso de falha do switch controlador da pilha, um controlador "backup" deve ser selecionado de forma automática, sem que seja necessária intervenção manual.

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

- A conexão entre os switches membros da pilha deve ser de pelo menos 20 Gbps.

- O empilhamento deverá ocorrer entre switches do mesmo tipo e entre os Tipos I, II e III;

36) Deve implementar o protocolo SpanningTree.

37) Deve implementar o Protocolo Spanning-Tree conforme padrão IEEE 802.1d.

38) Deve implementar o padrão IEEE 802.1s ("MultipleSpanningTree").

39) Deve implementar o padrão IEEE 802.1w ("RapidSpanningTree").

40) Implementar mecanismo de proteção da "root bridge" do algoritmo Spanning-Tree para prover defesa contra ataques do tipo "Denialof Service" no ambiente nível 2.

41) Deve implementar Per VLAN Spanning Tree.

42) Implementar funcionalidades IPv6 para gerenciamento.

43) Deve ser suportadas as funcionalidades de IPv6: Endereços de unicast, rotas estáticas, ICMP.

44) Deve ser implementado o protocolo Virtual RouterRedundancyProtocol (VRRP) ou Hot StandbyRouterProtocol (HSRP).

45) Deve ser implementado o protocolo IEEE 802.1AB Link Layer Discovery Protocol (LLDP) e sua extensão LLDP-MED, permitindo a descoberta dos elementos de rede vizinhos.

46) Deve ser implementado o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol).

47) Deve ser implementado o protocolo Telnet, conforme RFC 854. Devem ser implementados os protocolos TFTP e FTP, conforme RFC 783 e RFC 959, respectivamente.

48) Deve implementar roteamento estático.

49) Implementar roteamento de camada 3 entre VLANs (Interfaces Virtuais ou SVIs).

50) Deve possuir capacidade de comutação (switchingcapacity) de, no mínimo, 176 Gbpsfull duplex.

51) Possuir capacidade de processamento de pelo menos 100 Mpps (cem milhões de pacotes por segundo) considerando pacotes de 64 Bytes.

52) Possuir capacidade para no mínimo 8000 endereços MAC.

53) Ser fornecido com configuração de CPU e memória (RAM e Flash) suficiente para implementação de todas as funcionalidades descritas nesta especificação.

54) Suportar o encaminhamento de “jumbo frames” (frames de 9000 bytes) nas portas Gigabit Ethernet 10/100/1000 RJ45.

55) Implementar mecanismos de autenticação, autorização e accounting (AAA) via RADIUS e TACACS+ conforme RFCs 2138 e RFC1492 respectivamente.

56) Implementar mecanismos de AAA (Authentication, Authorization e Accounting) com garantia de entrega dos pacotes transferidos entre cliente e servidor AAA.

57) Controlar quais comandos os usuários e grupos de usuários podem executar nos equipamentos gerenciados. Devem ser registrados no servidor AAA todos os comandos executados.

58) Implementar controle de acesso por porta, usando o padrão IEEE 802.1x (PortBased Network Access Control).

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

60) Na autenticação 802.1x, deve implementar funcionalidade que designe VLAN específica para o usuário quando: a estação não tem cliente 802.1x (suplicante) ou as credenciais do usuário não estão corretas (falha de autenticação).

61) Na autenticação 802.1x, implementar associação automática de VLAN da porta do switch através da qual o usuário requisitou acesso à rede.

62) 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: identificação do usuário, porta do switch utilizada para acesso do usuário e identificação da sessão.

63) Na autenticação 802.1x, deve ser possível definir, por porta, o intervalo de tempo para obrigar o cliente a se reautenticar (reautenticação periódica).

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

65) Para equipamentos que não disponham de suplicantes 802.1x (impressoras, etc) deve ser suportado no mínimo a alocação dos mesmos em uma VLAN específica.

66) Implementar 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. Deve ser possível desabilitar a porta e enviar um trap SNMP caso algum MAC diferente tente se conectar na porta.

67) Deve ser possível estabelecer o número máximo de endereços MAC 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.

68) Implementar listas de controle de acesso (ACLs) baseadas em endereço IP de origem e destino, interfaces TCP e UDP de origem e destino e endereços MAC de origem e destino.

69) Possuir controle de broadcast, multicast e unicast por porta. Deve ser possível especificar limiares (“thresholds”) individuais para tráfego tolerável de broadcast, multicast e unicast em cada porta do switch.

70) Promover análise do protocolo ARP (AddressResolutionProtocol) e possuir proteção nativa contra ataques do tipo “ARP Poisoning”.

71) Deve implementar servidor DHCP.

72) Deve Implementar IGMP Snooping (v1, v2 e v3).

73) Implementar pelo menos quatro filas de saída por porta.

74) Implementar pelo menos uma fila de saída com prioridade estrita por porta e divisão ponderada de banda entre as demais filas de saída.

75) Implementar classificação, marcação e priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS).

76) Deve implementar classificação, marcação e priorização de tráfego baseada nos valores do campo “Differentiated Services Code Point” (DSCP) do

cabeçalho IP, conforme definições do IETF.

77) Desejável implementar classificação de tráfego baseada em endereço IP de origem/destino, interfaces TCP e UDP de origem e destino, endereços MAC de origem e destino.

78) Implementar funcionalidades de QoS de "TrafficPolicing". Deve ser possível a especificação de banda por classe de serviço. Para os pacotes que excederem a especificação deve ser possível configurar, no mínimo, a ação de descarte do pacote.

Item 33.Serviço de Instalação do Item 32

São de responsabilidade da contratada para a execução dos Serviços de Instalação, a instalação física e a configuração lógica do equipamento conforme os requisitos, localidades e condições descritas no item "2.3)Serviços de Instalação"deste documento.

Item 34. Serviço de Manutenção e Suporte do Item 32

1) Os serviços de Suporte e Manutenção deste Item deverão ser realizados em regime 8x5xNBD (8 horas x 5 dias da semana com prazo para inicio da resolução do problema até o dia útil subsequente à abertura do chamado técnico) pelo prazo mínimo de 12 (doze) meses que deverá ser considerado na planilha de preços como valor unitário por unidade de equipamento.

2) A CONTRATANTE poderá abrir chamados de manutenção diretamente no Fabricante do Item sem necessidade de prévia consulta e/ou qualquer liberação por parte da CONTRATADA.

3) Deverá ser garantido à CONTRATANTE o pleno acesso ao site do Fabricante dos equipamentos e softwares. Esse acesso deve permitir consultas a quaisquer bases de dados disponíveis para usuários relacionadas aos equipamentos e softwares especificados, além de permitir downloads de quaisquer atualizações de software ou documentação deste produto.

Item 35.Switch de Acesso Tipo II

1) Fornecimento de Switch de Acesso Tipo II 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.

2) O modelo ofertado deve ser do mesmo fabricante do Item "Switch Core" descrito neste Termo de Referência;

3) Possuir no mínimo um total de 50 (cinquenta) interfaces de rede dedicadas e não compartilhadas, sem uso de interfaces tipo "combo". Estas interfaces devem ser divididas da seguinte forma:

- Possuir, no mínimo, 2 (duas) interfaces ópticas dedicadas e não

compartilhadas padrão 10GBaseX 10Gigabit Ethernet, Full-duplex, baseadas em conectores ópticos (transceivers) padrão SFP+. Deverá ter capacidade para aceitar conectores ópticos dos padrões 10GBaseSR, 10GBaseLR e 10GBaseER.

- Possuir, no mínimo, 48 (quarenta e oito) interfaces dedicadas e não compartilhadas padrão Gigabit Ethernet 10/100/1000Base-T de 10/100/1000 Mbps, Full duplex, conector RJ-45 e com autosensing de velocidade. Estas portas não podem ser compartilhadas com slots utilizados para portas de uplink ou de empilhamento.

- Implementar o padrão PoE (Power over Ethernet) IEEE 802.3af simultaneamente em pelo menos 24 das 48 interfaces Ethernet 10/100/1000Base-T e possuir fonte interna com capacidade de prover, no mínimo, 370 watts de potência. Deverá implementar Power Over Ethernet Plus (PoE+) de acordo com o padrão IEEE 802.3at simultaneamente em pelo menos 12 das 48 interfaces Ethernet 10/100/1000Base-T.

4) Todas as interfaces Ethernet 10/100/1000Base-T devem obedecer às normas técnicas IEEE802.3 (10BaseT), IEEE802.3u (100BaseTX), 802.3ab (1000BaseT) e IEEE802.3x (FlowControl).

5) Possuir porta de console para gerenciamento e configuração via linha de comando. O conector deve ser RJ-45 ou padrão RS-232 (os cabos e eventuais adaptadores necessários para acesso à porta de console devem ser fornecidos).

6) Possuir fonte de alimentação interna ao equipamento, chaveada, com ajuste automático de tensão 110 e 220 volts e operando na frequência de 60 Hz.

7) Deve ser instalável em rack padrão de 19”, sendo que deverão ser fornecidos os respectivos Kit’s de fixação.

8) Deve possuir no máximo 1 rack unit (1RU) de altura.

9) Possuir LEDs, por porta, que indiquem a integridade e atividade do link e se a porta está transmitindo ou recebendo tráfego.

10) Possuir interfaces de gerenciamento baseadas em linha de comando (CLI) e WEB browser (HTTP e HTTPS) que permita aos usuários configurar e gerenciar switches através de um browser padrão.

11) Implementar HTTP com criptografia SSL versão 3 (HTTPS) de forma a prover uma conexão segura quando o switch é configurado ou monitorado via WEB Browser.

12) Gerenciável via Telnet (com no mínimo 5 sessões simultâneas) e porta de console.

13) Devem ser implementados, no mínimo, 3 (três) níveis de privilégios de

acesso para gerenciamento do switch via Telnet, a saber:

- Nível “Administrador” ou “Super-usuário”: acesso completo e ilimitado, sendo permitidas operações de leitura e escrita sobre todo o sistema.

- Nível “Operador”: acesso com operações leitura e escrita, tendo escopo de atuação limitada a portas específicas.

- Nível “Somente Leitura”: acesso limitado à visualização de configurações, sem direitos de modificações.

14) Deve ser gerenciável via SSH versão 2 (SSHv2).

15) Devem ser implementados, para maior segurança do SSHv2, os algoritmos de criptografia: 3DES (168 bits) e AES (128, 192 e 256 bits).

16) Possuir agente de gerenciamento MIB, MIB SNMP II (RFC 1213), MIB bridging (RFC 1493), que possua descrição completa das MIBimplementada no equipamento, inclusive as extensões privadas, se existirem.

17) Deve ser gerenciável via SNMP (v1, v2 e v3).

18) Implementar nativamente 4 grupos RMON (History, Statistics, Alarms e Events) conforme RFC 1757.

19) Deve permitir o espelhamento de VLANs ou portas e de um grupo de portas - independentemente de haver ou não políticas de tráfego aplicadas a estas portas - para pelo menos duas outras portas especificadas, no mesmo switch ou não.

20) O fabricante do equipamento ofertado deve possuir ferramenta que permita gerenciar as configurações física e lógica do mesmo.

21) Implementar o protocolo Syslog para funções de “logging” de eventos.

22) Possibilidade de upgrade de software através do protocolo TFTP.

23) Deve possuir arquitetura que utilize memória Flash-EPROM para armazenamento do sistema operacional.

24) O equipamento deve vir acompanhado de manuais que contenham informações suficientes para possibilitar a instalação, configuração e operacionalização.

25) Implementar Redes Locais Virtuais (VLANs).

26) ImplementarLANs Virtuais (VLANs) conforme definições do padrão IEEE 802.1Q.

27) Implementar a criação de no mínimo 255 VLANs ativas baseadas em interfaces.

28) Deve implementarVLANs dinâmicas. Deve implementar a criação, remoção e distribuição de VLANs de forma dinâmica através de interfaces configuradas como tronco IEEE 802.1Q.

29) Implementar "VLAN Trunking" conforme padrão IEEE 802.1Q nas interfaces Gigabit Ethernet. Deve ser possível estabelecer quais VLANs serão permitidas em cada um dos troncos 802.1Q configurados.

30) Implementar a funcionalidade de "PortTrunking" conforme padrão IEEE 802.3ad.

31) Deve implementar a função de Unidirection Link Detection (UDLD) para detecção de problemas no cabeamento da rede.

32) Deve ser possível criar grupos de interfaces contendo pelo menos 08 (oito) interfaces Gigabit Ethernet (em "full duplex").

33) Deve implementar empilhamento (stack). Deve ser acompanhado das interfaces e cabos necessários para empilhamento.

34) O empilhamento deve ser feito através de interfaces e slots dedicados, não compartilhados e não deve consumir interfaces de Rede.

35) A funcionalidade de empilhamento deve possuir pelo menos as seguintes características:

- Deve implementar a criação de pelo menos 06 (seis) grupos de interfaces agregadas por stack (pilha).
- Deve ser possível empilhar pelo menos 04 (quatro) destes switches por pilha.
- O empilhamento deve ser feito em anel ("stackring") para garantir que, na eventual falha de um link, a pilha continue a funcionar.
- A pilha deverá ser gerenciada através de um único endereço IP, implementar agregação lógica de links utilizando qualquer porta da pilha além de implementar espelhamento de interfaces de qualquer porta para qualquer porta da pilha.
- Em caso de falha do switch controlador da pilha, um controlador "backup" deve ser selecionado de forma automática, sem que seja necessária intervenção manual.
- O equipamento deve implementar a configuração com um único endereço IP para gerência e administração, para uso dos protocolos: SNMP, HTTPS, SSH, Telnet, TACACS+ e RADIUS, provendo

identificação gerencial única ao equipamento de rede.

- A conexão entre os switches membros da pilha deve ser de pelo menos 20 Gbps.

- O empilhamento deverá ocorrer entre switches do mesmo tipo e entre os Tipos I, II e III;

36) Deve implementar o protocolo SpanningTree.

37) Deve implementar o Protocolo Spanning-Tree conforme padrão IEEE 802.1d.

38) Deve implementar o padrão IEEE 802.1s (“MultipleSpanningTree”).

39) Deve implementar o padrão IEEE 802.1w (“RapidSpanningTree”).

40) Implementar mecanismo de proteção da “root bridge” do algoritmo Spanning-Tree para prover defesa contra ataques do tipo “Denialof Service” no ambiente nível 2.

41) Deve implementar Per VLAN Spanning Tree.

42) Implementar funcionalidades IPv6 para gerenciamento.

43) Deve ser suportadas as funcionalidades de IPv6: Endereços de unicast, rotas estáticas, ICMP.

44) Deve ser implementado o protocolo Virtual RouterRedundancyProtocol (VRRP) ou Hot StandbyRouterProtocol (HSRP).

45) Deve ser implementado o protocolo IEEE 802.1AB Link Layer Discovery Protocol (LLDP) e sua extensão LLDP-MED, permitindo a descoberta dos elementos de rede vizinhos;

46) Deve ser implementado o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol).

47) Deve ser implementado o protocolo Telnet, conforme RFC 854. Devem ser implementados os protocolos TFTP e FTP, conforme RFC 783 e RFC 959, respectivamente.

48) Deve implementar roteamento estático.

49) Implementar roteamento de camada 3 entre VLANs (Interfaces Virtuais ou SVIs).

50) Deve possuir capacidade de comutação (switchingcapacity) de no mínimo 176 Gbpsfull duplex.

51) Possuir capacidade de processamento de pelo menos 100 Mpps (cem milhões de pacotes por segundo) considerando pacotes de 64 Bytes.

52) Possuir capacidade para no mínimo 8000 endereços MAC.

53) Ser fornecido com configuração de CPU e memória (RAM e Flash) suficiente para implementação de todas as funcionalidades descritas nesta especificação.

54) Suportar o encaminhamento de "jumbo frames" (frames de 9000 bytes) nas portas Gigabit Ethernet 10/100/1000 RJ45.

55) Implementar mecanismos de autenticação, autorização e accounting (AAA) via RADIUS e TACACS+ conforme RFCs 2138 e RFC1492 respectivamente.

56) Implementar mecanismos de AAA (Authentication, Authorization e Accounting) com garantia de entrega dos pacotes transferidos entre cliente e servidor AAA.

57) Controlar quais comandos os usuários e grupos de usuários podem executar nos equipamentos gerenciados. Devem ser registrados no servidor AAA todos os comandos executados.

58) Implementar controle de acesso por porta, usando o padrão IEEE 802.1x (PortBased Network Access Control).

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

60) Na autenticação 802.1x, deve implementar funcionalidade que designe VLAN específica para o usuário quando: a estação não tem cliente 802.1x (suplicante) ou as credenciais do usuário não estão corretas (falha de autenticação).

61) Na autenticação 802.1x, implementar associação automática de VLAN da porta do switch através da qual o usuário requisitou acesso à rede.

62) 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: identificação do usuário, porta do switch utilizada para acesso do usuário e identificação da sessão.

63) Na autenticação 802.1x, deve ser possível definir, por porta, o intervalo de tempo para obrigar o cliente a se reautenticar (reautenticação periódica).

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

65) Para equipamentos que não disponham de suplicantes 802.1x (impressoras, etc) deve ser suportado no mínimo a alocação dos mesmos em uma VLAN específica.

66) Implementar 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. Deve ser possível desabilitar a porta e enviar um trap SNMP caso algum MAC diferente tente se conectar na porta.

67) Deve ser possível estabelecer o número máximo de endereços MAC 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.

68) Implementar listas de controle de acesso (ACLs) baseadas em endereço IP de origem e destino, interfaces TCP e UDP de origem e destino e endereços MAC de origem e destino.

69) Possuir controle de broadcast, multicast e unicast por porta. Deve ser possível especificar limiares ("thresholds") individuais para tráfego tolerável de broadcast, multicast e unicast em cada porta do switch.

70) Promover análise do protocolo ARP (AddressResolutionProtocol) e possuir proteção nativa contra ataques do tipo "ARP Poisoning".

71) Deve implementar servidor DHCP.

72) Deve Implementar IGMP Snooping (v1, v2 e v3).

73) Implementar pelo menos quatro filas de saída por porta.

74) Implementar pelo menos uma fila de saída com prioridade estrita por porta e divisão ponderada de banda entre as demais filas de saída.

75) Implementar classificação, marcação e priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS).

76) Deve implementar classificação, marcação e priorização de tráfego baseada nos valores do campo "Differentiated Services Code Point" (DSCP) do cabeçalho IP, conforme definições do IETF.

77) Desejável implementar classificação de tráfego baseada em endereço IP de origem/destino, interfaces TCP e UDP de origem e destino, endereços MAC de origem e destino.

78) Implementar funcionalidades de QoS de "TrafficPolicing". Deve ser possível a especificação de banda por classe de serviço. Para os pacotes que excederem a especificação deve ser possível configurar, no mínimo, a ação de descarte do pacote.

Item 36.Serviço de Instalação do Item 35

São de responsabilidade da contratada para a execução dos Serviços de Instalação, a instalação física e a configuração lógica do equipamento conforme os requisitos, localidades e condições descritas no item “2.3)Serviços de Instalação”deste documento.

Item 37.Serviço de Manutenção e Suporte do Item 35

1) Os serviços de Suporte e Manutenção deste Item deverão ser realizados em regime 8x5xNBD (8 horas x 5 dias da semana com prazo para inicio da resolução do problema até o dia útil subsequente à abertura do chamado técnico) pelo prazo mínimo de 12 (doze) meses que deverá ser considerado na planilha de preços como valor unitário por unidade de equipamento.

2) A CONTRATANTE poderá abrir chamados de manutenção diretamente no Fabricante do Item sem necessidade de prévia consulta e/ou qualquer liberação por parte da CONTRATADA.

3) Deverá ser garantido à CONTRATANTE o pleno acesso ao site do Fabricante dos equipamentos e softwares. Esse acesso deve permitir consultas a quaisquer bases de dados disponíveis para usuários relacionadas aos equipamentos e softwares especificados, além de permitir downloads de quaisquer atualizações de software ou documentação deste produto.

Item 38.Switch de Acesso Tipo III

1) Fornecimento de Switch de Acesso Tipo III 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.

2) O modelo ofertado deve ser do mesmo fabricante do Item “Switch Core” descrito neste Termo de Referência;

3) Possuir no mínimo um total de 50 (cinquenta) interfaces de rede dedicadas e não compartilhadas, sem uso de interfaces tipo "combo". Estas interfaces devem ser divididas da seguinte forma:

- Possuir, no mínimo, 2 (duas) interfaces ópticas dedicadas e não compartilhadas padrão 10GBaseX 10Gigabit Ethernet, Full-duplex, baseadas em conectores ópticos (transceivers) padrão SFP+. Deverá ter capacidade para aceitar conectores ópticos dos padrões 10GBaseSR, 10GBaseLR e 10GBaseER.

- Possuir, no mínimo, 48 (quarenta e oito) interfaces dedicadas e não compartilhadas padrão Gigabit Ethernet 10/100/1000Base-T de 10/100/1000 Mbps, Full duplex, conector RJ-45 e com autosensing de velocidade. Estas portas não podem ser compartilhadas com slots utilizados para portas de uplink ou de empilhamento.

- Implementar o padrão PoE (Power over Ethernet) IEEE 802.3af simultaneamente em todas as interfaces Ethernet 10/100/1000Base-T e possuir fonte interna com capacidade de prover, no mínimo, 740 watts de potência. Deverá implementar Power Over Ethernet Plus (PoE+) de acordo com o padrão IEEE 802.3at simultaneamente em pelo menos 24 das 48 interfaces Ethernet 10/100/1000Base-T.

4) Todas as interfaces Ethernet 10/100/1000Base-T devem obedecer às normas técnicas IEEE802.3 (10BaseT), IEEE802.3u (100BaseTX), 802.3ab (1000BaseT) e IEEE802.3x (FlowControl).

5) Possuir porta de console para gerenciamento e configuração via linha de comando. O conector deve ser RJ-45 ou padrão RS-232 (os cabos e eventuais adaptadores necessários para acesso à porta de console devem ser fornecidos).

6) Possuir fonte de alimentação interna ao equipamento, chaveada, com ajuste automático de tensão 110 e 220 volts e operando na frequência de 60 Hz.

7) Deve ser instalável em rack padrão de 19", sendo que deverão ser fornecidos os respectivos Kit's de fixação.

8) Deve possuir no máximo 1 rack unit (1RU) de altura.

9) Possuir LEDs, por porta, que indiquem a integridade e atividade do link e se a porta está transmitindo ou recebendo tráfego.

10) Possuir interfaces de gerenciamento baseadas em linha de comando (CLI) e WEB browser (HTTP e HTTPS) que permita aos usuários configurar e gerenciar switches através de um browser padrão.

11) Implementar HTTP com criptografia SSL versão 3 (HTTPS) de forma a prover uma conexão segura quando o switch é configurado ou monitorado via WEB Browser.

12) Gerenciável via Telnet (com no mínimo 5 sessões simultâneas) e porta de console.

13) Devem ser implementados, no mínimo, 3 (três) níveis de privilégios de acesso para gerenciamento do switch via Telnet, a saber:

- Nível "Administrador" ou "Super-usuário": acesso completo e ilimitado, sendo permitidas operações de leitura e escrita sobre todo o sistema.

- Nível "Operador": acesso com operações leitura e escrita, tendo escopo de atuação limitada a portas específicas.

- Nível "Somente Leitura": acesso limitado à visualização de configurações, sem direitos de modificações.

14) Deve ser gerenciável via SSH versão 2 (SSHv2).

15) Devem ser implementados, para maior segurança do SSHv2, os algoritmos de criptografia: 3DES (168 bits) e AES (128, 192 e 256 bits).

16) Possuir agente de gerenciamento MIB, MIB SNMP II (RFC 1213), MIB bridging (RFC 1493), que possua descrição completa das MIBimplementadano equipamento, inclusive as extensões privadas, se existirem.

17) Deve ser gerenciável via SNMP (v1, v2 e v3).

18) Implementar nativamente 4 grupos RMON (History, Statistics, Alarms e Events) conforme RFC 1757.

19) Deve permitir o espelhamento de VLANs ou portas e de um grupo de portas - independentemente de haver ou não política de tráfego aplicadas a estas portas - para pelo menos duas outras portas especificadas, no mesmo switch ou não.

20) O fabricante do equipamento ofertado deve possuir ferramenta que permita gerenciar as configurações física e lógica do mesmo.

21) Implementar o protocolo Syslog para funções de “logging” de eventos.

22) Possibilidade de upgrade de software através do protocolo TFTP.

23) Deve possuir arquitetura que utilize memória Flash-EPROM para armazenamento do sistema operacional.

24) O equipamento deve vir acompanhado de manuais que contenham informações suficientes para possibilitar a instalação, configuração e operacionalização.

25) Implementar Redes Locais Virtuais (VLANs).

26) ImplementarLANs Virtuais (VLANs) conforme definições do padrão IEEE 802.1Q.

27) Implementar a criação de no mínimo 255 VLANs ativas baseadas em interfaces.

28) Deve implementarVLANs dinâmicas. Deve implementar a criação, remoção e distribuição de VLANs de forma dinâmica através de interfaces configuradas como tronco IEEE 802.1Q.

29) Implementar “VLAN Trunking” conforme padrão IEEE 802.1Q nas interfaces Gigabit Ethernet. Deve ser possível estabelecer quais VLANs serão permitidas em cada um dos troncos 802.1Q configurados.

30) Implementar a funcionalidade de “PortTrunking” conforme padrão IEEE

802.3ad.

31) Deve implementar a função de Unidirection Link Detection (UDLD) para detecção de problemas no cabeamento da rede.

32) Deve ser possível criar grupos de interfaces contendo pelo menos 08 (oito) interfaces Gigabit Ethernet (em “full duplex”).

33) Deve implementar empilhamento (stack). Deve ser acompanhado das interfaces e cabos necessários para empilhamento.

34) O empilhamento deve ser feito através de interfaces e slots dedicados, não compartilhados e não deve consumir interfaces de Rede.

35) A funcionalidade de empilhamento deve possuir pelo menos as seguintes características:

- Deve implementar a criação de pelo menos 06 (seis) grupos de interfaces agregadas por stack (pilha).
- Deve ser possível empilhar pelo menos 04 (quatro) destes switches por pilha.
- O empilhamento deve ser feito em anel (“stackring”) para garantir que, na eventual falha de um link, a pilha continue a funcionar.
- A pilha deverá ser gerenciada através de um único endereço IP, implementar agregação lógica de links utilizando qualquer porta da pilha além de implementar espelhamento de interfaces de qualquer porta para qualquer porta da pilha.
- Em caso de falha do switch controlador da pilha, um controlador “backup” deve ser selecionado de forma automática, sem que seja necessária intervenção manual.
- O equipamento deve implementar a configuração com um único endereço IP para gerência e administração, para uso dos protocolos: SNMP, HTTPS, SSH, Telnet, TACACS+ e RADIUS, provendo identificação gerencial única ao equipamento de rede.
- A conexão entre os switches membros da pilha deve ser de pelo menos 20 Gbps.
- O empilhamento deverá ocorrer entre switches do mesmo tipo e entre os Tipos I, II e III.

36) Deve implementar o protocolo Spanning-Tree.

37) Deve implementar o Protocolo Spanning-Tree conforme padrão IEEE

802.1d.

38) Deve implementar o padrão IEEE 802.1s (“MultipleSpanningTree”).

39) Deve implementar o padrão IEEE 802.1w (“RapidSpanningTree”).

40) Implementar mecanismo de proteção da “root bridge” do algoritmo Spanning-Tree para prover defesa contra ataques do tipo “Denialof Service” no ambiente nível 2.

41) Deve implementar Per VLAN Spanning Tree.

42) Implementar funcionalidades IPv6 para gerenciamento.

43) Deve ser suportadas as funcionalidades de IPv6: Endereços de unicast, rotas estáticas, ICMP.

44) Deve ser implementado o protocolo Virtual RouterRedundancyProtocol (VRRP) ou Hot StandbyRouterProtocol (HSRP).

45) Deve ser implementado o protocolo IEEE 802.1AB Link Layer Discovery Protocol (LLDP) e sua extensão LLDP-MED, permitindo a descoberta dos elementos de rede vizinhos;

46) Deve ser implementado o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol).

47) Deve ser implementado o protocolo Telnet, conforme RFC 854. Devem ser implementados os protocolos TFTP e FTP, conforme RFC 783 e RFC 959, respectivamente.

48) Deve implementar roteamento estático.

49) Implementar roteamento de camada 3 entre VLANs (Interfaces Virtuais ou SVIs).

50) Deve possuir capacidade de comutação (switchingcapacity) de no mínimo 176 Gbpsfull duplex.

51) Possuir capacidade de processamento de pelo menos 100 Mpps (cem milhões de pacotes por segundo) considerando pacotes de 64 Bytes.

52) Possuir capacidade para no mínimo 8000 endereços MAC.

53) Ser fornecido com configuração de CPU e memória (RAM e Flash) suficiente para implementação de todas as funcionalidades descritas nesta especificação.

54) Suportar o encaminhamento de “jumbo frames” (frames de 9000 bytes) nas portas Gigabit Ethernet 10/100/1000 RJ45.

55) Implementar mecanismos de autenticação, autorização e accounting (AAA) via RADIUS e TACACS+ conforme RFCs 2138 e RFC1492 respectivamente.

56) Implementar mecanismos de AAA (Authentication, Authorization e Accounting) com garantia de entrega dos pacotes transferidos entre cliente e servidor AAA.

57) Controlar quais comandos os usuários e grupos de usuários podem executar nos equipamentos gerenciados. Devem ser registrados no servidor AAA todos os comandos executados.

58) Implementar controle de acesso por porta, usando o padrão IEEE 802.1x (PortBased Network Access Control).

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

60) Na autenticação 802.1x, deve implementar funcionalidade que designe VLAN específica para o usuário quando: a estação não tem cliente 802.1x (suplicante) ou as credenciais do usuário não estão corretas (falha de autenticação).

61) Na autenticação 802.1x, implementar associação automática de VLAN da porta do switch através da qual o usuário requisitou acesso à rede.

62) 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: identificação do usuário, porta do switch utilizada para acesso do usuário e identificação da sessão.

63) Na autenticação 802.1x, deve ser possível definir, por porta, o intervalo de tempo para obrigar o cliente a se reautenticar (reautenticação periódica).

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

65) Para equipamentos que não disponham de suplicantes 802.1x (impressoras, etc) deve ser suportado no mínimo a alocação dos mesmos em uma VLAN específica.

66) Implementar 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. Deve ser possível desabilitar a porta e enviar um trap SNMP caso algum MAC diferente tente se conectar na porta.

67) Deve ser possível estabelecer o número máximo de endereços MAC 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.

68) Implementar listas de controle de acesso (ACLs) baseadas em endereço IP de origem e destino, interfaces TCP e UDP de origem e destino e endereços MAC de origem e destino.

69) Possuir controle de broadcast, multicast e unicast por porta. Deve ser possível especificar limiares (“thresholds”) individuais para tráfego tolerável de broadcast, multicast e unicast em cada porta do switch.

70) Promover análise do protocolo ARP (AddressResolutionProtocol) e possuir proteção nativa contra ataques do tipo “ARP Poisoning”.

71) Deve implementar servidor DHCP.

72) Deve Implementar IGMP Snooping (v1, v2 e v3).

73) Implementar pelo menos quatro filas de saída por porta.

74) Implementar pelo menos uma fila de saída com prioridade estrita por porta e divisão ponderada de banda entre as demais filas de saída.

75) Implementar classificação, marcação e priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS).

76) Deve implementar classificação, marcação e priorização de tráfego baseada nos valores do campo “Differentiated Services Code Point” (DSCP) do cabeçalho IP, conforme definições do IETF.

77) Desejável implementar classificação de tráfego baseada em endereço IP de origem/destino, interfaces TCP e UDP de origem e destino, endereços MAC de origem e destino.

78) Implementar funcionalidades de QoSde“TrafficPolicing”. Deve ser possível a especificação de banda por classe de serviço. Para os pacotes que excederem a especificação deve ser possível configurar, no mínimo, a ação de descarte do pacote.

Item 39. Serviço de Instalação do Item 38

São de responsabilidade da contratada para a execução dos Serviços de Instalação, a instalação física e a configuração lógica do equipamento conforme os requisitos, localidades e condições descritas no item “2.3)Serviços de Instalação”deste documento.

Item 40.Serviço de Manutenção e Suporte do Item 38

1) Os serviços de Suporte e Manutenção deste Item deverão ser realizados em regime 8x5xNBD (8 horas x 5 dias da semana com prazo para inicio da resolução do problema até o dia útil subsequente à abertura do chamado

técnico) pelo prazo mínimo de 12 (doze) meses que deverá ser considerado na planilha de preços como valor unitário por unidade de equipamento.

2) A CONTRATANTE poderá abrir chamados de manutenção diretamente no Fabricante do Item sem necessidade de prévia consulta e/ou qualquer liberação por parte da CONTRATADA.

3) Deverá ser garantido à CONTRATANTE o pleno acesso ao site do Fabricante dos equipamentos e softwares. Esse acesso deve permitir consultas a quaisquer bases de dados disponíveis para usuários relacionadas aos equipamentos e softwares especificados, além de permitir downloads de quaisquer atualizações de software ou documentação deste produto.

Item 41.Switch Core

1) Fornecimento de Switch Core 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.

2) O modelo ofertado deve ser do mesmo fabricante dos itens 32, 35 e 38, descritos neste Termo de Referência.

3) Switch Core de Rede do tipo Chassis Modular.

4) Possuir, no mínimo, 09 (nove) slots para a inserção de módulos.

5) Possuir módulo de supervisão. O módulo de controle/supervisão deve suportar sozinho o controle da operação de todos os módulos de interface do switch em capacidade máxima.

6) Quando utilizando módulos Supervisores redundantes, deve:

- Implementar sincronismo entre informações de nível 2 contidas nos processadores e supervisores de modo que na perda de um processador ou supervisor primário não seja necessário reboot dos módulos de interfaces.

- Implementar sincronismo entre informações de nível 3, protocolos de roteamento, contidas nos processadores e supervisores, de modo que na perda de um processador ou supervisor primário não ocorra reconvergência

- O tempo máximo de “failover” (tempo para que o processador/supervisor secundário assuma todas as funções do primário) não pode ser superior a 8 segundos.

- Cada módulo de controle/supervisão deve suportar sozinho o controle da operação de todos os módulos de interface do switch em capacidade máxima.

- No caso de utilização de duas supervisoras, não deve haver perda de performance no equipamento em caso de falha de uma delas.

- Deve ser suportada a redundância de todas as funcionalidades de níveis 2, 3 e 4;

7) Deve possuir, no mínimo, 16 portas 10 Gigabit Ethernet 10GBase-X, padrão SFP+, XENPAK ou X2 para conectores SC ou LC.

8) Deverá possuir no mínimo 48 portas 10/100/1000Base-T, com conectores RJ45 e com autosensing de velocidade, distribuídos em, no máximo, 2 módulos de interface.

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

10) Possuir capacidade de associação das portas 10/100/1000 e 1000Base-SX, no mínimo, em grupo de 8 (oito) portas, formando uma única interface lógica com as mesmas facilidades das interfaces originais, compatível com a norma IEEE 802.3ad.

11) Deverá possuir, no mínimo, 24 portas 1000Base-X Gigabit ethernet, full-duplex, padrão SFP ou GBIC, para fibras óticas multimodo em, no máximo, 1 módulos de interface.

12) Permitir a agregação de portas que residam em módulos diferentes do switch

13) A conexão do módulo de interface com a switchingfabric deverá ser de, no mínimo, 80 Gbps para cada módulo de interfaces de 10Gbps;

14) A conexão do módulo de interface com a switchingfabric deverá ser de, no mínimo, 40 Gbps para cada módulo de interfaces de 1Gbps;

15) Suportar capacidade de encaminhamento de pacotes nas camadas 2, 3 e 4 do modelo OSI com capacidade de encaminhamento de pacotes em nível 3 de, no mínimo, 490 milhões de PPS (Mpps) em IPv4.

16) Todos os módulos ofertados devem utilizar a tecnologia que permita Switching/Routing local nos módulos Gigabit, sem que seja necessário o tráfego ir até o Switch Fabric caso as portas origem e destino estejam localizadas no mesmo módulo/slot. É permitido apenas que os primeiros pacotes do fluxo vão até o switch fabric para estabelecimento do fast-path local no módulo

17) Suportar a atualização do sistema operacional com o switch em operação.

18) Suportar capacidade de switchingfabric de, no mínimo, 1.400 (mil e quatrocentos) Gbps.

19) O módulo de controle/supervisão deve ser fornecido com no mínimo 1 (um) cartão de memória flash (PCMCIA, ATA PCMCIA ou Compact Flash) de no mínimo 1 GBytes cada.

20) Ser fornecido com configuração de CPU e memória (RAM e Flash) suficiente para implementação de todas as funcionalidades descritas nesta especificação.

21) Permitir endereçamento de no mínimo de 128.000 (cento e vinte e oito mil) endereços MAC, os quais deverão ser armazenados em uma única tabela.

22) Possuir Leds indicativos de atividade por porta.

23) Permitir a montagem em rack padrão de 19 polegadas, devendo ser fornecido o kit de fixação.

24) Possuir fonte de alimentação com as seguintes características:

- Interna ao equipamento.
- Chaveada.
- Capaz de sustentar a operação do equipamento com todos os slots ocupados por módulos ativos.
- Implementar redundância de alimentação elétrica através de uma segunda fonte de alimentação (1+1). A segunda fonte deve ser fornecida.
- Deve possuir fontes de alimentação redundantes com duas conexões de eletricidade diferentes.
- Suportar balanceamento de carga entre as fontes de alimentação redundantes.
- As fontes devem ser dimensionadas para permitir o completo funcionamento do switch com apenas 1 (uma) fonte.
- As fontes de alimentação deverão operar em tensões 100-240 V e frequência de 50/60 Hz.

25) Funcionalidades de camada 2 (vlan, spanning tree):

- Implementar LAN Virtual (VLAN) padrão IEEE 802.1Q.
- Permitir a criação de no mínimo 4.000 VLANs ativas baseadas em portas.
- Suportar a criação de VLANs baseadas em endereços MAC.

- Permitir a criação de subgrupos dentro de uma mesma VLAN com conceito de portas isoladas e portas "promíscuas", onde portas isoladas não se comunicam com outras portas isoladas, mas apenas com as portas promíscuas de uma dada VLAN.

- Deve permitir a criação, remoção e distribuição de VLANs de forma dinâmica através de portas configuradas como tronco IEEE 802.1Q.

- 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 "VLAN Trunking" padrão IEEE 802.1Q nas portas Fast Ethernet e Gigabit Ethernet.

- Deve ser possível estabelecer quais VLANs serão permitidas em cada um dos troncos configurados.

- Implementar a funcionalidade de "PortTrunking" conforme padrão IEEE 802.3ad.

- Deve ser possível criar grupos de portas contendo pelo menos 8 portas Fast Ethernet (em "full duplex").

- Deve ser possível criar grupos de portas contendo pelo menos 8 portas Gigabit Ethernet (em "full duplex").

- Deve ser possível criar grupos de portas contendo pelo menos 8 portas 10 Gigabit Ethernet (em "full duplex").

- Deve ser possível agregar portas que residem em módulos diferentes do switch.

- Deve permitir a criação de pelo menos 128 grupos de portas agregadas.

- Implementar o Protocolo Spanning-Tree (IEEE 802.1d).

- Implementar o padrão IEEE 802.1s ("MultipleSpanning-Tree"), com suporte a no mínimo 64 (sessenta e quatro) instâncias simultâneas do protocolo Spanning-Tree.

- Implementar o padrão IEEE 802.1w ("RapidSpanning-Tree").

- Implementar mecanismo de proteção da "root bridge" do algoritmo Spanning-Tree para prover defesa contra ataques do tipo "Denialof Service" no ambiente nível 2. Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo "fastforwarding" (conforme previsto no

padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente.

- O equipamento deverá permitir a detecção automática de falhas em conexões físicas, como rompimento de cabeamento, tanto de fibras ópticas quanto de pares-trançados, evitando o descarte "silencioso" de pacotes e loops em topologias de spanning-tree, ocasionados por links unidirecionais. A porta que recebe o cabeamento danificado será colocada em estado inativo e o equipamento enviará uma notificação.

- O equipamento deve responder a pacotes de testes para teste da implementação dos níveis de serviço especificados (SLA). Devem ser suportadas no mínimo as seguintes operações de teste:

  - ICMP echo;

  - TCP connect (em qualquer porta TCP do intervalo 1-50000 que o administradorespecifique);

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

  - O equipamento deve suportar pelo menos cinco destas operações de testes simultaneamente.

26) Quanto ao “Internet Protocol”versão 6 (IPv6), a solução deve:

- Implementar IPv6.

- Permitir a configuração de endereços IPv6 para gerenciamento.

- Permitir consultas de DNS com resolução de nomes em endereços IPv6.

- Implementar ICMPv6 com as seguintes funcionalidades:

  - ICMP request;

  - ICMP Reply;

  - ICMP Neighbor Discovery Protocol (NDP) ;

  - ICMPMTU Discovery;

- 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.

27) Quanto à qualidade de serviço, a solução deve:

- Implementar pelo menos 4 (quatro) filas de saída (hardware) por porta nos módulos de interface Gigabit Ethernet.

- Implementar pelo menos 8 (oito) filas de saída (hardware) por porta nos módulos de interface 10 Gigabit Ethernet.

- Suporte a uma fila com prioridade estrita (prioridade absoluta em relação às demais classes dentro do limite de banda que lhe foi atribuído) para tratamento do tráfego "real-time" (voz e vídeo).

- Implementar classificação, marcação e priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS).

- Implementar classificação, marcação e priorização de tráfego baseada nos valores do campo "Differentiated Services Code Point" (DSCP) do cabeçalho IP, conforme definições do IETF.

- Implementar classificação de tráfego baseada em endereço IP de origem/destino, portas TCP e UDP de origem e destino, endereços MAC de origem e destino.

- Implementar funcionalidades de QoS de "TrafficShaping" e "TrafficPolicing".

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

- Suportar diferenciação de QoS por VLAN.

28) Funcionalidades de gerência:

- Possuir interface de configuração via linha de comando para todos os módulos do switch.

- Possuir ferramentas de gerência com interface gráfica GUI para os módulos do switch.

- Possuir interface de gerenciamento baseada em Web (HTTP) que permita aos usuários configurar e gerenciar switches através de um browser padrão.

- Ser configurável e gerenciável via GUI (Graphical User Interface),

CLI (Command Line Interface), SNMP, Telnet, SSH, HTTP e HTTPS com, no mínimo, 5 sessões simultâneas e independentes.

- Deve permitir a transferência segura de arquivos para o equipamento através do protocolo SCP (SecureCopy) utilizando um cliente padrão ou SFTP (Secure FTP).

- 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) utilizando algoritmo de criptografia AES.

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

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

- Possuir porta de console para gerenciamento e configuração via linha de comando com conector RJ-45 ou conector padrão RS-232 com respectivo adaptador para conector RJ-45.

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

- Suportar com a utilização de probes externas (não é necessário o fornecimento das probes) todos os 9 grupos de RMON (History, Statistics, Alarms, Events, Matrix, Filter, Hosts, Hosts TopN e Capture) conforme RFC 2021;

- Suportar protocolo de coleta de informações de fluxos que circulam pelo equipamento contemplando no mínimo as seguintes informações:

    - IP de origem/destino,

    - Parâmetro “protocoltype”docabeçalho IP,

    - Porta TCP/UDP de origem/destino,

    - Campo TOS do cabeçalho IP,

- Interface de entrada do tráfego,

- A informação coletada deve ser automaticamente exportável em intervalos pré-definidos através de um protocolo IPFIX (IP FlowInformationExport) padronizado.

- Deve suportar a instalação de módulos internos de forma a prover serviços de:

  - Firewall;

  - VPN;

  - Controle de Pontos de Acesso WiFi;

- 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.

- Permitir o espelhamento da totalidade do tráfego de uma porta, de um grupo de portas e deVLANs 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.

- Deve ser possível espelhar o tráfego de portas que residem em um dado módulo para uma porta que reside em módulo diferente do switch.

- Devem ser suportadas pelo menos duas sessões simultâneas de espelhamento.

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

- Implementar o protocolo Syslog para funções de “logging” de eventos.

- Possuir armazenamento interno das mensagens de log geradas pelo equipamento de no mínimo 2.048 bytes.

- Possuir agente de gerenciamento SNMP, MIB I e MIB II, que possua descrição completa da MIB implementada no equipamento, inclusive as extensões privadas, se existirem.

- Possibilidade de upgrade de software através do protocolo TFTP.

- Implementar o protocolo NTPv3 (Network Time Protocol, versão 3).

- Deve ser suportada autenticação entre os peers, conforme definição da RFC 1305.

- Implementar DHCP Relay e DHCP Server em múltiplas VLANs.

- Implementar o protocolo VRRP ou mecanismo similar de redundância de gateway.

- Possuir suporte ao protocolo GRE (GenericRoutingEncapsulation), conforme RFCs 1701 e 1702.

- Permitir o armazenamento de sua configuração em memória não volátil, podendo, em uma queda e posterior restabelecimento da alimentação, voltar àoperação 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.

- O switch deve poder implementar, a criação de templates que agrupariam dois ou mais comandos existentes na CLI do switch, para fins de administração e padronização das configurações do equipamento. Depois de terem sido criadas as templates, essas devem ser implementadas a uma interface ou a um grupo de interfaces do switch.

- Deve ser fornecido com modulo de controle/supervisão, que permita a implementação de um cluster entre dois chassis idênticos, com as seguintes características:

  - Todas as funções de controle, como protocolos de gerencia e cálculos de protocolos nível 2 e 3 devem ser feitas pelo switch ativo do cluster;

  - Todas as funções de comutação de dados devem ser feita pelos dois switches do cluster, duplicando o desempenho de comutação de pacotes do switch.

  - Para a conexão dos switches no cluster deveram ser utilizadas no mínimo 2 (duas) interfaces de 10 Gigabits entre os dois switches presentes no modulo de controle/supervisão;

  - Deverá permitir a configuração de MultichassisEtherchannel entre um switch de acesso e os 2 (dois) switches do cluster, de forma que o switch de acesso tenha um único link lógico com os dois switches que formam o cluster;

- Deverá ser gerenciado como um único switch virtual;

- Deve implementar mecanismo de alta disponibilidade, onde em caso de falha de uma placa supervisora do cluster o segundo switch possa assumir todas as suas funções de nível 3 e gerência sem que haja parada do tráfego, ou recálculo das rotas nível 3.

- Caso o equipamento ofertado não implemente as funcionalidades que permitam a implementação de um cluster entre dois chassis idênticos, conforme descrito anteriormente, cada equipamento ofertado deve ser fornecido com módulos de controle/supervisão redundantes.

29) Quanto às funcionalidades de segurança, a solução deve:

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

- 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.

- Possuir suporte a protocolo de autenticação para controle do acesso administrativo ao equipamento que possua pelo menos as seguintes características:

  - Implementar mecanismos de AAA (Authentication, Authorization e Accounting) com garantia de entrega dos pacotes transferidos entre cliente e servidor AAA.

  - Criptografar todos os pacotes enviados ao servidor de controle de acesso e não só os pacotes referentes à senha.

  - Permitir controlar quais comandos os usuários e grupos de usuários podem executar nos equipamentos gerenciados. Devem ser registrados no servidor AAA todos os comandos executados, assim como todas as tentativas de execução de comandos não autorizadas feitas por usuários que tiverem acesso ao equipamento gerenciado.

  - Utilize o protocolo TCP para prover maior confiabilidade ao tráfego dos pacotes envolvidos no controle administrativo.

  - Deve haver autenticação mútua entre o servidor AAA e o cliente AAA.

- Implementar controle de acesso por porta (IEEE 802.1x).

- 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 802.1x via endereço MAC em substituição à identificação de usuário, para equipamentos que não disponham de suplicantes.
- Suportar a configuração de 802.1x utilizando autenticação via usuário e MAC simultaneamente na mesma porta do switch.
- Deve suportar a autenticação 802.1x através dos protocolos EAP-MD5, PEAP e EAP-TLS.
- Implementar serviço de DHCP Server em múltiplas VLANS simultaneamente, para que possa atribuir endereços IP aos clientes 802.1x autenticados e autorizados.
- Deve ser suportada a autenticação de múltiplos usuários em uma mesma porta.
- Deve ter tratamento de autenticação 802.1x diferenciado entre “VoiceVLAN” e “Data LAN”, na mesma porta para que um erro de autenticação em uma VLAN não interfira na outra.
- Deve ser suportada a atribuição de autenticação através do navegador (Web Authentication) caso a máquina que esteja utilizando para acesso à Rede não tenha cliente 802.1x operacional, o portal de autenticação local do switch deve utilizar protocolo seguro tal como

HTTPS.

- 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. Deve ser possível desabilitar a porta e enviar um trap SNMP caso algum MAC diferente teste se conectar à porta.

- Deve ser possível estabelecer o número máximo de endereços MAC 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 filtragem de pacotes (ACL - Access ControlList) para IPv4 e IPv6

- Implementar listas de controle de acesso (ACLs) baseadas em endereço IP de origem e destino, portas TCP e UDP de origem e destino e endereços MAC de origem e destino.

- Possuir controle de broadcast, multicast e unicast por porta. Deve ser possível especificar limiares (“thresholds”) individuais para tráfego tolerável de broadcast, multicast e unicast em cada porta do switch. Excedidos os valores pré-configurados deve ser possível enviar um trap SNMP e desabilitar a porta.

- Promover 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.

- O switch deve ter capacidade de realizar a análise granular de mensagens DHCP evitando que servidores DHCP não aprovados façam a entrega de endereçamento IP na rede. Basicamente as portas do switch definidas como “untrusted” não devem realizar a entrega de respostas reservadas de DHCP.

- O switch deve ter capacidade de realizar a análise granular de mensagens DHCP certificando de que o endereço MAC de origem e a informação de payload do DHCP coincidem a fim de evitar ataques do tipo DHCP Starvation.

- O switch deve ter a capacidade de registrar as informações de bind de DHCP atribuídas às portas untrusted que adquiriram o endereçamento IP com sucesso. Entre as informações registradas devem constar pelo menos o endereço IP, o MAC address, tamanho de lease, porta e VLAN.

- O switch deve possuir mecanismos que permitam a inspecção

dinâmica de todos os ARPrequests e replies (gratuitos ou não-gratuitos) vindos de portas classificadas como “untrusted” para assegurar e certificar que estas requisições e respostas pertencem realmente ao ARP owner, ou seja são pertecentes a porta que tem um DHCP binding e está em conformidade com o endereço IP contido no ARP reply evitando ataques baseados em ARP.

- Promover análise do protocolo ARP (AddressResolutionProtocol) e possuir proteção nativa contra ataques do tipo “ARP Poisoning”.

30) Funcionalidades de Camada 3 (multicast e roteamento) e roteamento IPv6:

- Implementar IP multicast.
- Implementar roteamento multicast PIM (ProtocolIndependentMulticast) nos modos “sparse-mode” (RFC 2362) e “dense-mode”.
- Implementar o protocolo IGMP v1, v2 e v3.
- Implementar em todas as interfaces do switch o protocolo IGMP Snooping (v1, v2, v3) conforme as RFC’s 1112 e 2236.
- Implementar em todas as interfaces do switch o protocolo MLD (MultcastListener Discovery) snooping (v1 e v2) para IPv6.
- Possuir roteamento nível 3 entre VLANs.
- Implementar roteamento estático.
- Implementar os protocolos de roteamento RIPv1 (RFC 1058) e RIPv2 (RFC 2453).
- Implementar protocolo de roteamento dinâmico OSPF (RFC 2328, 1587, 1765 e 2370).
- Implementar protocolo de roteamento BGPv4 (RFC 1771, 1965, 1997, 1745, 2385).
- Implementar mecanismo de segurança dos protocolos OSPF e BGP permitindo a autenticação mútua entre peers BGP e OSPF.
- Permitir o roteamento nível 3 entre VLANs.
- Implementar o protocolo VRRP (RFC 2338) ou mecanismo similar de redundância de gateway.
- Suportar resolução de nomes por DNS (“Domain Name System”).

- Suportar roteamento estático para IPv6.
- Suportar roteamento dinâmico RIPng para IPv6.
- Suportar protocolo de roteamento dinâmico OSPFv3 para IPv6.
- Suportar o protocolo VRRP (RFC 2338) ou mecanismo similar de redundância de gateway para IPv6.
- Suportar, no mínimo, 255 grupos VRRP ou de mecanismo similar de redundância de gateway simultaneamente, para IPv6.

Item 42. Serviço de Instalação do Item 41

São de responsabilidade da contratada para a execução dos Serviços de Instalação, a instalação física e a configuração lógica do equipamento conforme os requisitos, localidades e condições descritas no item "2.3)Serviços de Instalação"deste documento.

Item 43.Serviço de Manutenção e Suporte do Item 41

1) Os serviços de Suporte e Manutenção deste Item deverão ser realizados em regime 24x7x4 (24 horas x 7 dias da semana com prazo para inicio da resolução do problema até 04 horas subsequentes à abertura do chamado técnico) pelo prazo mínimo de 12 (doze) meses que deverá ser considerado na planilha de preços como valor unitário por unidade de equipamento.

2) A CONTRATANTE poderá abrir chamados de manutenção diretamente no Fabricante do Item sem necessidade de prévia consulta e/ou qualquer liberação por parte da CONTRATADA.

3) Deverá ser garantido à CONTRATANTE o pleno acesso ao site do Fabricante dos equipamentos e softwares. Esse acesso deve permitir consultas a quaisquer bases de dados disponíveis para usuários relacionadas aos equipamentos e softwares especificados, além de permitir downloads de quaisquer atualizações de software ou documentação deste produto.

Item 44. Conector Óptico Tipo I

1) Fornecimento de Conector Óptico Tipo I 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.

2) Interface óptica (transceiver)10Gigabit Ethernet 10Base-SR, para fibra óptica multimodo, com conector LC ou SC, segundo o padrão IEEE 802.3ae;

3) Compatível com os "Switches de Acesso" especificados neste termo de referência. A compatibilidade deve ser assegurada por declaração do fabricante dos switches ou através de comprovação diretamente no sítio do fabricante;

4) Todos os componentes de hardware necessários para instalação nos switches deverão ser fornecidos;

5) Acompanhar cordão óptico duplo, com terminações SC do lado da conexão com o DIO, de 2,5 metros.As extremidades do cordão óptico deverão ser conectorizadas e testadas de fábrica.

Item 45.Serviço de Instalação do Item 44

São de responsabilidade da contratada para a execução dos Serviços de Instalação, a instalação física e a configuração lógica do equipamento conforme os requisitos, localidades e condições descritas no item “2.3)Serviços de Instalação”deste documento.

Item 46. Conector Óptico Tipo II

1) Fornecimento de Conector Óptico Tipo II 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.

2) Interface óptica (transceiver)10Gigabit Ethernet 10Base-LR, para fibra óptica multimodo, com conector LC ou SC, segundo o padrão IEEE 802.3ae.

3) Compatível com os “Switches de Acesso” especificados neste termo de referência. A compatibilidade deve ser assegurada por declaração do fabricante dos switches ou através de comprovação diretamente no sítio do fabricante.

4) Todos os componentes de hardware necessários para instalação nos switches deverão ser fornecidos.

5) Acompanhar cordão óptico duplo, com terminações SC do lado da conexão com o DIO, de 2,5 metros.As extremidades do cordão óptico deverão ser conectorizadas e testadas de fábrica.

Item 47. Serviço de Instalação do Item 46

São de responsabilidade da contratada para a execução dos Serviços de Instalação, a instalação física e a configuração lógica do equipamento conforme os requisitos, localidades e condições descritas no item “2.3)Serviços de Instalação”deste documento.

Item 48. Conector Óptico Tipo III

1) Fornecimento de Conector Óptico Tipo III 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.

2) Interface óptica (transceiver)10Gigabit Ethernet 10Base-SR, para fibra óptica multimodo, com conector SC ou SC, segundo o padrão IEEE 802.3ae.

3) Compatível com o “SwitchCore” especificadoneste termo de referência. A compatibilidade deve ser assegurada por declaração do fabricante dos switches ou através de comprovação diretamente no sítio do fabricante.

4) Todos os componentes de hardware necessários para instalação nos switches deverão ser fornecidos.

5) Acompanhar cordão óptico duplo, com terminações SC do lado da conexão com o DIO, de 2,5 metros.As extremidades do cordão óptico deverão ser conectorizadas e testadas de fábrica.

Item 49.Serviço de Instalação do Item 48

São de responsabilidade da contratada para a execução dos Serviços de Instalação, a instalação física e a configuração lógica do equipamento conforme os requisitos, localidades e condições descritas no item “2.3)Serviços de Instalação”deste documento.

Item 50. Conector Óptico Tipo IV

1) Fornecimento de Conector Óptico Tipo IV 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.

2) Interface óptica (transceiver)10Gigabit Ethernet 10Base-LR, para fibra óptica multimodo, com conector LC ou SC, segundo o padrão IEEE 802.3ae.

3) Compatível com os “SwitchCore” especificadoneste termo de referência. A compatibilidade deve ser assegurada por declaração do fabricante dos switches ou através de comprovação diretamente no sítio do fabricante.

4) Todos os componentes de hardware necessários para instalação nos switches deverão ser fornecidos.

5) Acompanhar cordão óptico duplo, com terminações SC do lado da conexão com o DIO, de 2,5 metros.As extremidades do cordão óptico deverão ser conectorizadas e testadas de fábrica.

Item 51.Serviço de Instalação do Item 50

São de responsabilidade da contratada para a execução dos Serviços de Instalação, a instalação física e a configuração lógica do equipamento conforme os requisitos, localidades e condições descritas no item “2.3)Serviços de Instalação”deste documento.

Item 52. Conector Óptico Tipo V

1) Fornecimento de Conector Óptico Tipo V 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.

2) Interface óptica (transceiver) Gigabit Ethernet 1000Base-SX, para fibra óptica multimodo, com conector LC ou SC, segundo o padrão IEEE 802.3z.

3) Compatível com o "SwitchCore" especificados neste termo de referência. A compatibilidade deve ser assegurada por declaração do fabricante dos switches ou através de comprovação diretamente no sítio do fabricante.

4) Todos os componentes de hardware necessários para instalação nos switches deverão ser fornecidos.

5) Acompanhar cordão óptico duplo, com terminações SC do lado da conexão com o DIO, de 2,5 metros.As extremidades do cordão óptico deverão ser conectorizadas e testadas de fábrica.

Item 53.Serviço de Instalação do Item 52

São de responsabilidade da contratada para a execução dos Serviços de Instalação, a instalação física e a configuração lógica do equipamento conforme os requisitos, localidades e condições descritas no item "2.3)Serviços de Instalação"deste documento.

Item 54.Módulo de Firewall para Switch Core

1) Fornecimento de "Módulo de Firewall para Switch Core"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.

2) O modelo ofertado deve ser do mesmo fabricante do Item "Switch Core" descrito neste Termo de Referência.

3) Equipamento deve ser dedicado à função de Stateful Firewall.

4) Deve ser compatível com o Switch Core.

5) Deve suportar pelo menos 10.000.000 (dez milhões) de conexões simultâneas em sua tabela de estados(conexões concorrentes).

6) Deve suportar a criação de pelo menos 300.000 (trezentas mil) novas conexões TCP por segundo.

7) Deve suportar taxa de encaminhamento de pelo menos 5 Mpps (cinco milhões de pacotes por segundo).

8) Deve suportar funcionalidade de Stateful Firewall com desempenho mímino de 20 Gbps (vinte gigabits por segundo).

9) Os valores de desempenho especificados nos itens 5), 6),7) e 8) acima

devem ser ofertados de forma centralizada por módulo de firewall. Não serão aceitas soluções em que os valores especificados se baseiem em combinação de módulos de firewalls em um chassi.

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

11) Deve permitir no mínimo1000 (mil) interfaces lógicas associadas aVLANs e que permitam estabelecer regras de filtragem (Stateful Firewall) entre estas.

12) Deve construir registro de fluxos de dados relativos a cada sessãoiniciada, 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 sequência dos pacotes TCP, status dos flags “ACK”, “SYN” e “FIN”.

13) O equipamento deve permitir a “randomização” do número de sequência TCP, ou seja, funcionar como um “proxy” de número de sequência 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 sequência TCP real do host seguro (interno ao firewall) em uma sessão estabelecida entre os referidos hosts.

14) 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.

15) Deve suportar agrupamento lógico de objetos (“objectgrouping”) 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 ControlEntry”) individualmente, independentemente do fato de a configuração da política ter utilizado o conceito de agrupamento lógico de objetos.

16) 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.

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

18) Deve ser possível a integração do Firewall com a solução Microsoft Active Directory (MSAD), permitindo a criação de políticas de filtragem

baseados em usuários e grupos de usuários existentes na base MS AD.

19) 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 MSAD.

20) Implementar listas de controle de acesso em que o campo de destino seja baseado em FQDN (FullyQualified Domain Name).

21) Implementar políticas de controle de acesso baseadas em informações de horário ("time-basedaccesscontrol")

22) Deve implementar remontagem virtual de fragmentos ("Virtual FragmentReassembly") em conjunto com o processo de inspeção stateful. Deve ser possível estabelecer o número máximo de fragmentos por pacotes e timeouts de remontagem.

23) 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.

24) 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.

25) Possuir suporte a inspeção stateful dos protocolos de sinalização de telefonia H.323(v1,v2,v3,v4), SIP (SessionInitiationProtocol), MGCP e SCCP. A partir da inspeção dos protocolos de sinalização o firewall deve criar dinamicamente as permissões pertinentes para o tráfego de mídia (RTP/RTCP) entre os telefones envolvidos.

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

27) Possuir capacidade de limitar o número de conexões TCP incompletas ('half-open') simultâneas para cadaIP de origem (sem necessidade de especificar tal endereço IP).

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

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

30) Deve permitir simultaneamente com a implementação "Network AddressTranslation" 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 TransferProtocol (FTP) – modos “standard” e “passive”.

31) 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 (“requestmethod”) utilizado pelo cliente web.

- Deve possuir capacidade de filtrar “applets” Java e controlesActiveX.

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

- Permitir o bloqueio seletivo de comandos utilizados em requisiçõesFTP (“requestcommands”).

- 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.

33) Quanto ao suporte a Virtualização:

- Possuir suporte a tecnologia de Firewall Virtual, suportando instâncias totalmente isoladas entre si. 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 ser possível selecionar o modo de operação de cada instância de Firewall (seleção, por instância, de modo transparente ou roteado).

- Deve suportar a adição de instâncias virtuais através de licenças de software. Devem ser suportadas pelo menos 250 (duzentos e cinquenta) instâncias virtuais de Firewall.

- O equipamento deve ser fornecido com no mínimo 20 (vinte) instâncias virtuais de firewall;

- Deve ser suportada qualquer combinação de contextos em modo transparente e roteado, dentro do limite de instâncias suportadas.

34) Quanto ao gerenciamento e à conectividade:

- 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 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.

- 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 da funcionalidade de 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 (ProtocolIndependentMulticast) em SparseMode.

- 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 sequência TCP para conexões TCP que trafegam sobre IPv6.
- Deve suportar anti-spoofing (sem uso de ACLs) para endereços IPv6.
- Deve suportar gerenciamento sobre IPv6. Devem ser suportados pelo menos os seguintes protocolos de gerência: Telnet, SSH e HTTPS.
- Deve suportar statefulfailover de conexões IPv6.
- Deve suportar agrupamento lógico de objetos IPv6 (redes, hosts, serviços) e criação de regras (ACLs) usando tais objetos.

Item 55.Serviço de Instalação do Item 54

São de responsabilidade da contratada para a execução dos Serviços de Instalação, a instalação física e a configuração lógica do equipamento conforme os requisitos, localidades e condições descritas no item “2.3)Serviços de Instalação”deste documento.

Item 56.Serviço de Manutenção e Suporte do Item 54

1) Os serviços de Suporte e Manutenção deste Item deverão ser realizados em regime 24x7x4 (24 horas x 7 dias da semana com prazo para inicio da resolução do problema até 04 horas subsequentes à abertura do chamado técnico) pelo prazo mínimo de 12 (doze) meses que deverá ser considerado na planilha de preços como valor unitário por unidade de equipamento.

2) A CONTRATANTE poderá abrir chamados de manutenção diretamente no Fabricante do Item sem necessidade de prévia consulta e/ou qualquer liberação por parte da CONTRATADA.

3) Deverá ser garantido à CONTRATANTE o pleno acesso ao site do Fabricante dos equipamentos e softwares. Esse acesso deve permitir consultas a quaisquer bases de dados disponíveis para usuários relacionadas aos equipamentos e softwares especificados, além de permitir downloads de quaisquer atualizações de software ou documentação deste produto.

Item 57.Operação Assistida

1) A aquisição dos equipamentos e softwares relacionados no Grupo 3

ensejará a execução da fase de operação assistida descrita neste item.

2) Por operação assistida entende-se o acompanhamento presencial do funcionamento dos equipamentos e softwares instalados, com pronta intervenção no caso de qualquer problema detectado, bem como o esclarecimento de quaisquer dúvidas levantadas pela equipe técnica da CONTRATANTE.

3) A Unidade referente à "Operação Assistida" é por Dia Útil de trabalho, sendo que a quantidade mínima contratada não deverá ser menor que 5 (cinco) dias.

4) Após o atesto relativo à etapa de instalação e configuração dos equipamentos e softwares, a CONTRATADA deverá prover o serviço de operação assistida durante o período contratado.

5) Durante o período contratado de operação assistida, a CONTRATADA deverá manter nas dependências do CONTRATANTE, nos dias úteis, das 8h às 12h e das 13h às 17h, um profissional com certificação de nível profissional do mesmo fabricante da solução ofertada que tenha participado da etapa de instalação e configuração dos equipamentos.

6) Concluído o período contratado referente à etapa de operação assistida, e não havendo problemas técnicos, operacionais, de performance e/ou dúvidas sobre a gerência e funcionamento da solução implementada, o CONTRATANTE, por comissão especialmente constituída para este fim, subsidiada por sua equipe de gerência de redes, atestará o serviço em até 5 (cinco) dias úteis.

Item 58.Treinamento do Tipo II para a Solução de Segurança e Comunicação Unificada (Switching)

1) A CONTRATADA deverá prover um serviço de transferência de conhecimento, denominado simplesmente como "Treinamento do Tipo II para a Solução de Segurança e Comunicação Unificada" com base em material do fabricante da solução ofertada.

2) Caso a solução ofertada seja composta por mais de um fabricante, deverá ser ofertado "Treinamento do Tipo II para a Solução de Segurança e Comunicação Unificada" apenas para a solução que componha maior parte da solução;

3) O "Treinamento do Tipo II para a Solução de Segurança e Comunicação Unificada" deverá ser ministrado por profissional capacitado e certificado pelo Fabricante com foco na tecnologia de "Switching" que compõe a Solução de Segurança e Comunicação Unificada.

4) O "Treinamento do Tipo II para a Solução de Segurança e Comunicação Unificada" deverá ser realizado para um grupo de 5 (cinco) técnicos da CONTRANTE;

5) O "Treinamento do Tipo II para a Solução de Segurança e Comunicação Unificada" deverá possuir carga horária mínima de 40 (quarenta) horas e deverá ocorrer em meio período a ser definido pela CONTRATANTE;

6) O "Treinamento do Tipo II para a Solução de Segurança e Comunicação Unificada" deverá ser realizada utilizando conteúdo teórico e prático, através de laboratório preparado com equipamentos equivalentes aos ofertados, onde estarão disponíveis as mesmas funcionalidades solicitadas nas especificações técnicas dos itens referentes à tecnologia de "Switching";

7) O curso deverá ter conteúdo técnico teórico e prático, onde os alunos deverão ter conhecimentos básicos para instalação, operação e manutenção da tecnologia de "Switching" que compõe a solução de Segurança e Comunicação Unificada.

8) A CONTRATADA deverá disponibilizar instalações na cidade de Brasília/DF bem como todos os materiais necessários aos alunos para a realização do treinamento.

9) A CONTRATADA deverá prover toda a logística e todo o material necessário à execução da capacitação teórica e prática, ou seja, instalações adequadas, equipamentos, manuais e apostilas didáticas. Os manuais e apostilas fornecidos devem ser desenvolvidos com base nos materiais do fabricante.

10) Será permitida a utilização de acesso remoto aos equipamentos destinados ao conteúdo prático do treinamento quando necessário. Os equipamentos deverão ser de mesma marca e semelhante aos equipamentos ofertados.

11) A capacitação técnica deverá ter início em até 30 (trinta) dias após a assinatura do contrato, podendo ser adiada por conveniência da CONTRATANTE, quando então, em comum acordo com a CONTRATADA, será marcada a data definitiva.

GRUPO 4 - Segurança (itens 59 a 72)

Item 59.Solução de Firewall e IPS

1) Fornecimento de Solução de Firewall e IPS 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.

2) Equipamento do tipo “appliance” dedicado à função de Stateful Firewall e com suporte à terminação de VPN nos padrões IPSec e SSL-VPN.

3) 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).

4) Deve ser fornecido com pelo menos 08 (oito) interfaces 10/100/1000Base-Tauto-sense.

5) Deve suportar o acréscimo de pelo menos 06 (seis) interfaces Gigabit Ethernet 10/100/1000Base-T ou 06 (seis) interfaces Gigabit Ethernet 1000Base-X padrão SFP compatíveis com os conectores ópticos (transceivers) 1000Base-SX, 1000Base-LX e 1000Base-LH.

6) Deve suportar agregação de portas GigabitEthernet. Deve ser possível formar grupos de até 08 portas GigabitEthernet.

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

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

9) Deve suportar funcionalidade de Stateful Firewall com desempenho, mímino, de 2Gbps (Dois Gigabits por segundo).

10) Deve suportar taxa de encaminhamento de pelo menos 700.000 pps (setecentos mil pacotes por segundo).

11) Os valores de desempenho especificados nos ítens 7), 8), 9), e 10) acima devem ser ofertados de forma centralizada. Não serão aceitas soluções que se baseiem em valores combinados de módulos de firewalls em um chassi.

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

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

14) Deve construir registro de fluxos de dados relativos a cada sessãoiniciada, 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 sequência dos pacotes TCP, status dos flags “ACK”, “SYN” e “FIN”.

15) O equipamento deve permitir a “randomização” do número de sequência TCP, ou seja, funcionar como um “proxy” de número de sequência 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 sequência TCP real do host seguro (interno ao firewall) em uma sessão estabelecida entre os referidos hosts.

16) 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.

17) Deve suportar agrupamento lógico de objetos (“objectgrouping”) 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 ControlEntry”) individualmente, independentemente do fato de a configuração da política ter utilizado o conceito de agrupamento lógico de objetos.

18) 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.

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

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

21) 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.

22) Implementar listas de controle de acesso em que o campo de destino seja baseado em FQDN (FullyQualified Domain Name).

23) Implementar políticas de controle de acesso baseadas em informações de horário (“time-basedaccesscontrol”)

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

25) 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.

26) 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.

27) Possuir suporte a inspeção stateful dos protocolos de sinalização de telefonia H.323(v1,v2,v3,v4), SIP (SessionInitiationProtocol), MGCP e SCCP. A partir da inspeção dos protocolos de sinalização o firewall deve criar dinamicamente as permissões pertinentes para o tráfego de mídia (RTP/RTCP) entre os telefones envolvidos.

28) Deve ser suportada a inspeção do protocolo SIP (SIP over TLS) em ambientes com voz criptografada. A partir da inspeção do protocolo de sinalização, devem ser criadas as conexões pertinentes para o tráfego SRTP (Secure RTP)

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

30) Possuir capacidade de limitar o número de conexões TCP incompletas (‘half-open’) simultâneas para cadaIP de origem (sem necessidade de especificar tal endereço IP).

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

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

33) Deve permitir simultaneamente com a implementação “Network AddressTranslation” 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 TransferProtocol (FTP) – modos “standard” e “passive”.

34) 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 (“requestmethod”) utilizado pelo cliente web.

- Deve possuir capacidade de filtrar “applets” Java e controlesActiveX.

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

- Permitir o bloqueio seletivo de comandos utilizados em requisiçõesFTP (“requestcommands”).

- 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.

36) Quanto ao suporte e à virtualização:

- 1.20.2.1 Possuir suporte a tecnologia de Firewall Virtual, suportando instâncias totalmente isoladas entre si. 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 ser possível selecionar o modo de operação de cada instância de Firewall (seleção, por instância, de modo transparente ou roteado).

- Deve suportar a adição de instâncias virtuais através de licenças de software. Devem ser suportadas pelo menos 20 (vinte) instâncias virtuais de Firewall.

- Devem ser fornecidas 2 (duas) instâncias de firewall Virtual;

- Deve ser suportada qualquer combinação de contextos em modo transparente e roteado, dentro do limite de instâncias suportadas.

37) Quanto ao Suporte a VPN:

- A solução deve suportar a terminação de pelo menos 750 (setecentos e cinquenta) túneis IPSEC VPN simultaneamente. Devem ser fornecidas licenças de Cliente IPSEC VPN para pelo menos 750 (setecentos e cinquenta) 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 750 (setecentos e cinquenta) sessões SSL-VPN simultaneamente.

- Os clientes de VPN SSL devem suportar 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 1.500 (mil e quinhentos) mil usuários VPN.

- 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.

- 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 300 Mbps (trezentos megabits por segundo) para tratamento de conexões IPSEC (padrões AES e 3DES). A criptografia deve ser realizada em hardware dedicado.

- 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 (statefulfailover) 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 ("ExtendedAuthentication")

- 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 VPNsIPSec 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 dosendereços IP de VPN (endereços privados) aos clientes.

- O concentrador deve permitirque 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 AddressTranslation)

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

- 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 possível 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 7) 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 CertificateAuthorities (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 "PortForwarding", no mínimo as seguintes aplicações: Telnet, SSH, FTP over SSH, Windows Terminal Services, Outlook/Outlook Express e Lotus Notes.

- Deve suportar a criação de 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 suportar 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 ao qual o usuário que requisita o acesso

pertence. Deve ser possível especificar as URLs acessíveis através de conexões SSL VPN.

- Deve suportar o acesso SSL-VPN a pelo menos os seguintesaplicativos (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 suportar 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 suportar 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.

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

39) Deve ser gerenciável via SNMP, SNMPv2c e SNMPv3.

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

41) 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).

42) Deve permitir o armazenamento de pacotes capturados em formato tcpdump.

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

44) 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 enviados ao servidor TACACS+.

45) Deve vir acompanhado de interface gráfica para gerenciamento das funcionalidades de VPN eFirewall.

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

47) 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.

48) Implementar o protocolo PIM (ProtocolIndependentMulticast) em SparseMode.

49) Suporte a operação como IGMP Proxy Agent.

50) Deve suportar inspeção stateful de tráfego IPv6.

51) Deve suportar simultaneamente a criação de regras IPv4 e IPv6.

52) Deve suportar roteamento estático.

53) Deve implementar randomização do número de sequência TCP para conexões TCP que trafegam sobre IPv6.

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

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

56) Deve suportar statefulfailover de conexões IPv6.

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

58) Deve ser fornecido com solução integrada de IntrusionPrevention System (IPS).

59) A performance, mínima, de IPS deve ser de 600Mbps (600 Milhões de pacotes por segundo).

60) Deve ser possível selecionar, através de listas de controle de acesso, o tráfego que será enviado para inspeção pela solução de IPS.

61) A solução integrada de IPS deve suportar, no mínimo, as seguintes funcionalidades:

- 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).

- Deve utilizar assinaturas construídas com base em informações de vulnerabilidade e não somente em “exploits” específicos.

- 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.

- 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 "in-line" os pacotes associados ao ataque.

- Deve suportar "ProtocolAnomalyDetection" 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 ("StatefulPatternMatching").

- 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.

- Deve suportar "logging" de sessão via IP ("IP sessionlogging"). Os logs devem ser compatíveis com formato "TCPDump".

- 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).

- Deve possuir capacidade de bloquear tráfego de pelo menos os seguintes protocolos "peer-to-peer" (kazaa, gnutella, qtella, bearshare, gnucleus, limewire, morpheus, mutella, hotline, edonkey, soulseek, napster, bittorrent).

- Deve possuir capacidade de bloquear tráfego de pelo menos os seguintes sistemas de "instantmessaging" (yahoomessenger, ICQ, AOL, MSN).

- Deve ser capaz de detectar pelo menos os seguintes tipos de ataque:

Simplex-Mode TCP hijacking , E-mail Spam, BackOriffice2000 StealthMode, Unicode Decodes, IIS Unicode exploit, cross-site scripting, directorytraversal, commandinjection, SQL Injection, Header Spoofing.

- Deve sercapaz de detector atividade de Port Scanning (“Full connect”, “SYN Stealth”, “FIN Stealth”, UDP).

- 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.

Item 60.Serviço de Instalação do Item 59

São de responsabilidade da contratada para a execução dos Serviços de Instalação, a instalação física e a configuração lógica do equipamento conforme os requisitos, localidades e condições descritas no item “2.3)Serviços de Instalação”deste documento.

Item 61.Serviço de Manutenção e Suporte do Item 59

1) Os serviços de Suporte e Manutenção deste Item deverão ser realizados em regime 24x7x4 (24 horas x 7 dias da semana com prazo para inicio da resolução do problema até 04 horas subsequentes à abertura do chamado técnico) pelo prazo mínimo de 12 (doze) meses que deverá ser considerado na planilha de preços como valor unitário por unidade de equipamento.

2) A CONTRATANTE poderá abrir chamados de manutenção diretamente no Fabricante do Item sem necessidade de prévia consulta e/ou qualquer liberação por parte da CONTRATADA.

3) Deverá ser garantido à CONTRATANTE o pleno acesso ao site do Fabricante dos equipamentos e softwares. Esse acesso deve permitir consultas a quaisquer bases de dados disponíveis para usuários relacionadas aos equipamentos e softwares especificados, além de permitir downloads de quaisquer atualizações de software ou documentação deste produto.

Item 62.Software de Gerenciamento Centralizado de Firewall

1) Fornecimento de Software de Gerenciamento Centralizado de Firewall 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.

2) O modelo ofertado deve ser do mesmo fabricante dos itens “Módulo de Firewall para Switch Core” e “Solução de Firewall e IPS” descritos neste Termo de Referência.

3) Deve permitir a criação e distribuição de políticas de segurança de forma centralizada, suportando organização hierárquica de regras.

4) Deve ser possível associar regras de segurança a grupos lógicos de dispositivos.

5) A solução deve implementar uma tabela única de políticas de segurança, a qual deverá ser utilizada para a distribuição das políticas por todo o ambiente administrado.

6) A solução de gerenciamento deve suportar pelo menos 2.000 (dois mil) dispositivos de segurança providos pelo seu fabricante. Deve ser possível configurar de forma gráfica pelo menos as soluções de Firewall, IPSEC VPN e SSL VPN providas pelo fabricante desta solução.

7) A solução deve criar uma camada de abstração entre o processo de criação de regras e os modelos de dispositivos aos quais serão aplicadas. Desta forma as regras de Firewall, por exemplo, devem ser criadas sempre da mesma forma através da interface gráfica, independentemente do modelo específico de Firewall em que serão executadas.

8) Deve suportar a gerência de pelo menos 1 (um) milhão de regras de controle de acessos.

9) Suportar pelo menos 02 (dois) usuários simultâneos com acesso somente-leitura.

10) Suportar pelo menos 02 (dois) usuários simultâneos com acesso privilegiado.

11) A solução deve possuir ferramenta de análise de consistência das regras, para evitar conflitos lógicos entre novas regras com as regras existentes.

12) A solução deve permitir a identificação e exclusão de regras que estão aplicadas nos dispositivos, mas que não afetam o desempenho e a segurança da rede (regras em desuso sob o ponto de vista lógico).

13) A solução deve implementar a contabilização das Regras de Controle de Acesso – (ACEs = “Access Control Entries”) aplicadas aos dispositivos por ela gerenciados.

14) A solução deve permitir o agrupamento lógico de dispositivos, de acordo com a funcionalidade e com a localização física dos mesmos, permitindo o gerenciamento simultâneo de vários elementos.

15) A solução deve permitir que um dado equipamento possa pertencer simultaneamente a mais de um grupo de elementos gerenciados.

16) A solução deve permitir a reutilização de objetos lógicos em várias políticas de Segurança.

17) A solução deve permitir o retorno às configurações anteriores dos dispositivos, para a necessidade de recuperação de falhas (“Rollback de

configuração");

18) A solução deve permitir distribuição centralizada de softwares e suportar relatório de inventário de dispositivos.

19) A solução deve ser capaz de testar a conectividade dos equipamentos gerenciados.

20) A solução deve suportar configuração das funcionalidades de alta-disponibilidade dos equipamentos.

21) A solução deve permitir o gerenciamento de serviços tais como QoS em VPN, roteamento e Controle de Acesso à Rede nos elementos gerenciados.

22) A solução deve permitir a visualização de qual parte da topologia gerenciada (origem, destino, serviço, "wildcard") está sendo afetada por determinada regra.

23) A solução deve permitir a detecção de alteração e tentativas de alteração da configuração dos dispositivos por meio de acesso "out-of-band"(acessos que não usem a interface de gráfica de gerência provida pela ferramenta) e avisar o administrador.

24) A solução deve implementar funcionalidade de agrupamento de políticas de Segurança, ou seja, detectar um conjunto de regras que possa ser condensado em uma única regra que venha a produzir o mesmo efeito lógico no que concerne a Políticas de Segurança.

25) A solução deve suportar operação em modo de "workflow", ou seja, permitir que as regras sejam aplicadas somente após passar por um fluxo de aprovação gerencial.

26) A solução deve suportar acesso baseado em perfil de usuário com as permissões de visualizar, modificar, aprovar e distribuir por tipo de objeto e política. Deve ser possível definir os perfis de acesso à solução("Role Based Access Control" = RBAC) no sistema de Gerência de Controle de Acesso fornecido.

27) Deve suportar integração com solução de correlação de eventos. Deve suportar a visualização nesta solução de configuração as regras que geraram um determinado evento na solução de correlação.

28) A solução deve ser capaz de descobrir configurações existentes de VPN "site-to-site" e acesso remoto.

29) A solução deve permitir que as VPNs possam ser configuradas remotamente.

30) A solução deve permitir a configuração de dispositivos de VPN com suporte a failover automático e balanceamento de carga entre os

concentradores.

31) Deve ser fornecido em forma de appliance virtual (solução que permite ser instalado diretamente na plataforma de virtualização sem a necessidade de sistema operacional adicional), ou instalável na forma virtualizada (solução que permite ser instalado sobre um sistema operacional licenciado e virtualizado).

32) No caso de ser fornecido de forma virtualizada, deverão ser fornecidos os softwares e licenças necessárias para o pleno funcionamento da solução.

Item 63.Serviço de Instalação do Item 62

São de responsabilidade da contratada para a execução dos Serviços de Instalação, a instalação física e a configuração lógica do Item conforme os requisitos, localidades e condições descritas no item "2.3)Serviços de Instalação" deste documento.

Item 64.Serviço de Manutenção e Suporte do Item 62

1) Os serviços de Suporte e Manutenção deste Item deverão ser realizados em regime 24x7x4 (24 horas x 7 dias da semana com prazo para inicio da resolução do problema até 04 horas subsequentes à abertura do chamado técnico) pelo prazo mínimo de 12 (doze) meses que deverá ser considerado na planilha de preços como valor unitário por unidade de equipamento.

2) A CONTRATANTE poderá abrir chamados de manutenção diretamente no Fabricante do Item sem necessidade de prévia consulta e/ou qualquer liberação por parte da CONTRATADA.

3) Deverá ser garantido à CONTRATANTE o pleno acesso ao site do Fabricante dos equipamentos e softwares. Esse acesso deve permitir consultas a quaisquer bases de dados disponíveis para usuários relacionadas aos equipamentos e softwares especificados, além de permitir downloads de quaisquer atualizações de software ou documentação deste produto.

Item 65.Solução de Segurança Web

1) Fornecimento de Solução de Segurança WEB 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.

2) O modelo ofertado deve ser do mesmo fabricante do Item 59.

3) Solução em equipamento do tipo "appliance" para proteger o acesso de navegação à Internet e implementar conceito de políticas aceitáveis de uso (Acceptable Use Policies). Devem ser providas, no mínimo, as seguintes funcionalidades:

- Proxy de aplicação para os protocolos HTTP, HTTPS e FTP;

- Caching;
- Categorização e Controle de URL;
- Análise e bloqueio de URLs usando conceito de Reputação;
- Inspeção de Tráfego SSL;
- Controle e Visibilidade de Aplicações WEB;
- Filtragem de Conteúdo;
- Suportar, no mínimo, 2 (dois) módulos internos de Antivírus (de fabricantes diferentes);
- Módulo de controle AntiMalware interno;
- Monitoramento de camada 4 do modelo OSI para detectar atividades maliciosas em portas fora do padrão do proxy (80, 3128).

4) Asolução deverá prover proteção para, no mínimo,500 usuários simultâneos, devendo as licenças necessárias ser fornecidas.

5) A solução fornecida deve ser construída no conceito de appliance, sendo executada em Hardware e Software específicos e sistema operacional especializado. Todas as funcionalidades deverão ser executadas no mesmo equipamento, à exceção da solução de relatórios e gerenciamento, que poderá ser adicionada em um servidor ou appliance em paralelo. Toda a solução de hardware e software deverá ser fornecida pelo mesmo fabricante.

6) Características de Hardware e Requisitos de Desempenho para cada appliance:

- Possuir no máximo 1RU (Um Rack Unit) e suportar fixação em rack padrão 19 polegadas.
- Possuir no mínimo 1 (Um) processadorDual Core Intel Xeon com clock mínimo de 2.6GHz ou superior.
- Possuir no mínimo4 GB de memória RAM.
- Possuir no mínimo 2 (dois) discos de tipo SATA de no mínimo 250 GB.
- Possuir configuração RAID 1 dos discos e controladora do RAID em Hardware.
- Possuir no mínimo 2 (duas) interfaces Gigabit.

- Possuir fonteinterna ao equipamento.
- Possuir interface de console do tipo RS-232, ou similar.
- A solução deverá estar de acordo com as normas e padrões internacionais como:
    - FCC (U.S. only) Class A, ICES (Canada) Class A;
    - CE Mark (EN 55022 Class A, EN55024, EN61000-3-2, EN61000-3-3) ;
    - VCCI (Japan) Class A, BSMI (Taiwan) Class A.

7) O equipamento deve suportar no mínimo 300 requisições HTTP por segundo, considerando as configurações mínimas.

8) Possuir capacidade de suportar no mínimo 10.000 conexões TCP simultâneas.

9) Possuir latência de, no máximo, 50 milisegundos.

10) Essas funcionalidades deverão ser comprovadas mediante declaração do fabricante e/ou teste de bancada, ficando a cargo do órgão a execução do teste de bancada.

11) O Serviço de Proxy deverá ser compatível com navegação a partir de qualquer browser e sistema operacional.

12) Atuar nativamente como proxy dos protocolos HTTP, HTTPS e FTP.

13) Suportar controle de FTP sobre HTTP (nos modos ativo e passivo).

14) O cliente de FTP deve poder especificar a porta para controle de conexão através do seguinte formato: hostname:port.

15) Independente do modo de conexão iniciado pelo cliente FTP, o proxy deverá forçar a conexão ao servidor em modo passivo. Na situação em que o servidor FTP remoto não suporte modo passivo, o Proxy deverá operar em modo ativo.

16) Possibilitar a configuração da porta ou portas utilizadas para o serviço de Proxy para HTTP, HTTPS e FTP.

17) Possuir a capacidade de utilizar o proxy com o método CONNECT para portas tuneladas em HTTP.

18) O equipamento deve permitir requisições dos clientes da rede interna em uma interface de rede e a comunicação com a Internet em outra interface, possibilitando usar um endereço IP privado na interface de rede interna e um IP

público na interface de rede externa.

19) Deve ser capaz de criar lista de destinos que poderão pular as regras de proxy e políticas baseadas no mínimo em:

- Endereço IP;
- CIDR;
- Domínio;
- Hostname completo ou parcial;
- Grupo de usuários;
- Categorias de URL;
- Portas do proxy;
- Useragents.

20) O proxy fornecido deve suportar operação tanto em modo explícito como em modo transparente. No caso de modo transparente, deve ser implementado o redirecionamento de conexões através do protocolo WCCPv2.

21) A solução deverá permitir a reposição do PAC existente com uma nova versão do mesmo nome, e a solução deverá questionar se quer substituir ou não.

22) Deverá ser possível configurar múltiplos UpstreamProxy HTTP afim de redirecionar o tráfego se necessário para outras camadas de Proxy, possibilitando configurações de Failover, Balanceamento ou condicional.

23) A solução quando implementada com o recurso de upstreamproxy/ parent proxy, deverá permitir que o endereço IP seja especificado através do header X-forwarded-for, ao invés de ter somente o endereço IP do downstream proxy.

24) Deve possuir a funcionalidade de IP Spoofing (possibilitar encaminhar o endereço IP do cliente, e não do próprio proxy).

25) A funcionalidade de IP Spoofing deverá ser implementada em conjunto com WCCP (simultaneamente).

26) Possuir integração com serviços de diretório LDAP e domínios Windowspara auditoria e autenticação sem a necessidade de instalação de agentes ou plugins em nenhuma estação de trabalho ou servidor.

27) A solução deverá fazer a autenticação do usuário via NTLM de modo transparente, ou seja, utilizando usuário já autenticado em domínio Windows

sem pedir novamente a senha para o usuário.

28) O equipamento deve pedir autenticação (login, senha e domínio) para usuários que estejam utilizando sistemas operacionais diferentes do Windows (Linux, por exemplo), validando estes usuários nos serviços de diretórios: Microsoft Active Directory e LDAP.

29) Deve implementar autenticação de usuários e estações de trabalho sem a necessidade de instalação ou execução de qualquer software cliente ou qualquer módulo de software em estações de trabalho ou servidores.

30) Deve possuir integração total com Microsoft Active Directory para autenticação e importação de usuários e grupos.

31) Deve ser possível a um usuário com perfil de administrador acessar, a partir de uma máquina de outro usuário, sites e recursos que não estejam disponíveis para tal usuário com menor privilégio.

32) Devem ser suportadas políticas que permitam "bypass" de autenticação,de modo que usuários não-autenticados tenham acesso limitado à Internet.

33) Deve permitir a criação de políticas sofisticadas usando, no mínimo, os seguintes critérios:

- Grupos do domínio ou serviço de diretórios LDAP e AD aos quais o usuário pertence;
- Classificação das páginas (categorias de URLs);
- Tipos de arquivo;
- Porta do serviço de proxy a que o usuário conectou;
- Reputação do site de destino;
- Listas de URLs cadastradas;
- Base de URLs com contratação de atualizações com o fornecedor;
- Tipo de conteúdo;
- MIME Type;
- Presença de vírus e malware;
- Tamanho do download;
- Endereço IP;

- Expressões Regulares para URLs;
- Expressões Regulares para objetos;
- UserAgents.

34) Deverá permitir políticas baseadas em tempo (dias da semana, hora do dia) a fim de restringir acesso em horários pré-estipulados (ex. horário comercial).

35) O sistema deverá ser capaz de criar e hospedar arquivos PAC (Proxy Auto-configuration) e disponibilizá-lo através de portas configuráveis.

36) Permitir roteamento de Proxy baseado em:

- Origem e/ou destino;
- UserAgent .(ex. IE6,mozilla);
- Range (período) de tempo específico (dia, hora);
- Portas específicas;
- Categorias de URL's.

37) Deve permitir o armazenamento em Cache de conteúdo trafegados pelo protocolo HTTP.

38) Possuir a funcionalidade de eliminar o conteúdo do Cache (limpar o Cache).

39) Capacidade de criar listas de domínios cujo conteúdo não deve ser armazenado em cache.

40) Possuir sistema de arquivos que armazene o conteúdo de cada página em setores contíguos do disco para otimizar o acesso aos objetos armazenados.

41) Possuir espaço em cache para no mínimo 50Gb.

42) Características do Proxy HTTPS (Criptografado):

- Deve ser possível criar políticas de terminação HTTPS, usando pelo menos os seguintes critérios:
  - Categoria do site de destino;
  - Reputação do site de destino;
  - Status do certificado apresentado pelo site de destino. Os sites

com certificados expirados ou assinados por autoridade certificadora não confiável devem sempre ter as conexões HTTPS decifradas.

- O conteúdo HTTPS decifrado deve ser inspecionado pelo módulo de filtragem de URL e pela solução antimalware.

- A solução deverá atuar como um "man in themidle", e deverá suportar certificados locais (“on-box”). Deve ser possível importar certificados válidos e gerar certificados auto-assinados.

- A solução deverá suportar o envio de um CertificateSigningRequest (CSR) a uma CA para obtenção de um certificado digital. Todo o processo de requisição e instalação do certificado deve ser feito através da interface gráfica (GUI).

43) Características do Filtro de Conteúdo Web:

- O equipamento deve ter acesso a site proprietário de seu fabricante para atualizar automaticamente a base de URLs.

- Deve possuir uma base de URLs com, no mínimo, 60 categorias pré-definidas e 20 milhões de domínios cadastrados.

- A base de URLs deve possuir sites em no mínimo 50 línguas e de no mínimo 200 países.

- Deve permitir a criação de novas categorias por parte do administrador da solução. Devem ser suportados, no mínimo, os seguintes parâmetros na definição de novas categorias:

  - Endereço IP do servidor;

  - Sub-rede;

  - Domínio;

  - Expressões regulares nas URLs.

- Deve possibilitar o envio ao fabricante das URLs não cadastradas na base de dados para análise e inclusão na base de categorias via appliance ou via portal do fabricante.

- Deve possuir análise de conteúdo dinâmico dos sites permitindo a categorização em tempo real (web 2.0) dos sites que não pertencem a nenhuma categoria pré-estabelecida.

- Deve permitir notificar o usuário sobre a política de uso da empresa quando acessar sites proibidos, permitindo ou não o acesso se o usuário desejar continuar.

- A página de notificação para o usuário deverá rastrear quem aceitou a pagina do “EndUserAcknoledgement” por sessão do cookie ou endereço IP quando não houver um username disponível.

- A solução deveráarmazenar a Informação de Notificação “EndUserAcknoledgement” mesmo após a reinicialização do proxy.

- Possibilidade de bloqueio de acesso a sites de Chat e fóruns on-line.

- Possibilitar criar filtros URLs baseado em políticas de tempo, tais como dias da semana e range de horário, ou seja alguns sites só poderão ser acessados fora do horário de expediente.

- Deverá ser capaz de criar ações diferentes para as URLs em políticas por tempo.

- Deverá permitir customização da página de notificações aos usuários.

- Deve possuir no mínimo as seguintes categorias de URLs, sem custos adicionais:

    - Sites de conteúdos maliciosos;

    - Site de bate-papo (chat) e fóruns on-line;

    - Sites de FilterAvoidances;

    - Sites de relacionamento;

    - Sites de networking pessoal;

    - Sites de Acesso Remoto e Residencial – não permitir acesso a máquinas remotas via URLs dinâmicas e que caracterizem o acesso remoto;

    - Sites de pornografia (conteúdo adulto, pedofilia, erótico e também educação sexual);

    - Sites de webmails e de webmail corporativo (OWAs);

    - Sites de download e peer-to-peer (P2P);

    - Sites de streaming (audio e video on-line);

    - Sites de jogos;

    - Sites de hacking.

- Deve possuir a capacidade de criar regras de acesso diferenciadas por

categorias de URLs baseadas no mínimo em:

- Endereços IP;
- Sub-rede;
- Hostname;
- Domínio;
- Usuários (autenticados e não-autenticados);
- Grupos do domínio baseado em autenticação em LDAP.

- Dever possuir filtro contra perda de informações via Web (HTTP e HTTPS) e FTP analisando, no mínimo os seguintes parâmetros(Ex. Funcionários do Financeiro não pode enviar arqiuvo XLS via FTP):
  - Metadado de Arquivo (nome do arquivo, tipo do arquivo e tamanho do arquivo);
  - Usuário;
  - Grupo de usuários (intergração AD/LDAP);
  - URL, Categoria ou Reputação.
- Deve permitir integração com DLP (Data LossPrevention) externo.
- Deverá conter as seguintes ações:
  - Bloquear o site com log do acesso;
  - Liberar a página com log do acesso;
  - Redirecionar as requisições para uma URL determinada;
  - Realizar inspeção profunda (antimalware e inspeção de HTPPS).

44) Deve possuir um sistema de filtro de reputação que permita estabelecer uma reputação para cada endereço IP dos servidores de destino com as seguintes características:

- Deve utilizar dados de uma rede mundial de monitoração de tráfego web e de email para definir a reputação dos servidores de destino, consultando redes de participantes com cobertura global;
- A rede de reputação não deve somente ser baseada em informações de fluxo da própria base de Appliances instalada, mas sim em inúmeros

outros parâmetros provenientes de: listas negras de URL, listas brancas de URL, listas de equipamentos comprometidos, volume global de trafego, histórico dos sites, dados de categorização de URLs e web crawlers;

- Deve permitir ações diferenciadas de acordo com cada reputação obtida, como bloquear, permitir ou verificar detalhadamente os objetos de cada acesso.

45) O Anti-malware deve possuir as seguintes características:

- Efetuar todas as verificações de malware simultaneamente para cada objeto do site, em tempo real, e não sequencialmente, sem o uso de protocolos tais como ICAP.

- Deve suportar simultaneamente múltiplas ferramentas de filtragens de proteção contra malware (no mínimo duas) e de fabricantes diferentes.

- Se a detecção de malware não for feita no mesmo equipamento fornecido para filtro de conteúdo, a contratante deverá fornecer os appliances (conjunto de hardware e software de mesmo fabricante) para compor a solução, observando-se os requisitos de alta disponibilidade.

- Deve realizar a verificação de malware nos dois sentidos (download e upload).

- O mecanismo de verificação de malware deve reconhecer códigos maliciosos pelo menos nas seguintes categorias:

  - Adware;

  - Phishing;

  - Trojan Horse;

  - Commercial System Monitor;

  - Sessionhijackers;

  - Vírus

  - Worms;

  - Key Loggers;

  - OutbreakHeuristic;

- Possibilidade de armazenar o resultado das verificações de malware

em cache para minimizar a latência.

- Deve possuir mecanismo de verificação de tráfego na camada 4 do modelo OSI, permitindo identificar estações de trabalho infectadas por malwares na rede interna do cliente, com as seguintes características:

  - A monitoração de tráfego na camada 4 deve examinar o tráfego em todas as 65.535 portas do protocolo TCP;

  - A verificação de tráfego na camada 4 deve ser capaz de apenas monitorar ou monitorar e bloquear o tráfego suspeito;

  - Deverá ser disponibilizado um relatório de gerenciamento de camada 4, integrado ao appliance que exiba e determine os sites e aplicações que foram monitorados/bloqueados;

  - Deverá ser disponibilizado um relatório de gerenciamento de camada 4, integrado ao appliance que exiba e determine os TOP endereços IPs que acessaram sites com malware por portas.

46) O appliance fornecido deve possuir interface de gerência Web.

47) O appliance fornecido deve suportar configuração e monitorização via linha de comando (CLI).

48) Deve ser suportado o protocolo SSH para acesso seguro à CLI.

49) Devem estar disponíveis, no appliance, pelo menos os seguintes recursos:

- Tcpdump;
- Grep;
- Tail;
- Ping;
- Telnet.

50) Deve possuir MIB própria para verificação das informações de utilização via SNMP e deve possibilitar o envio de alertas administrativos utilizando e-mails.

51) A solução deverá ter ferramenta capaz de testar e simular alterações antes de serem aplicadas no sistema, de modo a permitir a validação das políticas antes que sejam aplicadas.

52) Possibilitar criar políticas de acesso à interface de gerenciamento baseada

em endereço IP e ranges de IPs que podem acessar o sistema.

53) Deve permitir integração com RADIUS para autenticar usuários na console de gerenciamento da solução.

54) A solução deverá permitir a criação de múltiplos servidores RADIUS para autenticação de usuários a gerencia.

55) O equipamento deve oferecer a possibilidade de envio de chamado ao suporte do fabricante utilizando comando interno que envie dados sobre a configuração do equipamento e informações de status e logs do equipamento para agilizar o atendimentok

56) A solução deverá permitir que os logs sejam configurados para serem enviados para um servidor externo baseado no tamanho do arquivo ou em horários pré definidos, como de hora em hora, diário, semanal mensal, ou horários customizados.

57) Possibilitar suporte remoto ao equipamento pelo fabricante através de acesso seguro ao equipamento habilitado pelo administrador.

58) Deve possuir pelo menos três classes de usuários, sendo elas administrador (com permissão de alterar configurações, gerenciar usuários e atualizar sistema operacional), operador (com permissão de alterar configurações) e convidado (somente acessar informações de relatório e status do equipamento).

59) A solução deverá exibir uma mensagem na interface gráfica, notificando ao administrador quando existe uma versão do sistema operacional mais nova disponível para ser baixada.

60) O appliance deve ser capaz de suportar toda a demanda e atender todos os requisitos desta especificação em um único equipamento.

61) Deverá ser compatível com SNMP Traps.

62) Deverá ser compatível com Syslog.

63) A solução deve atualizar todos os mecanismos de verificação de forma regular e automática, efetuando o download de forma incremental.

64) O Administrador poderá manualmente fazer as atualizações.

65) A solução deverá ser capaz de reverter a versão do sistema operacional, para uma versão prévia, já qualificada em casos emergenciais.

66) Deve possuir uma interface Web de geração de relatórios com informações em tempo real, integrada ao equipamento, com as seguintes características:

- Deve permitir a exportação dos dados dos relatórios para CSV e PDF;
- Deve possibilitar o agendamento do envio dos relatórios por e-mail;
- A interface Web de relatórios integrada ao equipamento com informações em tempo real deve ter, no mínimo, os seguintes relatórios:
    - Visão do sistema;
    - Categorias mais acessadas (10 categorias, pelo menos);
    - Usuários com mais acessos (10 usuários, pelo menos);
    - Atividades do usuário;
    - Detalhes do usuário;
    - Detalhes da categoria;
    - Detalhes do malware;
    - Monitor do filtro de reputação;
    - Monitor de tráfego na camada 4;
    - Uso de banda;
    - Banda economizada em função de bloqueios
    - Sites mais acessados;
    - Usuários com mais acessos.

Item 66. <u>Serviço de Instalação do Item 65</u>

São de responsabilidade da contratada para a execução dos Serviços de Instalação, a instalação física e a configuração lógica da solução conforme os requisitos, localidades e condições descritas no item “2.3)Serviços de Instalação”deste documento.

Item 67.<u>Serviço de Manutenção e Suporte do Item 65</u>

1) Os serviços de Suporte e Manutenção deste Item deverão ser realizados em regime 8x5xNBD (8 horas x 5 dias da semana com prazo para inicio da resolução do problema até o dia útil subsequente à abertura do chamado técnico) pelo prazo mínimo de 12 (doze) meses que deverá ser considerado na planilha de preços como valor unitário por unidade de equipamento.

2) A CONTRATANTE poderá abrir chamados de manutenção diretamente no

Fabricante do Item sem necessidade de prévia consulta e/ou qualquer liberação por parte da CONTRATADA.

3) Deverá ser garantido à CONTRATANTE o pleno acesso ao site do Fabricante dos equipamentos e softwares. Esse acesso deve permitir consultas a quaisquer bases de dados disponíveis para usuários relacionadas aos equipamentos e softwares especificados, além de permitir downloads de quaisquer atualizações de software ou documentação deste produto.

Item 68. Pacote de Expansão para Solução de Segurança Web

1) Fornecimento de um Pacote de Expansão Solução de Segurança Web 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.

2) O Pacote de Expansão deve ser totalmente compatível com a “Solução de Segurança Web” descrito neste documento. Pode ser oferecido em forma de hardware ou licença de software.

3) Deve, operando em conjunto com a "Solução de Segurança Web", atender a todas as características, as especificações e os requisitos descritos no Item “Solução de Segurança Web”.

4) Permitir a expansão da capacidade do Item “Solução de Segurança Web” para proteção de acesso a navegação de Internet a 100 (cem) novos usuários.

5) O pacote de expansão e a documentação (manuais) deverão ser fornecidos em CD/DVD ou ser disponibilizada senha para que seja realizado o “download” da página Internet do fabricante. Devem conter informações suficientes para possibilitar a instalação, configuração e operacionalização do módulo de expansão.

Item 69.Serviço de Instalação do Item 68

São de responsabilidade da contratada para a execução dos Serviços de Instalação, a instalação física e a configuração lógica do pacote de expansão conforme os requisitos, localidades e condições descritas no item “2.3)Serviços de Instalação”deste documento.

Item 70.Serviço de Manutenção e Suporte do Item 68

1) Os serviços de Suporte e Manutenção deste Item deverão ser realizados em regime 8x5xNBD (8 horas x 5 dias da semana com prazo para inicio da resolução do problema até o dia útil subsequente à abertura do chamado técnico) pelo prazo mínimo de 12 (doze) meses que deverá ser considerado na planilha de preços como valor unitário por unidade de equipamento..

2) Serão celebrados contratos de serviços de manutenção e suporte técnico entre a CONTRATADA e a CONTRATANTE.

3) O Suporte Técnico é um serviço de ajuda por telefone e por email/chat, prestado por técnicos especialistas na solução (devidamente credenciados pela empresa fabricante), com tempo para início de atendimento de no máximo 2 horas após a abertura do chamado.

4) A CONTRATANTE poderá abrir chamados de manutenção diretamente no Fabricante do Item sem necessidade de prévia consulta e/ou qualquer liberação por parte da CONTRATADA.

5) Deverá ser garantido à CONTRATANTE o pleno acesso ao site do Fabricante dos equipamentos e softwares. Esse acesso deve permitir consultas a quaisquer bases de dados disponíveis para usuários relacionadas aos equipamentos e softwares especificados, além de permitir downloads de quaisquer atualizações de software/firmware ou documentação deste produto.

Item 71.Operação Assistida

1) A aquisição dos equipamentos e softwares relacionados no Grupo 4 ensejará a execução da fase de operação assistida descrita neste item.

2) Por operação assistida entende-se o acompanhamento presencial do funcionamento dos equipamentos e softwares instalados, com pronta intervenção no caso de qualquer problema detectado, bem como o esclarecimento de quaisquer dúvidas levantadas pela equipe técnica da CONTRATANTE.

3) A Unidade referente à "Operação Assistida" é por Dia Útil de trabalho, sendo que a quantidade mínima contratada não deverá ser menor que 5 (cinco) dias.

4) Após o atesto relativo à etapa de instalação e configuração dos equipamentos e softwares, a CONTRATADA deverá prover o serviço de operação assistida durante o período contratado.

5) Durante o período contratado de operação assistida, a CONTRATADA deverá manter nas dependências do CONTRATANTE, nos dias úteis, das 8h às 12h e das 13h às 17h, um profissional com certificação de nível profissional do mesmo fabricante da solução ofertada que tenha participado da etapa de instalação e configuração dos equipamentos.

6) Concluído o período contratado referente à etapa de operação assistida, e não havendo problemas técnicos, operacionais, de performance e/ou dúvidas sobre a gerência e funcionamento da solução implementada, o CONTRATANTE, por comissão especialmente constituída para este fim, subsidiada por sua equipe de gerência de redes, atestará o serviço em até 5 (cinco) dias úteis.

Item 72. Treinamento do Tipo III para a Solução de Segurança e Comunicação Unificada (Segurança)

1) A CONTRATADA deverá prover um serviço de transferência de conhecimento, denominado simplesmente como "Treinamento do Tipo III para a Solução de Segurança e Comunicação Unificada" com base em material do fabricante da solução ofertada.

2) Caso a solução ofertada seja composta por mais de um fabricante, deverá ser ofertado "Treinamento do Tipo III para a Solução de Segurança e Comunicação Unificada" apenas para a solução que componha maior parte da solução.

3) O "Treinamento do Tipo III para a Solução de Segurança e Comunicação Unificada" deverá ser ministrado por profissional capacitado e certificado pelo Fabricante com foco na tecnologia de "Segurança" que compõe a Solução de Segurança e Comunicação Unificada.

4) O "Treinamento do Tipo III para a Solução de Segurança e Comunicação Unificada" deverá ser realizado para um grupo de 5 (cinco) técnicos da CONTRANTE.

5) O "Treinamento do Tipo III para a Solução de Segurança e Comunicação Unificada" deverá possuir carga horária mínima de 40 (quarenta) horas e deverá ocorrer em meio período a ser definido pela CONTRATANTE.

6) O "Treinamento do Tipo III para a Solução de Segurança e Comunicação Unificada" deverá ser realizada utilizando conteúdo teórico e prático, através de laboratório preparado com equipamentos equivalentes aos ofertados, onde estarão disponíveis as mesmas funcionalidades solicitadas nas especificações técnicas dos itens referente a tecnologia de "Segurança".

7) O curso deverá ter conteúdo técnico teórico e prático, onde os alunos deverão ter conhecimentos básicos para instalação, operação e manutenção da tecnologia de "Segurança" que compõea solução de Segurança e Comunicação Unificada.

8) A CONTRATADA deverá disponibilizar instalações na cidade de Brasília/DF bem como todos os materiais necessários aos alunos para a realização do treinamento.

9) A CONTRATADA deverá prover toda a logística e todo o material necessário à execução da capacitação teórica e prática, ou seja, instalações adequadas, equipamentos, manuais e apostilas didáticas. Os manuais e apostilas fornecidos devem ser desenvolvidos com base nos materiais do fabricante.

10) Será permitida a utilização de acesso remoto aos equipamentos destinados ao conteúdo prático do treinamento quando necessário. Os equipamentos deverão ser de mesma marca e semelhante aos equipamentos ofertados.

A capacitação técnica deverá ter início em até 30 (trinta) dias após a assinatura

do contrato, podendo ser adiada por conveniência daCONTRATANTE, quando então, em comum acordo com a CONTRATADA, será marcada a data definitiva.

GRUPO 5 (itens 73 e 74)

Item 73.Rack Tipo I

1) Cada rack deverá ser fornecido completo, novo e sem uso anterior, sendo todos da mesma marca.

2) Altura de no mínimo 44 Us (unidades modulares); Profundidade útil de no mínimo 570 mm,Largura interna de 23".

3) Base em chapa 2,50 mm, estrutura em chapa 1,50 mm, travessas horizontais e planos de montagem em chapa 1,50 mm.

4) Estrutura com 4 colunas soldadas ao teto e à base, confeccionada em chapa de aço carbono SAE 1010/1020.

5) Deverá permitir a instalação de kits (com no mínimo quatro ventiladores) de ventilação e/ou exaustores, de forma que não ocupem espaço útil dos planos de montagem.

6) Fechamentos laterais embutidos, confeccionados em estrutura de aço carbono, facilmente removíveis e perfurados.

7) Porta frontal confeccionada em chapa de aço carbono SAEperfurado, com fechadura e chave Yale.

8) Fechamento traseiro confeccionado em chapa de aço carbono SAE, facilmente removível e perfurado.

9) Planos frontais e traseiros de montagem em 19" reguláveis, confeccionados em chapa de aço carbono SAE 1010/1020 e furações de ½ em ½ U, conforme diretriz da Norma EIA 310-D, permitindo a instalação de equipamentos de rede rackeáveis e bandejas para equipamentos não rackeáveis, possui travessas laterais para sustentação e regulagem dos planos de montagem no sentido da profundidade.

10) Possui 4 organizadores verticais de 44 x 2" x 100 mm.

11) Possui base de sustentação para os organizadores verticais.

12) Possui pés niveladores para regulagem em pisos irregulares, rasgo com flange para passagem de cabos.

13) As chapas de aço carbono devem receber tratamento anticorrosivo com proteção contra oxidação e fungose que asseguram a melhor aderência da tinta a pó e maior proteção contra impactos mecânicos.

14) O acabamento deve ser executado através de pintura eletro estático com tinta híbrida a pó na cor Bege RAL 7032, mínimo de 80 micras.

15) Acompanha:

- Kit de ventilação/exaustão com 02 ventiladores, 110/220 v- 60 Hz, com chave liga e desliga, lâmpada piloto e seletor de voltagem;
- Bandeja fixacom aletas para ventilação (uma unidade) padrão 19 polegadas e 400 mm de profundidade, fixadas diretamente nos planos de montagem;
- Kit de fixação com 100 conjuntos (porca gaiola, arruela e parafuso Philips M5);
- Calha com 08 tomadas 2P + T, padrão NBR.

Item 74.Serviço de Instalação do Rack Tipo I

São de responsabilidade da contratada para a execução dos Serviços de Instalação, a instalação física e a configuração lógica do Item conforme os requisitos, localidades e condições descritas no item "2.3)Serviços de Instalação"deste documento.

GRUPO 6 (itens 75 a 76)

Item 75.Rack Tipo II

1) Cada rack deverá ser fornecido completo, novo e sem uso anterior, sendo todos do mesmo fabricante.

2) Altura de no mínimo 44 Us (unidades modulares); Profundidade útil de no mínimo 970 mm,Largura interna de 23".

3) Base em chapa 2,50 mm, estrutura em chapa 1,50 mm, travessas horizontais e planos de montagem em chapa 1,50 mm.

4) Estrutura com 04 colunas soldadas ao teto e à base, confeccionada em chapa de aço carbono SAE 1010/1020.

5) Deverá permitir a instalação de kits (com no mínimo quatro ventiladores) de ventilação e/ou exaustores, de forma que não ocupem espaço útil dos planos de montagem.

6) Fechamentos laterais embutidos, confeccionados em estrutura de aço carbono, facilmente removíveis e perfurados.

7) Porta frontal confeccionada em chapa de aço carbono SAEperfurado, com fechadura e chave Yale.

8) Fechamento traseiro confeccionado em chapa de aço carbono SAE, facilmente removível e perfurado.

9) Planos frontais e traseiros de montagem em 19" reguláveis, confeccionados em chapa de aço carbono SAE 1010/1020 e furações de ½ em ½ U, conforme diretriz da Norma EIA 310-D, permitindo a instalação de equipamentos de rede rackeáveis e bandejas para equipamentos não rackeáveis, possui travessas laterais para sustentação e regulagem dos planos de montagem no sentido da profundidade.

10) Possui 4 organizadores verticais de 44 x 2" x 100 mm.

11) Possui base de sustentação para os organizadores verticais.

12) Possui pés niveladores para regulagem em pisos irregulares, rasgo com flange para passagem de cabos.

13) As chapas de aço carbono devem receber tratamento anti-corrosivo com proteção contra oxidação e fungose que asseguram a melhor aderência da tinta a pó e maior proteção contra impactos mecânicos.

14) O acabamento deve ser executado através de pintura eletro estático com tinta híbrida a pó na cor Bege RAL 7032, mínimo de 80 micras.

15) Acompanha:

- Kit de ventilação/exaustão com 02 ventiladores, 110/220 v- 60 Hz, com chave liga e desliga, lâmpada piloto e seletor de voltagem;

- Bandeja fixacom aletas para ventilação (uma unidade) padrão 19 polegadas e 400 mm de profundidade, fixadas diretamente nos planos de montagem;

- Kit de fixação com 100 conjuntos (porca gaiola, arruela e parafuso Philips M5);

- Calha com 08 tomadas 2P + T, padrão NBR.

Item 76. <u>Serviço de Instalação do Rack Tipo II</u>

São de responsabilidade da contratada para a execução dos Serviços de Instalação, a instalação física e a configuração lógica do Item conforme os requisitos, localidades e condições descritas no item "2.3)Serviços de Instalação"deste documento.

5.4)<u>Serviços de Instalação</u>

a) Requisitos do Item

1) A CONTRATANTE irá definir junto a CONTRATADA através do relatório do Site Survey quantidade e os pontos onde a solução será instalada.

2) Durante reuniões entre a contratada e o CONTRATANTE que visem à elaboração do Plano de Instalação e Configuração da Solução de Segurança e Comunicação Unificada, a contratada deverá disponibilizar um Gerente de Projetos com certificação PMP.

3) O Plano de Instalação e Configuração consiste do Plano Geral do Projeto a ser executado para a implementação de rede sem fio, elaborado de acordo com metodologia aderente ao PMBoK e conter ainda:

- Descrição de todos os produtos a serem instalados;
- Diagrama de interconexão dos equipamentos;
- Projeto lógico de configuração.

4) O plano de Instalação e configuração deverá ser elaborado por, pelo menos, um profissional Gerente de Projetos com certificação PMP e um profissional que possua certificação específica para os equipamentos ofertados pela Contratada.

5) A Contratada deverá disponibilizar um técnico, certificado na solução, para instalação dos produtos no Ambiente da CONTRATANTE.

- A certificação do técnico deverá ser específica para os equipamentos a serem fornecidos.
- Caso um mesmo técnico não possua certificação em todos os tipos de equipamento, poderá ser disponibilizado mais de um técnico.

6) Os equipamentos de controle, gerenciamento e comunicação deverão ser instalados em racks de propriedade da CONTRATANTE.

7) Cabe à CONTRATADA a organização do rack e interconexão dos equipamentos com os patch pannels disponíveis, caso necessário, deverá ser fornecido pela contratada patch pannels adicionais.

8) Caberá à CONTRATADA providenciar todo e qualquer insumo necessário para instalação e funcionamento dos Access Points, incluindo cabos de rede, conectores, calhas e etc;

9) Os cabos de interconexão dos Access Points à rede devem ser embutidos e a instalação deverá preservar a arquitetura original do local em que forem instalados.

10) Após a instalação, cabem à CONTRATADA a limpeza e a remoção de qualquer resíduo proveniente do processo de instalação dos equipamentos.

11) A contratada deverá identificar todos os patch cords, relacionando a porta do switch com o Ponto de Acesso Gerenciável. Ao final da configuração deverá ser entregue documento contendo relação "Ponto de Acesso Gerenciável/porta do switch/andar/rack".

12) A CONTRATADA deverá apresentar, em até 20 dias úteis após a assinatura do contrato e a definição das quantidades e pontos em cada localidade junto a CONTRATANTE, um projeto executivo para implantação da solução adquirida.

13) O CONTRATANTEterá um prazo de 3 dias úteis para validar o projeto executivo e caso não aprove devolverá à contratada, a qual terá mais 3 dias úteis para realizar as devidas mudanças/adequações no referido projeto.

14) O projeto executivo deverá conter, no mínimo: descrição de todos os procedimentos a serem realizados, o cronograma de execução, e o plano de reversão a serem aplicados em caso de indisponibilidade, degradação de desempenho ou mau funcionamento.

15) O planejamento deverá ser executado no prazo de 30 (trinta) dias úteis após o recebimento dos equipamentos, e somente após aprovação do CONTRATANTE.

16) Todos os procedimentos necessários à implantação da solução que possam comprometer a disponibilidade do ambiente de tecnologia da informação da CONTRATANTE deverão ser realizados entre 19:30h e 07:00h do dia seguinte ou em finais de semana ou feriados.

Brasília – DF, 16 de setembro de 2013.

_____

PAULA MARIA DA COSTA PINTO PACHECO MORETTO - Cap
Chefe da SG3 / DEC - Resp. pelo Termo de Referência

De Acordo:

_____

ROBSON COCINODA COSTA– Cel
Ordenador de Despesas do DEC

ANEXO II

MODELO DE PROPOSTA DE PREÇOS (PAPEL TIMBRADO)

Local e data

Referência: Edital do Pregão Nr 017/2013– DEC

SR. PREGOEIRO,

A Empresa _____ sediada à (rua, bairro, cidade, telefone, etc), ___, inscrita no CNPJ/MF sob nº _____, neste ato representada por _____, abaixo assinada, propõe ao DEPARTAMENTO DE ENGENHARIA E CONSTRUÇÃO – DEC, o fornecimento dos serviços e materiais abaixo indicado(s)**, conforme Termo de Referência do Edital em epígrafe, nas seguintes condições:**

GRUPO	ITEM	DESCRIÇÃO	Unidade	Qtde	Valor Unitário Máximo que a ADM pode pagar (R$)	Valor Total Máximo (R$)
		SERVIÇOS PARA SOLUÇÃO DE SEGURANÇA E COMUNICAÇÃO UNIFICADA				
Grupo 1 **Solução WIFI**	1	CONTROLADOR WIFI	UN			
	2	Serviço de Instalação do Item 1	UN			
	3	Serviço de Manutenção e Suporte do Item 1	UN			
	4	CONTROLADOR WIFI REDUNDANTE	UN			
	5	Serviço de Instalação do Item4	UN			
	6	Serviço de Manutenção e Suporte do Item4	UN			
	7	PACOTE DE EXPANSÃO PARA CONTROLADOR WIFI	UN			
	8	Serviço de Instalação do Item7	UN			
	9	Serviço de Manutenção e Suporte do Item 7	UN			
	10	SOFTWARE DE GERENCIAMENTO DA REDE WIFI	UN			
	11	Serviço de Instalação do Item 10	UN			
	12	Serviço de Manutenção e Suporte do Item 10	UN			
	13	PACOTE DE EXPANSÃO PARA SOFTWARE DE GERENCIAMENTO DA REDE WIFI	UN			
	14	Serviço de Instalação do Item 13	UN			
	15	Serviço de Manutenção e Suporte do Item 13	UN			
	16	PONTO DE ACESSO WIFI INTERNO	UN			
	17	Serviço de Instalação do Item 16	UN			
	18	Serviço de Manutenção e Suporte do Item 16	UN			
	19	PONTO DE ACESSO WIFI EXTERNO	UN			
	20	Serviço de Instalação do Item 19	UN			
	21	Serviço de Manutenção e Suporte do Item 19	UN			
	22	SITE SURVEY	UN			
	23	OPERAÇÃO ASSISTIDA	DIA			

GRUPO	ITEM	DESCRIÇÃO	Unidade	Qtde	Valor Unitário Máximo que a ADM pode pagar (R$)	Valor Total Máximo (R$)
		SERVIÇOS PARA SOLUÇÃO DE SEGURANÇA E COMUNICAÇÃO UNIFICADA				
	24	TREINAMENTO DO TIPO I PARA A SOLUÇÃO DE SEGURANÇA E COMUNICAÇÃO UNIFICADA (WIFI)	UN			
Grupo 2 **Solução de Controle de Acesso**	25	SOLUÇÃO CENTRALIZADA DE CONTROLE DE ACESSO DE USUÁRIOS E DISPOSITIVOS	UN			
	26	Serviço de Instalação do Item 25	UN			
	27	Serviço de Manutenção e Suporte do Item25	UN			
	28	PACOTE DE EXPANSÃO PARA SOLUÇÃO CENTRALIZADA DE CONTROLE DE ACESSO DE USUÁRIOS E DISPOSITIVOS	UN			
	29	Serviço de Instalação do Item28	UN			
	30	Serviço de Manutenção e Suporte do Item28	UN			
	31	OPERAÇÃO ASSISTIDA	DIA			
Grupo 3 **Switching**	32	SWITCH DE ACESSO TIPO I	UN			
	33	Serviço de Instalação do Item32	UN			
	34	Serviço de Manutenção e Suporte do Item32	UN			
	35	SWITCH DE ACESSO TIPO II	UN			
	36	Serviço de Instalação do Item35	UN			
	37	Serviço de Manutenção e Suporte do Item35	UN			
	38	SWITCH DE ACESSO TIPO III	UN			
	39	Serviço de Instalação do Item38	UN			
	40	Serviço de Manutenção e Suporte do Item38	UN			
	41	SWITCH CORE	UN			
	42	Serviço de Instalação do Item41	UN			
	43	Serviço de Manutenção e Suporte do Item41	UN			
	44	CONECTOR ÓPTICO TIPO I	UN			
	45	Serviço de Instalação do Item44	UN			
	46	CONECTOR ÓPTICO TIPO II	UN			
	47	Serviço de Instalação do Item46	UN			
	48	CONECTOR ÓPTICO TIPO III	UN			
	49	Serviço de Instalação do Item48	UN			
	50	CONECTOR ÓPTICO TIPO IV	UN			
	51	Serviço de Instalação do Item50	UN			
	52	CONECTOR ÓPTICO TIPO V	UN			
	53	Serviço de Instalação do Item52	UN			
	54	MÓDULO DE FIREWALL PARA SWITCH CORE	UN			
	55	Serviço de Instalação do Item54	UN			
	56	Serviço de Manutenção e Suporte do Item54	UN			
	57	OPERAÇÃO ASSISTIDA	DIA			
	58	TREINAMENTO DO TIPO II PARA A SOLUÇÃO DE SEGURANÇA E COMUNICAÇÃO UNIFICADA (SWITCHING)	UN			
Grupo 4	59	SOLUÇÃO DE FIREWALL E IPS	UN			
	60	Serviço de Instalação do Item59	UN			

GRUPO	ITEM	DESCRIÇÃO	Unidade	Qtde	Valor Unitário Máximo que a ADM pode pagar (R$)	Valor Total Máximo (R$)
		SERVIÇOS PARA SOLUÇÃO DE SEGURANÇA E COMUNICAÇÃO UNIFICADA				
Segurança	61	Serviço de Manutenção e Suporte do Item59	UN			
	62	SOFTWARE DE GERENCIAMENTO CENTRALIZADO DE FIREWALL	UN			
	63	Serviço de Instalação do Item62	UN			
	64	Serviço de Manutenção e Suporte do Item62	UN			
	65	SOLUÇÃO DE SEGURANÇA WEB	UN			
	66	Serviço de Instalação do Item65	UN			
	67	Serviço de Manutenção e Suporte do Item65	UN			
	68	PACOTE DE EXPANSÃO PARA SOLUÇÃO DE SEGURANÇA WEB	UN			
	69	Serviço de Instalação do Item68	UN			
	70	Serviço de Manutenção e Suporte do Item68	UN			
	71	OPERAÇÃO ASSISTIDA	DIA			
	72	TREINAMENTO DO TIPO III PARA A SOLUÇÃO DE SEGURANÇA E COMUNICAÇÃO UNIFICADA (Segurança)	UN			
Grupo 5	73	RACK TIPO I	UN			
	74	Instalação RACK TIPO I	UN			
Grupo 6	75	RACK TIPO II	UN			
	76	Instalação RACK TIPO II	UN			

- Nos preços acima estão incluídos todos os insumos que compõem o objeto, inclusive as despesas com impostos, taxas, frete, seguros, garantia estendida e quaisquer outros que incidam direta ou indiretamente no fornecimento dos serviços e materiais;

- Prazo de entrega dos serviçose materiais: 60 (sessenta) dias corridos a contar do recebimento da nota de empenho;

- Garantia de fábrica;

- Garantia estendida (quando houver);

- A entrega dos serviços e materiais será feita no local determinado pelo Departamento de Engenharia e Construção – DEC, sem nenhum ônus para essa Organização Militar;

- Prazo de validade da proposta: (deverá ser no mínimo de 60 dias);

- Dados bancários: (informar banco, agência e conta-corrente);

- Declaramos que estamos de pleno acordo com todas as condições estabelecidas no Edital e seus anexos.

_____

Nome , Cargo e Identidade do Representante da Empresa

(PAPEL TIMBRADO)

ANEXO III

MODELO DE ATESTADO DE BOA E REGULAR EXECUÇÃO DO OBJETO (CAPACIDADE TÉCNICA)

Referência: Edital do Pregão Nr 017/2013– DEC

Nos termos do inciso II do art 30 da Lei 8.666/93, **ATESTO** que a empresa _____, inscrita no CNPJ/MF sob o nr _____, situada à _____ , **entregou o _____, cumprindo fielmente as condições contratuais e as exigências técnicas de adequação e qualidade.**

Local e data

_____

Nome - Cargo - Idt Nr

ÓRGÃO EMISSOR

(PAPEL TIMBRADO)

ANEXO IV

DECLARAÇÃO DA NÃO EXISTÊNCIA DE EMPREGADOS EM CONDIÇÕES EXCEPCIONAIS

Referência: Edital do Pregão Nr 017/2013 – CPL – DEC

A empresa _____, inscrita no CNPJ/MF sob nº _____, por intermédio de seu representante legal o(a) Sr.(a) _____, portador da carteira de identidade nº _____ e do CPF nº _____ , declara, para fins do disposto no inciso "V", art. 27, da Lei nº 8.666, de 21 de junho de 1993, acrescido pela lei nº 9.854, de 27 de outubro de 1999, que não emprega menores de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 (dezesseis) anos.

Ressalva: emprega menor, a partir de 14 (quatorze) anos na condição de aprendiz.

Brasília, ____de _____de 2013.

_____

Responsável ou Representante legal -idt nº

Observação: em caso afirmativo, assinalar a ressalva acima.

(PAPEL TIMBRADO)

ANEXO V

DECLARAÇÃO DE INEXISTÊNCIA DE FATO IMPEDITIVO DA HABILITAÇÃO

Referência: Edital do Pregão Nr 017/2013– DEC

A empresa _____, inscrita no CNPJ Nº _____, sediada no (a) _____, declara, para os devidos fins do pregão Nº ____/2008 - DEC, sob as penas da Lei que até a presente data inexistem fatos impeditivos para a sua habilitação no presente processo licitatório, ciente da obrigatoriedade de declarar ocorrências posteriores.

Brasília-DF, ____de _____de 2013.

_____

Diretor ou representante legal - Idt Nº

(PAPEL TIMBRADO)

ANEXO VI

DECLARAÇÃO PARA MICRO E PEQUENA EMPRESA E EPP

Referência: Edital do Pregão Nr 017/2013 – DEC

Declaro para fins de licitação junto ao Departamento de Engenharia e Construção (DEC) que a empresa _____ , CNPJ _____ encontra-se enquadrada no conceito de micro e pequena empresa, conforme disposição da Lei Complementar nº 123, de 14 de dezembro de 2006, de acordo com o documento comprobatório anexo.

BRASÍLIA/DF _____ de _____ de 2013.

_____

Ass. Responsável

NOME COMPLETO, IDT OU CPF,

MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
DEPARTAMENTO DE ENGENHARIA E CONSTRUÇÃO
(DEPARTAMENTO TÉCNICO E DE PRODUÇÃO DO EXÉRCITO/1946)

ANEXO VII

MINUTA DE CONTRATO

CONTRATO DE SERVIÇO DE TECNOLOGIA DA INFORMAÇÃO CELEBRADO ENTRE A UNIÃO, POR INTERMÉDIO DO DEPARTAMENTO DE ENGENHARIA E CONSTRUÇÃO E A .....(empresa).....

OBJETO: CONTRATAÇÃO DE SOLUÇÃO DE SEGURANÇA E COMUNICAÇÃO UNIFICADA
NATUREZA: OSTENSIVO

VIGÊNCIA: _____

TERMO DE CONTRATO Nr ___ /2013-DEC

A União, pessoa de direito público interno, por intermédio do Departamento de Engenharia e Construção (DEC) do Comando do Exército, inscrito no CNPJ sob o nº 07521315/0001-23, representado neste ato pelo Cel.ROBSON COCINO DA COSTA, Ordenador de Despesas, doravante denominado simplesmente CONTRATANTE e a empresa ....., estabelecida à ....., inscrita no CNPJ sob o nº ....., representada neste ato pelo .....(*seu(s) Diretor(es).....,de conformidade cm as disposições estatutárias ou do contrato social)* (ou pelo *seu(s) procurador(es) de conformidade com o instrumento de procuração), Sr* ....., carteira de identidade Nº....., CPF Nº....., daqui por diante denominada CONTRATADA, tendo em vista a Ata de Registro de Preços do Pregão nº 17/2013-DEC-SRP, Processo Administrativo nº

118/2013-DEC, firmam o presente CONTRATO de aquisição de solução de segurança e comunicação unificada na infraestrutura de tecnologia da informação do Departamento de Engenharia e Construção (DEC) e Diretorias Subordinadas, visando à adequação da tecnologia existente para uma infraestrutura com controles e administração efetiva, bem como a implantação de meios não existentes, como enlace externo próprio e infraestrutura de segurança interna e externa para atender a demanda do DEC, conforme especificações e quantidades previstas no Anexo I (Termo de Referência), atendendo às condições previstas no edital, sujeitando-se as partes às normas constantes na Lei nº 8.666, de 21 de junho de 1993 e suas alterações, no Decreto n.º 7.892, de 23 de janeiro de 2013 e na Lei nº 8.078, de 11 de setembro de 1990, e em conformidade com as disposições a seguir:

CLÁUSULA PRIMEIRA – OBJETO

- O Objeto deste Contrato é aquisição de solução de segurança e comunicação unificada na infraestrutura de tecnologia da informação do Departamento de Engenharia e Construção (DEC) e Diretorias Subordinadas, visando à adequação da tecnologia existente para uma infraestrutura com controles e administração efetiva, bem como a implantação de meios não existentes, como enlace externo próprio e infraestrutura de segurança interna e externa para atender a demanda do DEC.

CLÁUSULA SEGUNDA - FORMA DE FORNECIMENTO

- O Objeto deste Contrato deverá ser entregue e instalado conforme o especificado no Termo de Referência deste Edital.

CLÁUSULA TERCEIRA – PREÇOS

- Os preços unitário e total dos materiais e serviço que constituem o objeto deste Contrato, já incluídas as despesas de frete, impostos, seguro.

Qtd	Material	Marca	Modelo	Preço	
				Unitário	Total

CLÁUSULA QUARTA - CONDIÇÕES DE PAGAMENTO

4.1. O pagamento será efetuado em até 30 (trinta dias) dias corridos, contados da data da aceitação dos itens constantes das notas fiscais, observada a aceitabilidade pela equipe de fiscalização do contrato.

4.2. A liberação do pagamento ficará condicionada à consulta prévia ao SICAF (via ON LINE), devendo a contratada estar com sua documentação obrigatória válida.

4.3. No caso de incorreção nos documentos apresentados, inclusive na Nota Fiscal/Fatura, serão os mesmos restituídos à adjudicatária para as correções necessárias, não respondendo o DEC por quaisquer encargos resultantes de atrasos nos pagamentos correspondentes.

4.4. A contratada só poderá emitir a nota fiscal após autorização prévia, por escrito, do gestor do contrato.

CLÁUSULA QUINTA - DO PRAZO E DO LOCAL DE ENTREGA

- O objeto deste Contrato deverá ser entregue, conforme o constante do item 14.1. do Edital, ou seja, a entrega dos materiais deverá ser de no máximo 60 (sessenta) dias corridos, após o recebimento do empenho, pela contratada, e o início da prestação dos serviços deverão ocorrer até 20 (vinte) dias corridos, após o recebimento da ordem de serviço que será fornecida pelo gestor do contrato.

, no endereço constante do item 14.1. do Edital.

CLÁUSULA SEXTA – CONDIÇÕES DE RECEBIMENTO

6.1. O recebimento dos materiais e serviços far-se-á da seguinte forma:

6.1.1.provisoriamente, quantitativamente, para posterior comprovação da conformidade do bem com as especificações constantes do Anexo I (Termo de Referência) deste Edital;

6.1.2.definitivamente, pela Comissão de Recebimento e Exame, a ser designada pela Fiscalização, após comprovação da compatibilidade do bem com as especificações constantes do Anexo I (Termo de Referência) do Edital e o seu funcionamento, após a instalação;

6.1.3.rejeitado, quando os materiais estiverem em desacordo com o estabelecido no Anexo I (Termo de Referência) do Edital ou se os materiais apresentarem falhas de funcionamento e de uso.

6.2.A contratante convocará a licitante vencedora, durante a validade da ATA, para, no prazo máximo de 5 (cinco) dias, aceitar e retirar a nota de empenho (NE), sob pena de decair o direito ao fornecimento, sem prejuízo das sanções previstas no art. 81, da Lei 8.666/93. O prazo de convocação poderá ser prorrogado uma vez, por igual período, quando solicitado pela licitante vencedora durante o seu transcurso, desde que ocorra motivo justificado e aceito pela contratante.

6.3.O prazo de entrega dos materiais deverá ser de no máximo 60 (sessenta) dias corridos, após o recebimento do empenho, pela contratada, e o início da prestação dos serviços deverão ocorrer até 20 (vinte) dias corridos, após o recebimento da ordem de serviço que será fornecida pelo gestor do contrato.

6.4 Os treinamentos serão realizados quando das instalações dos equipamentos e softwares, em datas propostas pela contratada e aprovadas pela contratante.

6.5. A CONTRATANTE rejeitará, no todo ou em parte, mediante Termo de Rejeição Total ou Parcial, o que for fornecido em desacordo com este Contrato.

6.5.1. Os materiais rejeitados serão colocadas à disposição da CONTRATADA, que deverá retirá-las, refazê-las ou substituí-las, às suas expensas, entregando as novas no mesmo endereço da Organização Militar que fez a recusa.

6.5.2. Fica estabelecido o prazo de 10 (dez) dias corridos para a retirada dos materiais rejeitados, contado da data do recebimento do Termo de Rejeição.

6.6. A recusa dos materiais não justificará atrasos nos prazos de entrega fixados neste Contrato.

6.7. Ocorrendo pela segunda vez a rejeição dos materiais, este Contrato poderá ser rescindido e aplicadas as penalidades correspondentes.

6.8. O recebimento do material estará condicionado à observância de suas Especificações Técnicas, e instruções, cabendo a verificação respectiva à Comissão de Recebimento de cada Organização Militar.

6.9. Os ensaios, testes e demais provas exigidos por normas técnicas para aferição técnica dos materiais correrão por conta da CONTRATADA.

CLÁUSULA SÉTIMA – RECURSOS FINANCEIROS

- A despesa com a execução deste Contrato, no valor de R$.... (.....), será atendida por recursos da dotação orçamentária do PJT/ATV....., ND ....., Fonte ....., já empenhado o valor de R$... (...), conforme Nota de Empenho nº .....

CLÁUSULA OITAVA – GARANTIA TÉCNICA

8.1. O prazo de garantia técnica mínima do Objeto deste Contrato será até _____ (_____), contados da **data do seu recebimento definitivo**, considerando-se o somatório da garantia de fábrica e da garantia estendida, de acordo com exigência do Edital e Termo de Referência constante da proposta apresentada pela CONTRATADA. Fica a CONTRATADA obrigada a substitui ou reparar às suas expensas os materiais, peças ou componentes em que se verificarem vícios, defeitos ou incorreções resultantes da fabricação ou montagem.

8.2. Constatada a falha ou defeito, a CONTRATANTE notificará a CONTRATADA para sanar a deficiência apresentada, no prazo máximo de 30 (trinta) dias.

8.3. Se os defeitos verificados no objeto deste Contrato forem oriundos de negligência ou de uso indevido pela CONTRATANTE, constatada essa condição de comum acordo entre as partes, as despesas decorrentes da substituição ou reparação serão de responsabilidade da CONTRATANTE.

CLÁUSULA NONA - GARANTIA DE ASSISTÊNCIA TÉCNICA

- A CONTRATADA deverá prestar assistência técnica de modo a garantir o desempenho satisfatório e a segurança operacional dos materiais fornecidos, por pessoal habilitado, sempre que necessário, durante todo o período da garantia, conforme o estabelecido no Termo de Referência e no Edital para todos os itens licitados .

CLÁUSULA DÉCIMA - CONTINUIDADE NO FORNECIMENTO

- A CONTRATADA obriga-se a assegurar continuidade de fornecimento de peças, sobressalentes ou componentes, nos termos dos contratos que com ela venham a ser firmados, durante o período de _____ ( ) meses.

CLÁUSULA DÉCIMA PRIMEIRA – ACOMPANHAMENTO E FISCALIZAÇÃO

11.1. Nos termos do art. 67, § 1°, da Lei n° 8.666/93, a CONTRATANTE designará um representante para acompanhar e fiscalizar a execução do Contrato, anotando em

registro próprio todas as ocorrências que porventura existirem e determinando o que for necessário à regularização das falhas ou defeitos observados.

11.2. Da mesma forma, a CONTRATADA deverá indicar um **preposto** para, se aceito pela CONTRATANTE, representá-la na execução do Contrato.

11.3 - Quaisquer exigências da fiscalização, inerentes ao objeto do Contrato, deverão ser prontamente atendidas pela CONTRATADA, sem ônus para a CONTRATANTE.

CLÁUSULA DÉCIMA SEGUNDA– PRORROGAÇÃO DO PRAZO DE ENTREGA

12. 1. Os prazos de entrega poderão ser prorrogados, desde que ocorra um dos seguintes motivos:

12.1.1. Alteração das especificações pela CONTRATANTE;

12.1.2. superveniência de fato excepcional ou imprevisível, estranho à vontade das partes, que altere fundamentalmente as condições de execução deste Contrato;

12.1.3. interrupção da execução deste Contrato ou diminuição do ritmo de trabalho por ordem e no interesse da CONTRATANTE;

12.1.4. impedimento de execução deste Contrato por ato ou fato de terceiro reconhecido pela CONTRATANTE em documento contemporâneo a sua ocorrência;

12.1.5.omissão ou atraso de providências a cargo da Contratante, inclusive quanto aos pagamentos previstos de que resulte diretamente impedimento ou retardamento na execução deste Contrato.

12.2. Verificado algum dos motivos relacionados, a CONTRATANTE poderá conceder a prorrogação necessária, desde que o respectivo pedido seja apresentado pela CONTRATADA, por escrito, devidamente fundamentado, até 10 (dez) dias antes do vencimento do prazo contratual.

12.3. Nos casos previstos nesta Cláusula, os prazos serão prorrogados por período considerado razoável de comum acordo entre as partes, em face das circunstâncias do caso verificado.

CLÁUSULA DÉCIMA TERCEIRA – DAS SANÇÕES ADMINISTRATIVAS E PENALIDADES

17.1. Nos termos do art. 7º da Lei nº 10.520/2002 e art. 28 do Decreto nº 5.450/2005, ficará impedida de licitar e contratar com a União, Estados, Distrito Federal ou

Municípios e será descredenciada do SICAF ou dos sistemas de cadastramento de fornecedores a que se refere o inciso XIV do art. 4º da mesma Lei, pelo prazo de até 5 (cinco) anos, sem prejuízo das multas previstas no Edital e das demais penalidades legais, a licitante que:

g. não retirar a Nota de Empenho, quando convocada dentro do prazo de validade de sua proposta;

h. apresentar documentação falsa;

i. deixar de entregar os documentos exigidos para o certame;

j. retardar, falhar ou fraudar a execução da obrigação assumida;

k. não mantiver a proposta; e

l. comportar-se de modo inidôneo ou cometer fraude fiscal.

17.2. Com fundamento nos artigos 86 e 87 da Lei nº 8.666/93 e no Decreto n° 3.555/2000, a adjudicatária ficará sujeita, no caso de atraso injustificado, assim considerado pela Administração, execução parcial ou inexecução da obrigação, sem prejuízo das responsabilidades civil e criminal, assegurada a prévia e ampla defesa, às seguintes penalidades:

c. advertência;

d. multa, nas condições estabelecidas neste edital.

17.3.O valor dos juros de mora serão calculados por dia de atraso, contados dia a dia, e aplicados cumulativamente com as multas moratórias e compensatórias, limitada a incidência a 30 (trinta) dias. Após o trigésimo dia e a critério da Administração, poderá ocorrer a não aceitação do objeto, de forma a configurar, nessa hipótese, inexecução total da obrigação assumida, sem prejuízo da rescisão unilateral da avença. Para a inexecução total do contrato será aplicada a multa de 60% do valor deste contrato;

17.4.O descumprimento total ou parcial das obrigações assumidas pelo licitante, sem justificativa aceita pelo DEC, resguardados os procedimentos legais pertinentes, poderá acarretar:

VIII. Multa de 0,33% (trinta e três centésimos por cento) por dia de atraso, na entrega de material ouexecução de serviços, calculado sobre o valor correspondente à parte inadimplente, até o limite de 9,9%, que corresponde a até 30 (trinta) dias de atraso.

IX. Após 30 (trinta) dias de atraso, a critério da contratante, será aplicada a Multa de 0,66 % (sessenta e seis centésimos por cento) por dia de atraso, na entrega dematerial ou execução de serviços, calculado, desde o trigésimo primeiro dia de atraso, sobre o valor correspondente à parte inadimplente, em caráter excepcional, podendo chegar até 30 (trinta) dias de atraso. Findo este novo prazo, a critério da contratante, o contrato poderá ser rescindido unilateralmente, sem eximir a contratada das penalidades previstas neste edital.

X. Multa de 15% (quinze por cento) em caso de recusa injustificada do adjudicatário em assinar o contrato ou retirar o instrumento equivalente, dentro do prazo estabelecido neste Edital;

XI. 10% (dez por cento) sobre o valor do contrato, pelodescumprimento de qualquer cláusula do contrato, exceto prazo de entrega;

XII. Advertência;

XIII. Suspensão do direito de contratar com o Contratante por até 2 (dois) anos;

XIV. Declaração de inidoneidade para licitar com a Administração Pública

17.5. A multa será formalizada por simples apostilamento contratual, na forma do art. 65, § 8º, da Lei nº 8.666/93 e será executada após regular processo administrativo, oferecido à contratada a oportunidade de defesa prévia, no prazo de 05 (cinco) dias úteis, a contar do recebimento da notificação, nos termos do § 3º do art. 86 da Lei nº 8.666/93, observada a seguinte ordem:

I - mediante desconto no valor da garantia depositada do respectivo contrato;
II - mediante desconto no valor das parcelas devidas à contratada; e
III - mediante procedimento administrativo ou judicial de execução.

17.6. Se a multa aplicada for superior ao valor da garantia prestada, além da perda desta, responderá à contratada pela sua diferença, devidamente atualizada pelo Índice Geral de Preços de Mercado (IGP-M) ou equivalente, que será descontada dos pagamentos

eventualmente devidos pela Administração ou cobrados judicialmente. A contratada terá o prazo de 15 (quinze) dias para apresentar nova garantia contratual.

17.7. O atraso, para efeito de cálculo de multa, será contado em dias corridos, a partir do dia seguinte ao do vencimento do prazo de entrega ou execução do contrato, se dia de expediente normal no Departamento de Engenharia e Construção, ou no primeiro dia útil seguinte.

17.8. Em despacho, com fundamentação sumária, poderá ser relevado:

> I - o atraso não superior a 5 (cinco) dias; e
> II - a execução de multa cujo montante seja inferior ao dos respectivos custos decobrança.

17.9.A multa poderá ser aplicada cumulativamente com outras sanções, segundo a natureza e a gravidade da falta cometida, observado o princípio da proporcionalidade.

17.10. A aplicação das sanções previstas não exclui a possibilidade da responsabilidade civil do Contratado por eventuais perdas e danos causados à Administração Pública. Nos casos em que houver perdas e danos para a Administração, poderá incidir multa compensatória em favor da Contratante, nos termos do art. 408 do CCB e seguintes, no valor de 100%(cem por cento) do valor do contrato por inexecução total deste.

17.11. A multa aplicada deverá ser recolhida ao Tesouro Nacional por meio de GRU (Guia de Recolhimento da União), no prazo máximo de 10 (dez) dias corridos, a contar da data do recebimento da notificação enviada pelo Contratante.

17.12. O valor da multa, no caso de não recolhimento, poderá ser descontado dos pagamentos eventualmente devidos pela Administração ou cobrada judicialmente.

17.13. A licitante convocada dentro do prazo de validade de sua proposta, que deixar de entregar ou apresentar documentação falsa exigida para o certame, ensejar o retardamento da execução de seu objeto, não mantiver a proposta, falhar ou fraudar a execução dos serviços e/ou materiais, comportar-se de modo inidôneo ou cometer fraude fiscal, poderá sofrer sanção de impedimento de licitar com a Administração Pública. Poderá ser descredenciada junto ao SICAF, pelo prazo de 5 (cinco) anos, sem prejuízo das multas previstas neste Edital e das demais cominações legais, garantido o direito do contraditório e da ampla defesa.

18.10. Decorridos 60 (trinta) dias de atraso, a nota de empenho e/ou contrato deverão ser cancelados e/ou rescindidos, exceto se houver justificado interesse da Administração em admitir atraso superior a 60 (sessenta) dias.Neste caso, o atraso não poderá ultrapassar de 15 (quinze) dias corridos, cujo valor da multa diária será igual a multa prevista no nº II do subitem 17.4 deste Edital.

CLÁUSULA DÉCIMA QUARTA – RESCISÃO

14.1. Este contrato poderá ser rescindido se ocorrer um dos casos previstos no art. 78 da Lei 8666/93, que de alguma forma comprometa ou torne duvidoso o cumprimento das obrigações assumidas.

14.2. No caso de rescisão administrativa, a CONTRATANTE poderá executar a garantia de execução para ressarcimento dos valores de multa e indenização a ela devidos e reter os créditos decorrentes deste Contrato até o limite dos prejuízos causados à CONTRATANTE, sem prejuízo das sanções da lei.

14.3. A contratada reconhece os direitos da Administração, em caso de rescisão administrativa prevista no Art. 57 da Lei 8.666/93.

CLÁUSULA DÉCIMA QUINTA - DAS OBRIGAÇÕES

15.1. Da Contratada:

15.1.2.executar os serviços conforme especificado no Termo de Referência, Anexo II a este Edital;

15.1.3.prestar os esclarecimentos solicitados pelo Contratante;

15.1.4.guardar sigilo sobre as informações a que tiver acesso em razão dos serviços prestados, respondendo pela inobservância deste item, inclusive após o término do contrato;

15.1.5.providenciar a assinatura do Termo de Confidencialidade e Sigilo pelos técnicos da Contratada;

15.1.6.manter durante a vigência contratual as condições de habilitação exigidas neste Edital;

15.1.7.dar ciência ao Contratante, por escrito, de qualquer anormalidade que verificar na execução dos serviços;

15.1.8.corrigir, sem ônus para o Contratante, os defeitos, omissões ou quaisquer irregularidades dos serviços executados, ainda que identificados após o ateste dos serviços pelo Contratante;

15.1.9.apresentar a relação dos funcionários que irão prestar os serviços para a execução contratual perante o contratante, entre eles um responsável técnico e o preposto, estas duas funções poderão ser acumuladas;

15.1.10.responder pelas despesas relativas a encargos trabalhistas, seguro de acidentes, impostos, contribuições previdenciárias, deslocamentos de técnicos, postagem de software e quaisquer outras despesas que forem devidas e referentes aos serviços executados por seus funcionários, visto que os mesmos não possuem nenhum vinculo empregatício com o Contratante;

15.1.11. prestar suporte "on site", caso o chamado não possa ser resolvido por meio eletrônico;

15.1.12.fornecer documentação técnica detalhada sobre as atualizações do produto;

15.1.13.prestar informações e orientações necessárias à utilização e ao perfeito funcionamento dos softwares e hardwares instalados;

15.1.14.refazer serviços quando apresentarem padrões de qualidade inferiores aos definidos neste edital, sem ônus adicionais para o Contratante, nos prazos estabelecidos em contrato, contados a partir da notificação;

15.1.15.prestar os serviços conforme a quantidade, a qualidade e a pontualidade exigidas neste Edital;

15.1.16.não transferir a outrem, no todo ou em parte, os serviços contratados;

15.1.17. enquanto durar o contrato, a contratada terá que disponibilizar atendimento para abertura de chamados de assistência técnica através de discagem direta local para o município de Brasília/DF, 24 horas e 7 dias por semana, ou disponibilizar um serviço de chamada gratuita para chamadas interurbanas, caso a Contratada não disponha de instalação no município de Brasília/DF;

15.1.18.comprovar a especialização e certificação dos técnicos envolvidos na instalação, com certificados emitidos pelo fabricante da solução ou por entidades credenciadas pelos fabricantes dos equipamentos e/ou softwares propostos;

15.1.19.possuir atestados de capacidade técnica, em seu nome emitido por Pessoa Jurídica de Direito Publico ou Privado, comprovando que realizou serviços de instalação e manutenção de hardware do equipamento ofertado;

15.1.20.comprovar que existe em seu quadro de funcionários, na data da assinatura do contrato, profissional detentor de certificado emitido pelo fabricante da ferramenta ofertada, ou por entidades credenciadas pelos fabricantes (sejam hardwares ou softwares);

15.1.21.enquanto durar o contrato, atender ao pedido de assistência técnica no local dos sistemas e equipamentos instalados na sede do Contratante, 24 (vinte quatro) horas por dia, 7 (sete) dias por semana e dar encaminhamento ao problema em até 24 (vinte e quatro) horas do dia seguinte ao da abertura do chamado;

15.1.22.atender ao pedido de assistência técnica por telefone, fax ou e-mail dos sistemas e equipamentos instalados nas cidades de Brasília durante todo o período de garantia, nos dias úteis (segunda a sexta-feira), no horário comercial (8 às 18 horas) e dar encaminhamento ao problema em até 24 (vinte e quatro) horas do dia seguinte ao da abertura do chamado;

15.1.23.providenciar, durante o período de vigência de contrato e suas possíveis renovações, atualização e "upgrade" de versão, bem como, patches corretivos para todos os sistemas fornecidos;

15.1.24.fornecer senha de acesso ao site do fabricante do software, com permissão para o Contratante efetuar download de novas versões e patches.

15.1.25.indenizar às suas expensas, quaisquer danos causados a terceiros em decorrência do cumprimento do presente edital;

15.2. Da Contratante:

15.2.1.efetuar o pagamento do objeto deste contrato nas condições estabelecidas por este instrumento e, após a conferência realizada pela equipe de fiscalização do Contratante, bem como realizar a retenção dos tributos e impostos, em conformidade com a legislação pertinente;

15.2.2.efetuar as requisições, de conformidade com a discriminação constante deste edital;

15.2.3.proporcionar condições necessárias ao fornecimento dos produtos solicitados;

15.2.4.prestar informações e esclarecimentos que venham a ser solicitados pela Contratada com relação ao objeto desta licitação;

15.2.5.fiscalizar e acompanhar a execução e a entrega do objeto desta licitação; e

15.2.6.comunicar à Contratada toda e qualquer ocorrência relacionada com a entrega do objeto, diligenciando nos casos que exigem providências corretivas.

15.2. DA CONTRATANTE

15.2.1. Efetuar o pagamento do objeto deste contrato nas condições estabelecidas por este instrumento e no Edital de licitação anexo a este Instrumento, após a conferência realizada pelo Fiscal Administrativo do DEC e realizar a reter dos tributos, em conformidade com a legislação pertinente.

15.2.2. Efetuar as requisições, de conformidade com a discriminação constante deste edital.

15.2.3. Proporcionar todas as facilidades necessárias ao fornecimento dos produtos solicitados.

15.2.4. Prestar as informações e os esclarecimentos que venham a ser solicitados pela licitante vencedora com relação ao objeto desta licitação.

15.2.5. Fiscalizar e acompanhar a execução e entrega do objeto desta licitação.

15.2.6. Comunicar à licitante toda e qualquer ocorrência relacionada com a entrega do objeto, diligenciando nos casos que exigem providencias corretivas.

CLÁUSULA DÉCIMA SEXTA– COMUNICAÇÃO

- Qualquer notificação, solicitação ou comunicação que as partes devam enviar uma à outra, em virtude deste Contrato, será feita por escrito e considerar-se-á efetuada no momento em que o documento for entregue ao destinatário nos endereços a seguir indicados:

CONTRATANTE: COMANDO DO EXÉRCITO

DEPARTAMENTO DE ENGENHARIA E CONSTRUÇÃO

QGEx - Bloco “B” – 3º PISO - SMU

Brasília –DF

CEP: 70630-901

CONTRATADA: _____

CLÁUSULA DÉCIMA SÉTIMA – ALTERAÇÃO CONTRATUAL

- Qualquer alteração neste Contrato será feita por Termo Aditivo e obedecerá as mesmas formalidades deste Contrato.

CLÁUSULA DÉCIMA OITAVA – HABILITAÇÃO E QUALIFICAÇÃO

- A CONTRATADA obriga-se a manter, durante toda a execução deste Contrato, em compatibilidade com as obrigações por ela assumidas, todas as condições de habilitação e qualificação exigidas.

CLÁUSULA DÉCIMA NONA – CESSÃO OU TRANSFERÊNCIA

- O presente Contrato não poderá ser objeto de cessão ou transferência, no todo ou em parte.

CLÁUSULA VIGÉSIMA – ANEXOS

- Constituem anexos deste Contrato, dele fazendo parte integrante:

20.1. A proposta da CONTRATADA, de _____ de ____de _____

20.2. Especificações Técnicas;

20.3.Notas de Empenho 2012NE _____ de ____ de _____

20.4.Cronograma de entrega.

CLÁUSULA VIGÉSIMA PRIMEIRA – DA PUBLICIDADE

- O DEC fará publicar no DOU o extrato do presente contrato, de acordo com o § único do Art. 61 da Lei 8666/93 e Art. 13 da IN Nr 08, de 04 Dez 98-MARE.

CLÁUSULA VIGÉSIMA SEGUNDA – DA VIGÊNCIA

22.1 O prazo de vigência do presente contrato será a contar de sua assinatura até 12meses (prazo de entrega somado ao prazo de garantia de fábrica somado ao prazo de garantia estendida) e eficácia na data da publicação no DOU.

22.2 O prazo de vigência supra rende-se aos aspectos de vigência das garantias.

CLÁUSULA VIGÉSIMA TERCEIRA – DA COMPROVAÇÃO DA ORIGEM DOS BENS IMPORTADOS OFERECIDOS

- Deverá ser comprovado a origem dos bens importados oferecido se da quitação dos tributos de importação a eles referentes, que deve ser apresentada no momento da entrega do objeto, sob pena de rescisão contratual e multa.

CLÁUSULA VIGÉSIMA QUARTA - DAS FERRAMENTAS DE MEDIÇÃO

- O Departamento de Engenharia e Construção por intermédio da Assessoria Especial de Tecnologia e Informação (AETI), utilizará as ferramentas de medição para aferir o desempenho dos bens ofertados, quando for o caso.

CLÁUSULA VIGÉSIMA QUINTA – FORO

- As questões decorrentes da execução deste Edital, que não possam ser dirimidas administrativamente, serão processadas e julgadas na Justiça Federal, no Foro da cidade de Brasília/DF, Seção Judiciária do Distrito Federal, com exclusão de qualquer outro.

E, por estarem justos e contratados, preparam este instrumento, em 03 (três) vias de igual teor, para um só efeito, que depois de lido e achado conforme será assinado pelas partes contratantes e duas testemunhas, para que produza os efeitos legais, comprometendo-se as partes contratantes a cumprir o presente Contrato em todas as suas cláusulas.

Brasília-DF, _____ de_____ de 2013.

_____ CPF: Ordenador de Despesas do DEC	_____ CPF: Representante da empresa _____
_____ CPF: 1ª Testemunha	_____ CPF: 2ª Testemunha

MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
DEPARTAMENTO DE ENGENHARIA E CONSTRUÇÃO
(Departamento Técnico e de Produção do Exército/1946)

ANEXO VIII - MINUTA DA ATA DE REGISTRO DE PREÇOS

PREGÃO ELETRÔNICO PARA REGISTRO DE PREÇOS Nº 017/2013-DEC

ATA DE REGISTRO DE PREÇOS

PROCESSO ADMINISTRATIVO Nº 118/ 2013

VALIDADE: 12 (DOZE) MESES

Aos ____ de _____ de _____ , no DEPARTAMENTO DE ENGENHARIA E CONSTRUÇÃO (DEC) – Órgão de Direção Setorial do Comando do Exército, localizado no Quartel General do Exército – Bl "B" – 3º piso, nesta Capital Federal, o pregoeiro, nos termos da Lei nº 10.520, de 17 de julho de 2002, publicada no D. O. de 18 de julho de 2002, e os Decretos nºs 3.555, de 08 de agosto de 2000, publicado no D.O. de 09 de agosto de 2000, 4.342, de 23 de agosto de 2002, publicado no D.O. de 26 de agosto de 2002, 3.931, de 19 de setembro de 2001, 5.450 de 31 de maio de 2005, e 3.784, de 06 de abril de 2001, publicado no D.O. de 09 de abril de 2001, em decorrência da aceitação, habilitação, adjudicação e homologação da proposta apresentada no **Pregão Eletrônico para Registro de Preços nº 17/2013-DEC** - **Processo Administrativo nº 118/2013-DEC** e do Aviso de Julgamento de Preços e Ato de Homologação da Ordenador de Despesas do DEC, publicada no Diário Oficial da União do dia ___ de _____ de 2013, **RESOLVE** registrar o(s) preço(s) do(s) **item(ns) descritos na cláusula primeira,** para à empresa _____, **CNPJ** _____ .

CLÁUSULA PRIMEIRA – DO OBJETO

Registro de Preços para aquisição **de material de Informática para o DEC** do(s) **item (ns) Nr** _____, _____ (especificar o objeto de acordo com o anexo I do edital), conforme as condições e as especificações técnicas constantes do Termo de Referência – anexo _____ do edital, no valor unitário de R$ _____ , de acordo com o encarte anexo.

CLÁUSULA SEGUNDA - DA VALIDADE DOS PREÇOS

2.1. A presente Ata de Registro de Preços terá a **validade de 12 (doze) meses**, **a partir de ____ de _____ de 2013a _____ de _____ de _____.**

2.2. Durante o prazo de validade desta Ata de Registro de Preços, o DEC não será obrigado a adquirir o material referido na Cláusula Primeira exclusivamente pelo Sistema de Registro de Preços, podendo fazê-lo através de outra licitação quando julgar conveniente, sem que caiba recurso ou indenização de qualquer espécie à empresa detentora ou, cancelar a Ata, na ocorrência de alguma das hipóteses legalmente previstas para tanto, garantidos à detentora, neste caso, o contraditório e a ampla defesa.

CLÁUSULA TERCEIRA - DA UTILIZAÇÃO DA ATA DE REGISTRO DE PREÇOS

3.1. Serão usuários do Registro de Preços o órgão vinculados ao Comando do Exército e outros que órgãos que aderirem a IRP (Intenção de Registro de Preços).

3.2. O preço ofertado pela empresa signatária da presente Ata de Registro de Preços é o especificado na cláusula primeira e aquele constante nos registros eletrônicos do pregão.

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

3.4. Os órgãos e entidades que não participaram do registro de preços, quando desejarem fazer uso da ata de registro de preços, deverão consultar o órgão gerenciador da ata para manifestação sobre a possibilidade de adesão.

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

3.6. As aquisições ou contratações adicionais a que se refere este artigo não poderão exceder, por órgão ou entidade, a cem por cento dos quantitativos dos itens do instrumento convocatório e registrados na ata de registro de preços para o órgão gerenciador e órgãos participantes, limitadas as caronas ao quíntuplo das quantidades totais registradas.

3.7. O órgão gerenciador somente poderá autorizar adesão à ata após a primeira aquisição ou contratação por órgão integrante da ata, exceto quando, justificadamente, não houver previsão no edital para aquisição ou contratação pelo órgão gerenciador.
3.8. Após a autorização do órgão gerenciador, o órgão não participante deverá efetivar a aquisição ou contratação solicitada em até noventa dias, observado o prazo de vigência da ata.
3.9. Compete ao órgão não participante os atos relativos à cobrança do cumprimento pelo fornecedor das obrigações contratualmente assumidas e a aplicação, observada a ampla defesa e o contraditório, de eventuais penalidades decorrentes do descumprimento de cláusulas contratuais, em relação às suas próprias contratações, informando as ocorrências ao órgão gerenciador.
3.10. É facultada aos órgãos ou entidades municipais, distritais ou estaduais a adesão a ata de registro de preços da administração pública federal.
3.11. Para cada material de que trata esta Ata, serão observadas, quanto ao preço, as cláusulas e condições constantes do Edital do PREGÃO ELETRÔNICO PARA REGISTRO DE PREÇOS Nº. 017/2013, **que o precedeu e integra o presente instrumento de compromisso, bem como a** proposta apresentada pela empresa.

CLÁUSULA QUARTA - DO LOCAL E PRAZO DE ENTREGA

4.1. O recebimento, o local e o prazo de entrega dos bens deverão ocorrer de acordo com o Edital. Os materiais e a instalação, configuração, treinamento e operação deverão ocorrer no Departamento de Engenharia e Construção, sito na Avenida do Exército – QG Ex – Bloco "B" – 3º Piso – Brasilia-DF.
4.2. A empresa deverá comunicar ao **DEC,** com **72 horas** de antecedência, a data e o horário previsto para a entrega dos materiais, que só poderá ocorrer no período compreendido entre 09:00h e 11:00H e 13:30h e 16:00h, de Segunda a Quinta-feira e de 08:00h e 11:00h de Sexta-feira.

CLÁUSULA QUINTA - DO PAGAMENTO

5.1. O pagamento será efetuado em uma única parcela mediante apresentação da Nota Fiscal, discriminada de acordo com a Nota de Empenho. Observados o recebimento provisório e definitivo, a Nota Fiscal, emitida pela empresa e entregue no Almoxarifado do DEC com discriminação dos bens, após atestada, será encaminhada ao Setor Financeiro para liquidação e pagamento.

5.2. O pagamento será creditado em favor do FORNECEDOR por meio de ordem bancária. Para isso deverá ser indicada na Nota Fiscal o nome do Banco, agência, localidade e número da conta corrente em que deverá ser efetivado o crédito. Será procedida consulta **"ON LINE"** junto ao **SICAF** antes de cada pagamento para verificação da situação do fornecedor, relativamente às condições exigidas na contratação, cujos resultados serão impressos e juntados aos autos do processo próprio.
5.3. Caso haja aplicação de multa, o valor será descontado de qualquer fatura ou crédito existente junto ao DEC. Caso o mesmo seja superior ao crédito eventualmente existente, a diferença será cobrada administrativamente ou judicialmente, se necessário.

CLÁUSULA SEXTA - DAS CONDIÇÕES DE FORNECIMENTO

A entrega do produto só estará caracterizada após a liquidação da despesa pelo DEC. **O fornecedor ficará obrigado a atender todos os pedidos efetuados durante a vigência desta Ata, mesmo que a entrega dos itens estiver prevista para data posterior à expiração da ATA.**

CLÁUSULA SÉTIMA - DO CANCELAMENTO DA ATA DE REGISTRO DE PREÇOS.

A Ata de Registro de Preços poderá ser cancelada pela Administração:
a) Automaticamente:
1) por decurso de prazo de vigência;
2) quando não restarem fornecedores registrados;
3) pelo DEC, quando caracterizado o interesse público.
b) A pedido, quando:
1) o fornecedor comprovar estar impossibilitado de cumprir as exigências da Ata, por ocorrência de casos fortuitos ou de força maior;
2) o seu preço registrado se tornar, comprovadamente, inexeqüível em função da elevação dos preços de mercado e dos insumos que compõem o custo dos materiais.
A solicitação dos fornecedores para cancelamento dos preços registrados deverá ser formulada com a antecedência de **30** (trinta) dias, facultada à Administração a aplicação das penalidades previstas na Cláusula Sétima, caso não aceitas as razões do pedido.
c) Por iniciativa do DEC, quando:
1) o fornecedor não aceitar reduzir o preço registrado, na hipótese deste se tornar superior àqueles praticados no mercado;

2) o fornecedor perder qualquer condição de habilitação ou qualificação técnica exigida no processo licitatório;

3) o fornecedor não cumprir as obrigações decorrentes desta Ata de Registro de Preços;

4) o fornecedor não comparecer ou se recusar a retirar, no prazo estabelecido, os pedidos decorrentes desta Ata de Registro de Preços;

5) caracterizada qualquer hipótese de inexecução total ou parcial das condições estabelecidas nesta Ata de Registro de Preço ou nos pedidos dela decorrentes.

CLÁUSULA OITAVA – DAS OBRIGAÇÕES

24.1. DA CONTRATADA

24.1.1. Executar o objeto, descrito, nas condições de sua proposta e de acordo com as especificações constantes do Edital que deu origem ao presente instrumento. O serviço objeto desta licitação será recebido obedecida a adequação eas características técnicas exigidas no termo de referência do edital;

24.1.2. Indenizar às suas expensas, quaisquer danos causados a terceiros em decorrência do cumprimento do presenteedital;

24.1.3. Assumir todos os encargos trabalhistas, previdenciários, securitários, fiscais, tributários e quaisquer outros resultantes da execução deste Contrato, os quais já estão incluídos no custo total, ficando a Contratante isenta do pagamento de quaisquer obrigações decorrentes da execução deste instrumento contratual;

24.1.4. Manter durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação, que serão confirmadas pela Contratante por meio de consulta “on line” no SICAF.

24.2. DA CONTRATANTE

24.2.1. Efetuar o pagamento do objeto deste contrato nas condições estabelecidas por este instrumento e no Edital de licitação anexo a este Instrumento, após a conferência realizada pelo Fiscal Administrativo do DEC e realizar a retenção dos tributos, em conformidade com a legislação pertinente.

24.2.2. Efetuar as requisições, de conformidade com a discriminação constante deste edital.

24.2.3. Proporcionar todas as facilidades necessárias ao fornecimento dos produtos solicitados.

24.2.4. Prestar as informações e os esclarecimentos que venham a ser solicitados pela licitante vencedora com relação ao objeto desta licitação.

24.2.5. Fiscalizar e acompanhar a execução e entrega do objeto desta licitação.

24.2.6. Comunicar à licitante toda e qualquer ocorrência relacionada com a entrega do objeto, diligenciando nos casos que exigem providencias corretivas.

CLÁUSULA NONA - DAS DISPOSIÇÕES FINAIS

11.1. Integram esta ATA o edital do PREGÃO ELETRÔNICO PARA REGISTRO DE PREÇOS Nº 017/2013-DEC e a proposta da empresa: _____, apresentada no certame mencionado.

11.2. Os casos omissos serão resolvidos com observância das disposições constantes da Lei 8.666/93 e dos Decretos nº 3.555/2000, 3.931/2001, 3.784/2001, 4.342/2002 e 5.450/2005.

11.3. As questões decorrentes da utilização da presente ATA, que não puderem ser dirimidas administrativamente, serão processadas e julgadas na Justiça Federal no foro da cidade de Brasília – DF, Seção Judiciária do Distrito Federal, com exclusão de qualquer outro.

Brasília-DF, _____ de _____ de 2013.

_____

xxxxxxxxxxxxxxxxxx

Ordenador de Despesas do Departamento de Engenharia e Construção

_____

Pregoeiro

_____

XXXXXXX

Representante da Empresa

PREGÃO ELETRÔNICO Nr 017/2013 - REGISTRO DE PREÇOS

ENCARTE À ATA

Empresa: _____ , CNPJ Nr _____, com sede na cidade de _____, Av/Rua/Quadra _____ , Fone: (XX) _____ , Fax: (XX) _____, representada neste ato pelo Sr.(a) _____, CPF Nr _____, RG Nr _____.

ITEM	ESPECIFICAÇÃO	MARCA	UNIDADE	QTD GLOBAL	UNITÁRIO	TOTAL

(PAPEL TIMBRADO)

ANEXO IX

MODELO DE DECLARAÇÃO DE ELABORAÇÃO
(INDEPENDENTE DE PROPOSTA)

(Identificação da Licitante)

(Identificação completa do representante da licitante) como representante devidamente constituído de (identificação completa da licitante ou do consorcio) doravante denominada (licitante/consórcio) para fins do disposto no item (completar) do Edital (completar com identificação do Edital), declara sob as penas da Lei, em especial o Art 299 do Código Penal Brasileiro que:

(a) a proposta apresentada para participar da (identificação da licitação), foi elaborada de maneira independente (pelo licitante/consórcio) e o conteúdo da proposta não foi,no todo ou em parte, direta ou indiretamente, informado, discutido ou recebido de qualquer outro participante potencial ou de fato da (identificação da licitante), por qualquer meio ou por qualquer pessoa;

(b) a intenção de apresentar a proposta elaborada para participar da (identificação da licitação) não foi informada, discutida ou recebida de qualquer outro participante potencial ou de fato (identificação da licitante), por qualquer meio ou por qualquer pessoa;

(c) que não tentou, por qualquer meio ou por qualquer pessoa, influir na decisão de qualquer outro participante potencial ou de fato da (identificação da licitação) quanto a participar ou não da referida licitação;

(d) que o conteúdo da proposta apresentada para participar da (identificação da licitação) não será no todo ou parte direta ou indiretamente comunicado ou discutido com qualquer outro participante potencial ou de fato da (identificação da licitante) antes da adjudicação do objeto da referida licitação;

(e) que o conteúdo da proposta apresentada para participar (identificação da licitação) não foi, no todo ou em parte direta ou indiretamente informado, discutido ou recebido de qualquer integrante de (órgão licitante) antes da abertura oficial das propostas; e

(f) que está plenamente ciente do teore da extensão desta declaração e que detém plenos poderes e informações para firma-la.

_____, em____de_____de_____

_____
(representante legal do licitante/consórcio, no âmbito da licitação, com identificação completa)

ANEXO X

DECLARAÇÃO DE PREFERÊNCIA DE CONTRATAÇÃO

_____(IDENTIFICAÇÃO DA LICITAÇÃO)

(**IDENTIFICAÇÃO COMPLETA DO REPRESENTANTE DA LICITANTE**), COMO REPRESENTANTE DEVIDADEMENTE CONSTITUÍDO DE(**IDENTIFICAÇÃO COMPLETA DA LICITANTE OU DO CONSÓRCIO**) DORAVANTE DENOMINADO (**LICITANTE/CONSÓRCIO**), PARA FINS DO DISPOSTO NO ITEM (**COMPLETAR**) DO EDITAL (**COMPLETAR COM IDENTIFICAÇÃO DO EDITAL**), DECLARA, SOB AS PENAS DA LEI, EM ESPECIAL O ART. 299 DO CÓDIGO PENAL BRASILEIRO, QUE :

POSSUO A CERTIFICAÇÃO DE TECNOLOGIA DESENVOLVIDA NO PAÍS, NOS TERMOS DA LEI Nº 8.248, DE 23 DE OUTUBRO DE 1991 E DOS DECRETOS Nº 5.906, DE 26 DE SETEMBRO DE 2006, OU PELO DECRETO Nº 6.008, DE 29 DE DEZEMBRO DE 2006;

POSSUO A CERTIFICAÇÃO DE PROCESSO PRODUTIVO BÁSICO, NOS TERMOS DA LEI Nº 8.248, DE 23 DE OUTUBRO DE 1991 E DOS DECRETOS Nº 5.906, DE 26 DE SETEMBRO DE 2006, OU PELO DECRETO Nº 6.008, DE 29 DE DEZEMBRO DE 2006;

AINDA, DECLARA, QUE ESTÁ PLENAMENTE CIENTE DO TEOR E DA EXTENSÃO DESTA DECLARAÇÃO E QUE DETÉM PLENOS PODERES E INFORMAÇÕES PARA FIRMÁ-LA.

_____EM____DE_____DE _____

_____

(NOME COMPLETO)
(REPRESENTANE LEGAL DO LICITANTE/CONSÓRCIO, NO AMBITO DO PREGÃO ELETRÔNICO 64/2010-DEC-SRP)
CPF:

RG:

ANEXO XI

MODELO DO TERMO DE CONFIDENCIALIDADE DE SIGILO (PARA A EMPRESA CONTRATADA)

_____(IDENTIFICAÇÃO DA LICITAÇÃO)

A Empresa _____ (Nome da Empresa)**, inscrita no CNPJ sob o nº** 00000, abaixo firmado, assume o compromisso de manter confidencialidade e sigilo sobre todas as informações técnicas e outras relacionadas ao contrato nº ____ , celebrado para **a implantação de uma solução de segurança e comunicação unificada na infraestrutura de tecnologia da Informação do Departamento de Engenharia e Construção ,** Organização Militar do Exército Brasileiro, inscrito no CNPJ nº 07.521.315/0001-23, torna público que terá acesso as instalações da Contratante para cumprir o objeto contratado e que por meio deste termo de confidencialidade de sigilo compromete-se a:

1. A não utilizar as informações confidenciais a que tiver acesso, para gerar benefício próprio exclusivo e/ou unilateral, presente ou futuro, ou para o uso de terceiros;

2. A não efetuar nenhuma gravação ou cópia da documentação confidencial a que tiver acesso;

3. A não apropriar-se para si ou para outrem de material confidencial e/ou sigiloso da tecnologia que venha a ser disponível ou implantada;

4. A não repassar o conhecimento das informações confidenciais, responsabilizando-se por todas as pessoas que vierem a ter acesso às informações, por seu intermédio, e obrigando-se, assim, a ressarcir a ocorrência de qualquer dano e / ou prejuízo oriundo de uma eventual quebra de sigilo das informações fornecidas.

Neste Termo, as seguintes expressões serão assim definidas:

Informação Confidencial significará toda informação revelada através da apresentação da tecnologia, a respeito de, ou, associada com a Avaliação, sob a forma escrita, verbal ou por quaisquer outros meios.

Informação Confidencial inclui, mas não se limita, à informação relativa às operações, processos, planos ou intenções, informações sobre produção, instalações, equipamentos, segredos de negócio, segredo de fornecedores, dados, habilidades especializadas, projetos, métodos e metodologia, fluxogramas, especializações, componentes, fórmulas, produtos, amostras, diagramas, desenhos técnicos e/ou projetos, patentes, oportunidades de mercado e questões relativas a negócios revelados da tecnologia supra mencionada.

Avaliação significará todas e quaisquer discussões, conversações ou negociações entre, ou com as partes, de alguma forma relacionada ou associada com a implantação da solução contratada.

A vigência da obrigação de confidencialidade e sigilo, assumida neste termo, terá a validade enquanto a informação não for tornada de conhecimento público pela contratante, ou mediante autorização escrita, concedida à empresa pelas partes interessadas neste termo.

Pelo não cumprimento do presente Termo de Confidencialidade e Sigilo, fica o abaixo assinado ciente de todas as sanções judiciais que poderão advir.

Brasília/DF, ____/____/_____

_____

(NOME COMPLETO)
(REPRESENTANE LEGAL DO LICITANTE/ NO AMBITO DO CONTRATO Nº _____ REFERENTE AO PREGÃO ELETRÔNICO __/2013-DEC-SRP)
CPF:

RG:

ANEXO XII

MODELO DO TERMO DE CONFIDENCIALIDADE DE SIGILO (PARA OS FUNCIONÁRIOS DA EMPRESA CONTRATADA)

_____(IDENTIFICAÇÃO DA LICITAÇÃO)

Eu _____ (Nome do Funcionário), Identidade nº_____, CPF nº_____ matrícula nº _____ (ou nº do contrato de trabalho), funcionário da Empresa _____ (Nome da Empresa)**, inscrita no CNPJ sob o nº** 00000, abaixo firmado, assumo o compromisso de manter confidencialidade e sigilo sobre todas as informações técnicas e outras relacionadas ao contrato nº ____ , celebrado para **a implantaçãode uma solução de segurança e comunicação unificada na infraestrutura de Tecnologia da Informação do Departamento de Engenharia e Construção ,** Organização Militar do Exército Brasileiro, inscrito no CNPJ nº 07.521.315/0001-23, torno público que terei acesso as instalações da Contratante para cumprir o objeto contratado e que por meio deste termo de confidencialidade de sigilo comprometo-me a:

1. A não utilizar as informações confidenciais a que tiver acesso, para gerar benefício próprio exclusivo e/ou unilateral, presente ou futuro, ou para o uso de terceiros;

2. A não efetuar nenhuma gravação ou cópia da documentação confidencial a que tiver acesso;

3. A não apropriar-se para si ou para outrem de material confidencial e/ou sigiloso da tecnologia que venha a ser disponível ou implantada;

4. A não repassar o conhecimento das informações confidenciais, responsabilizando-se por todas as pessoas que vierem a ter acesso às informações, por seu intermédio, e obrigando-se, assim, a ressarcir a ocorrência de qualquer dano e / ou prejuízo oriundo de uma eventual quebra de sigilo das informações fornecidas.

Neste Termo, as seguintes expressões serão assim definidas:

Informação Confidencial significará toda informação revelada através da apresentação da tecnologia, a respeito de, ou, associada com a Avaliação, sob a forma escrita, verbal ou por quaisquer outros meios.

Informação Confidencial inclui, mas não se limita, à informação relativa às operações, processos, planos ou intenções, informações sobre produção, instalações, equipamentos, segredos de negócio, segredo de fornecedores, dados, habilidades especializadas, projetos, métodos e metodologia, fluxogramas, especializações, componentes, fórmulas, produtos, amostras, diagramas, desenhos técnicos e/ou projetos,

patentes, oportunidades de mercado e questões relativas a negócios revelados da tecnologia supra mencionada.

Avaliação significará todas e quaisquer discussões, conversações ou negociações entre, ou com as partes, de alguma forma relacionada ou associada com a implantação da solução contratada.

A vigência da obrigação de confidencialidade e sigilo, assumida neste termo, terá a validade enquanto a informação não for tornada de conhecimento público pela contratante, ou mediante autorização escrita, concedida à empresa pelas partes interessadas neste termo.

Pelo não cumprimento do presente Termo de Confidencialidade e Sigilo, fica o abaixo assinado ciente de todas as sanções judiciais que poderão advir.

Brasília/DF, ____/____/_____

_____

(NOME COMPLETO DO FUNCIONÁRIO)
(REPRESENTANE LEGAL DO LICITANTE/ NO AMBITO DO CONTRATO Nº _____ REFERENTE AO PREGÃO ELETRÔNICO __/2013-DEC-SRP)
CPF:
RG:

_____

(NOME COMPLETO)
(REPRESENTANE LEGAL DO LICITANTE/ NO AMBITO DO CONTRATO Nº _____ REFERENTE AO PREGÃO ELETRÔNICO __/2013-DEC-SRP)
CPF:
RG: