

<b>Câmara Municipal de Anchieta/ES</b>	
<b>Licitação PREGÃO PRESENCIAL Nº 03/2011</b> (Regido pela Lei Federal n. 10.520/2002 e, subsidiariamente, pela Lei Federal n.8.666/93, pela Lei Complementar 123 e demais normas pertinentes e pelas condições estabelecidas no presente edital)	
TIPO:	<b>"Menor Preço por Lote"</b>
OBJETO:	<b>Aquisição de SOFTWARE de Gerenciamento de Backup, aquisição e implantação de nova Solução de Segurança (antivírus), aquisição de um servidor para rack e implantação de soluções baseadas no MS Windows Server 2008, nos moldes da descrição constante no Anexo I deste edital.</b>

DIA:	<b>06/07/2011 (Quarta-feira)</b>
HORA:	<b>15:00 horas</b>
LOCAL:	<b>Câmara Municipal de Anchieta/ES</b>
ENDEREÇO:	<b>Rua Nancy Ramos Rosa, 87, Portal de Anchieta, Anchieta/ES, CEP: 29230-000</b>
INFORMAÇÕES:	<b>Fone: 0 xx (28) 35360304 E-mail: pregão@camaraanchieta.es.gov.br</b>
PROCESSO:	<b>Nº 87/2011</b>

A Câmara Municipal de Anchieta, através do PREGOEIRO designado pela Resolução – MDC nº 109/2011, torna público para conhecimento dos interessados que na data, horário e local acima indicados, com obediência ao disposto na **Lei n. 10.520 e, subsidiariamente, pela Lei Federal n.8.666/93, pela Lei Complementar e demais normas pertinentes e pelas condições estabelecidas no presente edital**, fará realizar Licitação na modalidade **PREGÃO PRESENCIAL**, do tipo **MENOR PREÇO**, destinada à contratação do objeto de que trata o Anexo I do presente Edital.

## 1. DO OBJETO

**1.1** Constitui objeto da presente licitação a **AQUISIÇÃO DE SOFWARES**, de acordo com as especificações constantes do Anexo I (Termo de Referência).

**1.2** Constituem os Anexos do presente edital:

- a) Anexo I : Termo de Referência;
- b) Anexo II : Planilha de Orçamento Estimado;
- c) Anexo III : Modelo de Declaração (Item 8.1, alínea "a", do Edital);

- d) Anexo IV : Modelo de Declaração ref. Art. 7º, XXXIII, CF/88;  
 e) Anexo V : Modelo de Carta de Representação;  
 f) Anexo VI : Modelo de Minuta do Contrato

## 2. DOS RECURSOS ORÇAMENTÁRIOS

a) Exercício	: 2011
b) Dotações	: 333903900000 e 344905200000
c) Atividade	: 001001.0103100012.001
d) Valor estimado	: R\$ 35.166,00

## 3. DAS CONDIÇÕES PARA PARTICIPAÇÃO

**3.1** Poderão participar da presente licitação empresas do ramo do objeto da licitação que no dia, hora e local designados para a realização do Pregão se fizerem representar na forma do Item 4 deste Edital.

**3.2** Não será admitida a participação na presente licitação de empresas que se encontrem em uma ou mais das seguintes situações:

- a) em processo de falência, sob concurso de credores, em dissolução ou liquidação;
- b) reunidas em consórcio, qualquer que seja sua forma de constituição;
- c) estrangeiras que não funcionem no país;
- d) que tenham sido suspensas do direito de licitar por ato desta Administração ou que tenham sido declaradas inidôneas por qualquer órgão da Administração Pública.

## 4. DO CREDENCIAMENTO

**4.1** Antes da abertura dos envelopes de propostas, ocorrerá a **fase de credenciamento**, onde serão vistos e identificados os representantes das licitantes.

**4.1.1.** Uma vez dado início ao credenciamento no horário previsto no preâmbulo deste Edital, não serão mais aceitos novos participantes no certame.

**4.2. Somente poderão participar da fase de lances verbais desta licitação empresas que atendendo as condições estabelecidas no item 3, no dia, hora e local da realização do Pregão se fizerem representar por pessoa com poderes para formular ofertas e lances verbais, negociar preços, declarar a intenção de interpor recurso, renunciar ao direito de interposição de recursos, enfim, para praticar em nome da licitante todos os atos pertinentes a este Pregão** comprovados tais poderes da seguinte forma:

- a) se titular, diretor, sócio ou gerente: através de cópia do estatuto ou contrato social, ou instrumento específico que lhe confira poderes para tanto (**com firma reconhecida**), devendo identificar-se exibindo a carteira de identidade ou outro documento equivalente;
- b) se por outra pessoa: mediante apresentação de instrumento público ou particular de mandato (procuração) (**com firma reconhecida**), **com poderes para formular ofertas e lances de preço e praticar todos os demais atos pertinentes ao certame em nome da**

representada, inclusive renúncia ao direito de interpor e desistir de recursos, devendo igualmente identificar-se exibindo a carteira de identidade ou outro documento equivalente.

**Obs.: Os instrumentos previstos nas alíneas "a" e "b" poderão ser substituídos por Carta de Representação (com firma reconhecida), podendo ser utilizado o modelo constante do Anexo V deste Edital.**

4.2.1 A autenticação dos documentos poderá ser feita pelo Pregoeiro Oficial ou por qualquer outro membro da equipe de apoio.

4.3. **Os documentos referidos nas alíneas "a" e "b" do item 4.2, deverão ser apresentados em separado dos envelopes referidos no item 5, durante o ato específico para o credenciamento e/ou representação**, e em forma de cópias autenticadas ou acompanhadas dos originais, estes para fins de conferência, sendo que as primeiras farão, posteriormente, parte dos autos.

4.4. **O representante da licitante que não se credenciar perante o Pregoeiro ficará impedido de participar da fase de lances verbais, de negociação de preços, de declarar a intenção de interpor recurso, de renunciar ao direito de interposição de recursos**, enfim, para representar a licitante durante a reunião de abertura dos envelopes "Proposta de Preços" ou "Documentação" relativos a este **Pregão**.

4.4.1 **Nesse caso, a licitante ficará excluída da etapa de lances verbais, sendo mantido, porém, o seu preço apresentado na proposta escrita, para efeito de ordenação das propostas e apuração do menor preço.**

## **5 DA PARTICIPAÇÃO DE MICRO-EMPRESA E EMPRESA DE PEQUENO PORTE**

5.1 Nos termos dos artigos 42 e 43 da Lei Complementar nº 123, de 14/12/2006, as microempresas e empresas de pequeno porte deverão apresentar toda a documentação exigida para efeito de comprovação de regularidade fiscal, conforme item 9 deste edital, mesmo que esta apresente alguma restrição.

5.1.1 Havendo alguma restrição na comprovação da regularidade fiscal, será assegurado o prazo de 4 (quatro) dias úteis, cujo termo inicial corresponderá ao momento em que o proponente for declarado o vencedor do certame, prorrogáveis por igual período, a critério da Administração Pública, para a regularização da documentação, pagamento ou parcelamento do débito, e emissão de eventuais certidões negativas ou positivas com efeito de certidão negativa.

5.2 A não-regularização da documentação no prazo previsto no subitem 4.1.1., implicará decadência do direito à contratação, sem prejuízo das sanções previstas no artigo 81 da Lei nº 8.666/93, sendo facultado à Administração convocar para nova sessão pública os licitantes remanescentes, na ordem de classificação, para contratação, ou revogar a licitação.

5.3 Será assegurado, como critério de desempate, preferência de contratação para as microempresas e empresas de pequeno porte, entendendo-se por empate aquelas situações em que as propostas apresentadas pelas microempresas e empresas de pequeno porte sejam iguais ou até 10% (dez por cento) superiores à proposta mais bem

classificada e desde que a melhor oferta inicial não seja de uma microempresa e empresa de pequeno porte.

**5.4** Ocorrendo o empate, proceder-se-á da seguinte forma:

- 5.4.1** A microempresa e empresa de pequeno porte mais bem classificada poderá apresentar proposta de preço inferior àquela considerada vencedora do certame, situação em que será adjudicado em seu favor o objeto licitado;
- 5.4.2** Não ocorrendo a contratação da microempresa e empresa de pequeno porte, na forma do subitem 4.4.1., serão convocados as remanescentes que porventura se enquadrem na hipótese do subitem 4.3., na ordem classificatória, para o exercício do mesmo direito;
- 5.4.3** No caso de equivalência dos valores apresentados pelas microempresas e empresas de pequeno porte que se encontre no intervalo estabelecido no subitem 4.3., será realizado sorteio entre elas para que se identifique aquela que o primeiro poderá apresentar a melhor oferta;
- 5.4.4** Na hipótese da não-contratação nos termos previstos acima, o objeto licitado será adjudicado em favor da proposta originalmente vencedora do certame, em sessão pública, após verificação da documentação de habilitação;
- 5.4.5** A microempresa e empresa de pequeno porte que usufruir dos benefícios de que trata a LC 123/2006 deverá apresentar, na forma da lei, juntamente com os documentos de habilitação e certidão da Junta Comercial.

## **6. DA FORMA DE APRESENTAÇÃO DAS PROPOSTAS E DOS DOCUMENTOS DE HABILITAÇÃO.**

**6.1** A **PROPOSTA DE PREÇOS** e os **DOCUMENTOS PARA HABILITAÇÃO** deverão ser apresentados no dia, hora e local designados para a realização do Pregão, quando assim solicitados pelo Pregoeiro, aconicionados em envelopes separados e lacrados, identificados com os seguintes elementos:

<b>ENVELOPE Nº 01 – PROPOSTA DE PREÇOS</b>	<b>ENVELOPE Nº 02 – DOCUMENTOS PARA HABILITAÇÃO</b>
<b>Câmara Municipal de Anchieta/ES</b> <b>PREGÃO PRESENCIAL Nº 03/2011</b> Data e hora da abertura. Razão Social e CNPJ. Endereço completo do licitante.	<b>Câmara Municipal de Anchieta/ES</b> <b>PREGÃO PRESENCIAL Nº 03/2011</b> Data e hora da abertura. Razão Social e CNPJ. Endereço completo do licitante.

## **7. DAS PROPOSTAS DE PREÇOS**

**7.1** A proposta de preços será apresentada com assinatura do proponente e sem rasuras, emendas ou entrelinhas e, ainda, com as seguintes informações:

- a) fazer menção ao número deste **Pregão** e conter a razão social da licitante, o CNPJ, número(s) de telefone(s) e de fax e, se houver, *e-mail*, e o respectivo endereço com CEP, e, de preferência, com a indicação do banco, a agência e respectivos códigos e o número da conta corrente.
- b) **Marca e descrição completa do objeto ofertado.**
- c) **Preço(s) unitário(s) e total(is) proposto(s) para o(s) objeto(s) ofertado(s)**, expressos em reais, junto aos quais considerar-se-ão inclusas todas e quaisquer despesas incidentes sobre o objeto licitado (tributos, seguros, fretes, encargos de qualquer natureza etc.);
- d) **Prazo de entrega não superior a 20 (vinte) dias corridos**, contados do recebimento da **Nota de Empenho**. Caso tal prazo seja omitido, o Pregoeiro o entenderá como sendo igual ao máximo permitido. Caso seja indicado prazo de entrega superior ao máximo permitido, o Pregoeiro efetuará diligências para esclarecimentos/correções, e, se for o caso, desclassificará a proposta.
- e) **Prazo de validade da proposta não inferior a 60 (sessenta) dias corridos**. As propostas que omitirem prazo de validade serão entendidas como válidas pelo período de 60 (sessenta) dias corridos. Caso seja indicado prazo de validade da proposta inferior ao mínimo permitido, o Pregoeiro efetuará diligências para esclarecimentos/correções, e, se for o caso, desclassificará a proposta.
- f) **TODOS OS VALORES NÃO PODERÃO ESTAR ACIMA DOS VALORES CONSTANTES NO ANEXO II DESTA EDITAL. Caso o licitante cote qualquer valor acima daqueles limites sua proposta será automaticamente desclassificada.**

7.2 A licitante não está obrigada a cotar em ambos os Lotes.

7.3 No valor final proposto serão consideradas as seguintes regras:

- a) quanto à fração relativa aos centavos, apenas os numerais correspondentes às duas primeiras casas decimais que se seguirem à vírgula, sem qualquer tipo de arredondamento;
- b) discrepância entre os valores expressos em numerais e por extenso, valem estes últimos;
- c) discrepância entre o valor unitário e o global, vale apenas o primeiro.

7.4 Serão corrigidos automaticamente pelo Pregoeiro quaisquer erros de:

- a) soma e/ou multiplicação;
- b) falta de data e/ou rubrica da proposta poderá ser suprida pelo representante legal presente à reunião de abertura dos envelopes de "propostas de preços" com poderes para esse fim; e
- c) a falta do CNPJ e/ou endereço completo poderá também ser preenchida pelos dados constantes dos documentos apresentados dentro do envelope de "documentos para habilitação".

## 8. DO JULGAMENTO

8.1 No julgamento das propostas considerar-se-á vencedora aquela que, obedecendo as condições e especificações estabelecidas neste Edital, apresentar o **"MENOR PREÇO POR LOTE"**.

8.2 No caso de se verificar empate entre duas ou mais propostas e estando superada a fase de oferta de lances verbais, a classificação será obtida mediante sorteio realizado no próprio ato, vedado qualquer outro tipo de procedimento.

## **9. DA HABILITAÇÃO**

### **9.1 HABILITAÇÃO JURÍDICA**

- 9.1.1 Ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado, em se tratando de sociedades comerciais, e, no caso de sociedades por ações, acompanhado de documentos de eleição de seus administradores;
- 9.1.2 Registro comercial, no caso de empresa individual;
- 9.1.3 Cédula de Identidade dos sócios;
- 9.1.4 Documentos de eleição dos atuais administradores, tratando-se de sociedades por ações;
- 9.1.5 Declaração de empregado menor, conforme descrito no Anexo II.

## **10 REGULARIDADE FISCAL**

- 10.1 Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas do Ministério da Fazenda (CNPJ);
- 10.2 Certificado de regularidade de situação com o Fundo de Garantia por Tempo de Serviço (FGTS), emitido pela Caixa Econômica Federal, ou documento equivalente que comprove a regularidade, com validade na data da realização da Licitação;
- 10.3 Certidão de regularidade de débito com o Sistema de Seguridade Social (CND), com validade na data da realização da Licitação;
- 10.4 Prova de inscrição no Cadastro de Contribuinte Estadual ou Municipal relativo à localidade da Licitante, pertinente ao seu ramo de atividade e compatível com o objeto do certame, com validade na data da realização da Licitação;
- 10.5 Certidão conjunta negativa de débitos relativos a tributos federais e à dívida ativa da União expedida pela Secretaria da Receita Federal, com validade na data da realização da Licitação;
- 10.6 Certidão de regularidade de débito com a Fazenda Estadual e Municipal da localidade da Licitante, pertinente ao seu ramo de atividade e relativa aos tributos relacionados com o objeto ou outra prova equivalente na forma da lei;
- 10.7 Prova de regularidade com a Procuradoria Geral da Fazenda Nacional da sede da empresa com validade na data da realização da licitação;
- 10.8 Serão aceitas certidões positivas com efeito de negativa e certidões positivas que noticiem que os débitos certificados estão garantidos ou com sua exigibilidade suspensa.

## **11 QUALIFICAÇÃO ECONÔMICO-FINANCEIRA**

- 11.1 Declaração formal do licitante da sua disponibilidade para cumprimento do objeto da licitação, mediante a apresentação de relação explícita dos equipamentos e pessoal técnico responsável, conforme previsão contida no parágrafo 6º, do artigo 30 da Lei nº 8.666/93;
- 11.2 Todos os documentos exigidos para habilitação deverão ser específicos da matriz ou filial da empresa licitante. Não serão aceitos documentos emitidos pela matriz a parte pela filial.

## **12 QUALIFICAÇÃO TÉCNICA**

- 12.1 Atestado de bom desempenho anterior em fornecimento da mesma natureza e porte, fornecido pela contratante. Este atestado deverá conter a especificação do tipo de compra ou serviço, com indicações das quantidades fornecidas, prazos de execução, outros dados característicos dos fornecimentos prestados e avaliação;
- 12.2 Alvará de localização e funcionamento, expedido pela Prefeitura Municipal da Jurisdição Fiscal do estabelecimento licitante da pessoa jurídica;
- 12.3 Declaração de que a licitante visitou a sede da Câmara e tem pleno conhecimento dos serviços a serem executados e que se sujeita a todas as condições estabelecidas, assinada por representante(s) legal (is) da empresa.

## **10. DA SESSÃO DO PREGÃO**

**10.1** A sessão de recebimento e abertura dos envelopes contendo as propostas de preços e os documentos para habilitação será realizada no local, data e horário indicados no preâmbulo deste Edital, sendo recomendável a presença dos participantes com 10 (dez) minutos de antecedência em relação ao horário previsto para a sua abertura, especialmente quando necessária a autenticação de documentos, e desenvolver-se-á da seguinte forma:

**10.1.1** Declarada aberta a sessão, serão convidados os representantes das empresas que se fizerem presentes para apresentarem junto à mesa os documentos necessários ao credenciamento e/ou representação, na forma do item 4 do edital, os quais poderão ser vistos e conferidos por todos os participantes e, necessariamente, rubricados.

**10.1.2** Em seguida serão anunciadas as empresas legalmente representadas, devendo tais empresas efetuar a entrega dos envelopes com as propostas de preços e de documentos para habilitação, apresentados na forma do item 5.

**10.1.3** Abertura dos envelopes contendo as propostas de preços, escolha daquela que apresentar o **MENOR PREÇO POR LOTE**, classificação daquelas cuja variação situar-se no limite de até 10% (dez por cento) acima do menor preço total do lote ou, em não havendo pelo menos 3 (três) propostas naquelas condições, escolha de tantas quantas forem necessárias, na ordem crescente do preço ofertado, para alcançar o número mínimo de 3 (três) participantes, exceto se igual ou maior número de licitantes não estiver participando do certame (incisos VI e VII do artigo 11 do Decreto n. 3.555/00).

**10.1.4** Análise de todas as propostas quanto à sua conformidade com as exigências do Edital, procedendo-se a desclassificação daquelas desconformes e a sua substituição por outra, de forma a definir aquelas que se encontrarem aptas para a fase de lances verbais.

**10.1.4.1 Na análise das propostas, o Pregoeiro poderá utilizar-se da ajuda de representantes da Diretoria do Serviço de Informática, determinando, inclusive, a suspensão temporária da reunião, para analisar mais detalhadamente o conteúdo das propostas.**

**10.1.5** Início da fase dos lances verbais, os quais serão formulados pelos proponentes de forma sucessiva, em valores numéricos distintos e decrescentes, a partir do autor da proposta de maior preço, observando o seguinte:

**10.1.5.1 As rodadas de lances verbais serão repetidas quantas vezes forem necessárias, tendo como tempo máximo o período de 10 (dez) minutos para a conclusão dos lances verbais de cada Lote. A critério do Pregoeiro, o referido período poderá ser prorrogado.**

**10.1.5.2** A cada nova rodada será efetivada a classificação momentânea das propostas, de forma a definir a seqüência dos lances ulteriores.

**10.1.5.3** O lance inicial ofertado deverá sempre cobrir o valor da proposta de menor preço, e a partir de então o lance de menor valor da rodada em andamento ou precedente, conforme o caso.

**10.1.5.4** A desistência em apresentar lance verbal, quando para esse fim convocado, implicará na exclusão do licitante quanto à fase de lances verbais, mantendo-se, todavia, o último preço por ele apresentado para efeito da classificação final das propostas.

**10.1.5.5** A desistência dos lances ofertados sujeita o seu proponente às penalidades cabíveis.

**10.1.6** Encerrada a etapa de oferta de lances, as propostas serão ordenadas exclusivamente pelo critério de menor preço, sendo objeto de exame e decisão motivada quanto à aceitabilidade do valor apresentado por aquela classificada em primeiro lugar.

**10.1.7** Sendo aceitável a oferta da proposta classificada em primeiro lugar, em relação ao seu proponente será verificado o atendimento das condições habilitatórias, mediante abertura do respectivo envelope de documentação e consulta ao SICAF, na forma do item 8 deste Edital, sendo-lhe assegurado o direito de apresentar no próprio ato a documentação porventura necessária à atualização e regularização de sua situação.

**10.1.8** Constatado o atendimento pleno às exigências editalícias, o proponente será declarado vencedor, sendo-lhe adjudicado o respectivo item do Pregão.

**10.1.9** Se a oferta não for aceitável ou se o proponente não atender às exigências habilitatórias, serão examinadas as ofertas subseqüentes, inclusive quanto a sua aceitabilidade, por ordem de classificação, até a apuração de uma que atenda a todas as exigências editalícias, sendo o respectivo proponente declarado vencedor e a ele adjudicado o correspondente objeto.

**10.1.10** Caso ocorram as hipóteses dos subitens 9.1.7 e 9.1.8, ou de não haver oferta de lances verbais, ou mesmo quando houver ofertas de lances verbais, após a decisão do pregoeiro, em qualquer dos casos, quanto à aceitabilidade da proposta ainda será lícito ao pregoeiro negociar diretamente com o proponente para a obtenção de preço melhor do que aquele ofertado.

**10.1.11** Da reunião lavrar-se-á ata circunstanciada, ao final assinada pelo Pregoeiro e licitantes presentes, facultada a assinatura dos membros da equipe de apoio e ouvintes, na qual serão registrados todos os fatos relevantes da sessão, inclusive quanto ao previsto no item 11.1.

**10.1.11.1.** A adjudicação do objeto obedecerá a estrita ordem de classificação e será praticada pelo pregoeiro na própria ata de reunião.

## **11. DA IMPUGNAÇÃO DO EDITAL**

**11.1** Decairá do direito de impugnar os termos deste Edital aquele que não o fizer até 2 (dois) dias úteis antes da data designada para a realização do Pregão, apontando de forma clara e objetiva as falhas e/ou irregularidades que entende viciarem o mesmo.

**11.1.1** Caberá ao Pregoeiro decidir, no prazo de 24 (vinte e quatro) horas, sobre a impugnação interposta.

**11.1.2** Se procedente e acolhida a impugnação do edital, seus vícios serão sanados e nova data será designada para a realização do certame.

## **12. DOS RECURSOS**

**12.1** A manifestação da intenção de interpor recurso, pleiteada pela licitante, deverá ser feita ao final da sessão, com registro em ata da síntese das suas razões de recorrer, momento a partir do qual será concedido ao interessado o prazo de **3 (três) dias** para a apresentação das razões do recurso, ficando as demais licitantes, desde logo, intimadas para apresentar as contra-razões, em igual número de dias, que começarão a correr do término do prazo do recorrente, sendo-lhes assegurada vista imediata dos autos.

**12.1.1** A falta de manifestação imediata e motivada da intenção de interpor recurso, no momento da sessão deste **Pregão**, implicará **decadência e preclusão** desse direito da **licitante**, devendo o Pregoeiro adjudicar o objeto à **vencedora**.

**12.2** Na hipótese da interposição de recurso, os autos do processo permanecerão com vista franqueada aos interessados, na Câmara Municipal de Anchieta/ES, no local indicado para a realização do certame, em dias úteis, no horário das 13:00 às 18:00 horas.

**12.3** Os **recursos** deverão ser protocolizados na Secretaria da Câmara Municipal de Anchieta e direcionados ao Pregoeiro Oficial, e observarão:

- a) quanto à sua interposição, o prazo de 3 (três) dias, a contar da manifestação de sua intenção de recorrer, registrada em ata;
- b) a forma escrita, com a assinatura do licitante ou seu representante legal;
- c) a legitimidade e o interesse recursais;
- d) a fundamentação.

## **13. DO RECEBIMENTO**

**13.1** Os bens e/ou serviços serão **recebidos provisoriamente** para posterior verificação da conformidade com o exigido no Edital.

**13.2** O **recebimento definitivo, de responsabilidade da Diretoria do Serviço de Informática, dar-se-á no prazo máximo de 5 (cinco) dias úteis**, contados do recebimento provisório.

**13.3.** Verificando-se defeitos nos bens, a empresa será notificada para saná-los ou efetuar a troca devida, no prazo máximo de 5 (cinco) dias úteis, ficando nesse período interrompido a contagem do prazo para recebimento definitivo.

**13.4** O recebimento provisório ou definitivo não exclui as responsabilidades civil e penal da licitante.

## **14. DAS PENALIDADES**

**14.1** Pela inexecução total ou parcial do contrato, a Administração poderá, garantida a prévia defesa, aplicar à contratada, segundo a extensão da falta cometida, as seguintes penalidades, previstas no artigo 87 da Lei n. 8.666/93, na Lei n. 10.520/02 e Decreto n. 3.555/00, além das seguintes penalidades:

**14.1.1** Advertência, nas hipóteses de execução irregular do contrato, que não resulte prejuízo para o serviço desta Câmara Municipal;

**14.1.2** Multa, prevista na forma do item 14.2, nas hipóteses de inexecução do contrato, com ou sem prejuízo para o serviço;

**14.1.3** Suspensão temporária do direito de licitar e de contratar com este Órgão, por período de até 5 (cinco) anos, nas hipóteses e nos termos da Lei n. 10.520/02 e artigo 14 do Decreto n. 3.555/00;

**14.1.4** Declaração de inidoneidade para licitar ou contratar com a Administração Pública, pelo prazo de até 5 (cinco) anos, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a autoridade que aplicar a penalidade, nos termos do art. 87, inciso IV, da Lei n. 8.666/93.

**14.1.4.1** A aplicação da sanção de Declaração de Inidoneidade implica na inativação do cadastro do fornecedor ou interessado junto ao SICAF, impossibilitando-o de relacionar-se comercialmente com a Administração Federal, no âmbito do SISG e dos demais Órgãos/entidades que o utilizam, conforme estabelece o item 6.4 da IN MARE n. 05/95.

**14.2** Caso a licitante declarada vencedora se recuse a receber/retirar a **Nota de Empenho**, será aplicada-lhe a multa de 10% (dez por cento) sobre o valor total adjudicado, exceto se a causa for decorrente de caso fortuito ou motivo de força maior, devidamente comprovada e acatada pela Administração.

**14.3** Expirado o prazo proposto para a entrega dos produtos, sem que a contratada o cumpra, iniciar-se-á a aplicação da penalidade de multa, correspondente a 1 % (um por cento) por dia de atraso, incidente sobre o valor total da Nota de Empenho.

**14.3.1** A multa prevista neste item será aplicada até o limite de 10 % (dez por cento), o que não impede, a critério da administração do TRT, a aplicação das demais sanções a que se refere o item 13.1.

**14.4** A multa referida no item 13.2 será cobrada administrativamente, enquanto que aquelas referidas nos itens 13.3 e 13.3.1 serão cobradas por compensação financeira dos créditos que a contratada tiver a receber e não impedem, em razão da extensão da falta cometida, a aplicação das demais sanções previstas no item 13.1 e seus subitens.

**14.5** Contra os atos de aplicação das penalidades previstas neste título também cabem recursos, a serem interpostos no prazo de 5 (cinco) dias úteis, contados da intimação do ato, observando, no que couber, as regras do item 11.3 do presente Edital.

## **15. DO PAGAMENTO**

**15.1** - O(s) pagamento(s) será(ão) efetuado(s) até vinte (20) dias após a entrega do objeto mediante a apresentação à Câmara Municipal, de documento(s) fiscal(is) hábil(eis), sem emendas ou rasuras, observada a periodicidade mensal.

**15.2** - Ocorrendo erros na apresentação do(s) documento(s) fiscal(is), o(s) mesmo(s) será(ão) devolvido(s) à contratada para correção, ficando estabelecido que o prazo para pagamento será contado a partir da data de apresentação da nova fatura, devidamente corrigida.

**15.3** - A Câmara Municipal poderá deduzir do pagamento importâncias que a qualquer título lhe forem devidos pela contratada, em decorrência de inadimplemento contratual.

**15.4** - O pagamento da fatura somente será feito em carteira ou cobrança simples, sendo expressamente vedada à contratada a cobrança ou desconto de duplicatas através da rede bancária ou de terceiros.

## **16. DISPOSIÇÕES FINAIS**

**16.1** Ao Pregoeiro ou à Autoridade Superior é facultado, em qualquer fase da licitação, a promoção de diligências destinadas a esclarecer ou complementar a instrução do processo, vedada a inclusão posterior de documento ou informação que deveria constar no ato da sessão pública.

**16.2** A simples participação na licitação implicará no conhecimento e aceitação tácita das condições estabelecidas neste Edital.

**16.3** A contratada fica obrigada a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, observados os termos dos parágrafos 1º e 2º do artigo 65 da Lei n. 8.666/93.

**16.4** As normas que disciplinam este pregão serão sempre interpretadas em favor da ampliação da disputa entre os interessados, sem comprometimento da segurança do futuro contrato.

**16.5** Aos casos omissos aplicar-se-ão as demais disposições constantes na legislação pertinente.

**16.6** Não serão levadas em consideração as propostas que fizerem referência às de outras licitantes ou que apresentem qualquer oferta de vantagem não prevista, tal como proposta alternativa.

**16.7** Serão desclassificadas as propostas elaboradas em desacordo com os termos deste Edital.

**16.8** Os eventuais pedidos de substituição do objeto inicialmente proposto observarão, como condição de possível deferimento, a fundamentação da solicitação e a plena satisfação do interesse público, caracterizada mediante comprovação da similaridade e da correspondência de preço e qualidade entre o material/equipamento cotado e aquele ofertado em substituição.

**16.9** Quaisquer esclarecimentos necessários ao perfeito conhecimento do objeto da presente licitação poderão ser obtidos junto à Câmara Municipal de Anchieta/ES, com o Pregoeiro Oficial ou sua equipe de apoio.

**Antônio Valente Ferreira Neto**  
**Pregoeiro Oficial**

## **ANEXO I – TERMO DE REFERÊNCIA**

**OBJETO: AQUISIÇÃO DOS PRODUTOS ABAIXO ESPECIFICADOS.**

### **OBJETO: Aquisição dos seguintes equipamentos de informática:**

Lote 01-

Item 1	Aquisição e implantação de software de Gerenciamento de Backup
Item 2	Aquisição e implantação de nova Solução de Segurança (Antivírus)
Item 3	Implantação de soluções baseadas no MS Windows Server 2008

Lote 02-

Item 1	Aquisição de um servidor para rack.
--------	-------------------------------------

#### **Item 01 - Aquisição e implementação de software de Gerenciamento de Backup**

Fornecimento de licença de software de backup para os dados da Câmara Municipal de Anchieta, contendo os seguintes módulos e funcionalidades.

- Compatibilidade do software de backup com plataformas Windows Server 2000, 2003 ou 2008; de 32 e 64-bits.
- Disponibilização de 1 (uma) interface gráfica com o usuário, contendo um "Backup Assistant" que ofereça acesso rápido às informações de suporte técnico, manuais on-line e assistentes que orientam os usuários nas tarefas mais comuns, simplificando a configuração, rotação de mídias, compartilhamento de dispositivos e recuperação de desastres;
- O servidor de gerência de backup deverá ser instalado em ambiente Windows 2003/2008;
- Possuir a função de backups completos (FULL), incrementais e diferenciais de servidores;
- Permitir transferência de dados através de uma rede dedicada, para operações de backup e restore via WAN.
- Oferecer monitoramento e administração remotos de servidores individuais a partir de qualquer servidor ou estação de trabalho Windows (para operações de backup altamente distribuídas).
- Oferecer relatórios de todos os servidores de backup remotos através de uma única interface.
- O software deve ter a capacidade de realizar "Verify" e "Database Consistency Check", no intuito de garantir a integridade dos dados através de uma verificação de alta velocidade;
- Possuir modulo de gerenciamento de ambiente de backup ( Dashboard ) com suporte a visualização de todas as rotinas de backup, com opções de gerar relatórios online e enviar os mesmo por e-mail.

- Possuir modulo de instalação de agentes e atualizações, sem ter a necessidade de deslocar uma pessoa para fazer a instalação destes dispositivos.
- Possuir modulo de Multi-Streaming.
- Deve ter a capacidade de executar filtragem, de histórico e de alertas, além de configuração aperfeiçoada de notificação, quando da especificação de recipientes;
- Deverá permitir, em nível de software, o envio automático de alertas, quando da falha de um procedimento de backup ou restore, através de mensagem de correio eletrônico (SMTP ou MAPI) ;
- Possuir integração com "Automated Server Recovery (ASR)" da Microsoft e o uso da API "ASR", visando aumentar a eficiência e agilidade nas operações de recuperação de desastres em servidores Windows 2003 ou Windows XP, mesmo com hardware diferente.
- Possui suporte a "Volume Shadow Copy" para proteção do Microsoft Virtual Server 2005.
- Possuir recursos de "Job Test Run" para verificar a capacidade das fitas, outros critérios para identificar problemas potenciais que possam impedir uma conclusão bem sucedida do job e notificar o administrador através de correio eletrônico, pager, telefone ou pelo console de administração.
- Possuir modulo de Multiplexing, com opção de até 32 jobs simultâneos.
- Possuir recursos para monitorar a mídia remota por localização de cofre, atribuir prioridade de um job sobre outro e estabelecer proativamente normas de administração de erros para automatizar o processo.
- Compatibilidade com recursos de Cluster, visando a tolerância a falhas do sistema e protegendo máquinas que disponham de mecanismo de alta disponibilidade que utilizem o Microsoft Cluster Server (MSCS), para efetuar o failover automático de servidor de backup em disponibilizações de cluster ativas/passivas.
- Suportar dispositivos de armazenamento do tipo "Write once, read many" (WORM)
- Ter a capacidade de expandir para sistemas de fitotecas multidrive, permitindo que drives adicionais em uma fitoteca sejam acessados, garantindo uma expansão da capacidade de armazenamento;
- Possuir licença de acesso para agentes remotos para servidores Windows, Netware, MacOS X, Linux e UNIX.
- Possuir licença de acesso para agentes online Microsoft Exchange Server (2003 e 2007), Microsoft SharePoint Portal Server (versões 2003 e 2007), Lotus Domino Server (7.x e 8), Microsoft SQL Server (2000, 2005 e 2008), para servidores Windows.
- Possuir licença de acesso para agentes online Microsoft Data Protection Manager
- Suporte de backup e restore em ambiente AS400.
- Deverá disponibilizar recursos que implementem a cópia direta de dados entre fitas magnéticas
- Deverá disponibilizar recursos que implementem a execução de backup de arquivos abertos, mesmo que estejam sendo alterados durante a operação de backup, sem necessidade de suspender a utilização das aplicações pelos usuários nem a conexão da rede. A cópia do arquivo salvo deverá ser idêntica ao arquivo residente em disco, quando do início da operação de backup;
- Permitir através do agente on-line para MS-Exchange Server, a ação de restore de caixas postais individuais e de mensagens específicas de uma caixa postal, sem a necessidade de restore de toda a Base de Dados.
- Deve ter uma console de administração central, de múltiplos servidores de backup, com a opção de centralização, distribuição e replicação dos catálogos e permitir a instalação automática do produto, suas opções e modelos de job para servidores remotos;
- Deve ter a capacidade de efetuar backups para disco com retenções, através de políticas pré-definidas e agendadas.
- Possuir aplicativo para download e instalação de updates, upgrades e novas versões do produto, de forma manual, agendada ou sem intervenção do administrador.
- Possibilidade de listar no log, todas as mídias utilizadas nas rotinas de backup, através da tela de Histórico dos Jobs.

- Possibilidade de restaurar apenas as permissões de segurança de diretórios em volumes NTFS.
- Possuir módulo de controle de acesso e auditoria dos usuários que acessa a solução de backup.
- Possuir módulo de gerenciamento de criptografia de em todos os processos de backup.
- Possuir suporte aos protocolos de rede IPv4 e IPv6 para rotinas de backup e restore.
- Possuir módulo nativo de criptografia AES 128-bits, 256-bits
- Possuir suporte nativo de criptografia para unidades de fita LTO-4.
- Permitir através do agente online backup e restore do MS Active Directory com opções de restauração de toda a arquitetura do MS Active Directory. O restore dos objetos não deve exigir um reboot no servidor Domain Controller.
- Solução integrado com Vmware consolidate Backup (VCB), permitindo que em uma única tarefa de backup full, incremental ou diferencial seja possível restaurar de forma granular os arquivos pertencentes a uma máquina virtual e também restaurar a máquina virtual (VMDK), sem necessidade de scripts e sem necessidade de voltar o restore da máquina por completo, no caso de restore granular. As tarefas de backup/recovery deverão ser realizadas via interface gráfica.
- Solução integrado com Microsoft Hyper-V permitindo que em uma única tarefa de backup full, incremental ou diferencial seja possível restaurar de forma granular os arquivos pertencentes a uma máquina virtual e também restaurar a máquina virtual (VHD), sem necessidade de scripts. As tarefas de backup/recovery deverão ser realizadas via interface gráfica.
- Possuir módulo de deduplicação através do Software de backup garantindo a redundância e eliminando duplicidade dados em ambiente virtual (VMware e Hyper-V).
- Possuir módulo de backup de storages conectados à rede (NAS) através do protocolo NDMP.
- Possibilidade de geração de relatórios customizados, utilizando as seguintes categorias : alertas, configurações, jobs, mídia, dispositivos, e política.
- Possuir tecnologia de deduplicação de backup em desktops e laptops e servidores através de agente de sistema operacional, sem a necessidade de uma solução complementar.
- Possuir recursos avançados de agendamento de rotinas de backup e restore, para datas específicas, dias da semana recorrentes, dias do mês recorrentes, intervalo de dias e intervalo de reinício.
- Possuir recurso que permita a escolha de uma interface de rede secundária de backup, criando assim uma "Backup Area Network" (BAN).
- Possuir compatibilidade com "Storage Area Networks" (SAN), em ambientes Windows e permitindo backups e restores de alta velocidade e o compartilhamento de dispositivos de armazenamento entre múltiplos servidores de backup.
- Suporte a tecnologia de Serverless Backup.
- Possibilidade de gerar relatórios customizados de volume de backup realizados por período, por localidade, custo por GB (bilhetagem), tendência de crescimento, qual a porcentagem de backups realizados de máquinas físicas e virtuais, identificarem uso dos tape drives;
- Suporte para proteção de no mínimo 100 servidores clientes utilizando um único servidor de backup/recovery;
- Deverá possuir sistema de gerenciamento automático de verificação e instalação de atualizações e novas versões (Live Update);
- Apresentar 01 (um) atestado fornecido por empresa pública ou privada comprovando que o licitante forneceu soluções semelhantes ao objeto deste edital (inclusive em quantitativos e serviços/treinamento) com no mínimo mesmo porte de ambiente computacional da CMA.
- Deverá ser realizado um treinamento, para capacitação de 01 (um) colaborador da equipe técnica da Câmara Municipal de Anchieta.
- O treinamento deverá ser realizado nas dependências da CMA ou outro local providenciado por esta.

- A contratada deverá fornecer ao término do projeto a documentação da solução implementada.
- O software deverá ser fornecido com a quantidade e módulos relacionados abaixo:

ITEM	QTDE	DESCRIÇÃO
01	01	Modulo de Gerenciamento (Tipo CA Storage Media Kit)
02	01	Modulo para servidor de arquivos (Tipo CA ARCserve Backup r15 for Windows Essentials File Server Module)
03	04	Modulo para backup de máquinas virtuais VMware (Tipo CA ARCserve Backup r15 for Windows Guest Based Virtual Machine Agent Bundle)

- Suporte/garantia: os produtos adquiridos deverão contemplar suporte/assistência 24 horas por dia, 7 dias por semana (24 x 7) "telefônico" - disponibilização de central 0800 - via Internet/Web, por um período de garantia de até 36 (trinta e seis) meses.

#### Item 02 – Solução de segurança (Antivírus)

Fornecimento de **SOLUÇÃO DE SEGURANÇA** por um período de 36 meses, para o ambiente de tecnologia da informação da Câmara Municipal de Anchieta, juntamente com os serviços de instalação e configuração e treinamento dos softwares que irão compor a solução, composto pelos seguintes subsistemas de segurança: ANTIVÍRUS/ANTISPYWARE, PERSONAL FIREWALL, PROTEÇÃO CONTRA INTRUSOS E CONTROLE DE ACESSO A REDE, de acordo com a descrição abaixo:

##### 1. Servidor de Administração e Console Administrativa

###### 1.1. Compatibilidade:

- 1.1.1. Microsoft Windows Server 2003 ou superior
- 1.1.2. Microsoft Windows Server 2003 x64 ou superior
- 1.1.3. Microsoft Windows Server 2008
- 1.1.4. Microsoft Windows Server 2008 Core
- 1.1.5. Microsoft Windows Server 2008 x64 SP1
- 1.1.6. Microsoft Windows Server 2008 R2
- 1.1.7. Microsoft Windows Server 2008 R2 Core
- 1.1.8. Microsoft Windows XP Professional SP2 ou superior
- 1.1.9. Microsoft Windows XP Professional x64
- 1.1.10. Microsoft Windows Vista SP1
- 1.1.11. Microsoft Windows Vista x64 SP1
- 1.1.12. Microsoft Windows Seven

###### 1.2. Características:

- 1.2.1. A console deve ser acessada via WEB (HTTPS) ou MMC;
- 1.2.2. Capacidade de remover remotamente qualquer solução de anti-virus (própria ou de terceiros) que estiver presente nas estações e servidores;
- 1.2.3. Capacidade de instalar remotamente a solução de anti-virus nas estações e servidores Windows, através de compartilhamento administrativo, login script e/ou GPO de Active Directory;
- 1.2.4. Capacidade de instalar remotamente a solução de segurança em smartphones Symbian, Windows Mobile e BlackBerry, utilizando estações como intermediadoras;
- 1.2.5. Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux) protegidos pela solução anti-virus;

- 1.2.6. Capacidade de gerenciar smartphones (tanto Symbian quanto Windows Mobile e BlackBerry) protegidos pela solução anti-virus;
- 1.2.7. Deve gerenciar todos os módulos das soluções acima em uma única console.
- 1.2.8. Capacidade de gerar pacotes customizados (auto-executáveis) contendo a licença e configurações do produto;
- 1.2.9. Capacidade de atualizar os pacotes de instalação com as últimas vacinas, para que quando o pacote for utilizado em uma instalação já contenha as últimas vacinas lançadas;
- 1.2.10. Capacidade de fazer deployment (distribuição) remota de qualquer software, ou seja, deve ser capaz de remotamente enviar qualquer software pela estrutura de gerenciamento de anti-virus para que seja instalado nas máquinas clientes;
- 1.2.11. Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas;
- 1.2.12. Capacidade de monitorar diferentes subnets de rede a fim de encontrar máquinas novas para serem adicionadas a proteção;
- 1.2.13. Capacidade de monitorar grupos de trabalhos já existentes e quaisquer grupos de trabalho que forem criados na rede, a fim de encontrar máquinas novas para serem adicionadas a proteção;
- 1.2.14. Capacidade de, assim que detectar máquinas novas no Active Directory, subnets ou grupos de trabalho, automaticamente importar a máquina para a estrutura de proteção da console e verificar se possui o antivírus instalado. Caso não possuir, deve instalar o anti-virus automaticamente;
- 1.2.15. Capacidade de agrupamento de máquina por características comuns entre as mesmas, por exemplo: agrupar todas as máquinas que não tenham o antivírus instalado, agrupar todas as máquinas que não receberam atualização nos últimos 2 dias, etc;
- 1.2.16. Capacidade de definir políticas de configurações diferentes por grupos de estações, permitindo que sejam criados subgrupos e com função de herança de políticas entre grupos e subgrupos;
- 1.2.17. Deve fornecer as seguintes informações dos computadores; :
  - 1.2.17.1. Se o anti-virus está instalado;
  - 1.2.17.2. Se o anti-virus está iniciado;
  - 1.2.17.3. Se o anti-virus está atualizado;
  - 1.2.17.4. Minutos/horas desde a última conexão da máquina com o servidor administrativo;
  - 1.2.17.5. Minutos/horas desde a última atualização de vacinas
  - 1.2.17.6. Data e horário da última verificação executada na máquina;
  - 1.2.17.7. Versão do anti-virus instalado na máquina;
  - 1.2.17.8. Se é necessário reiniciar o computador para aplicar mudanças;
  - 1.2.17.9. Data e horário de quando a máquina foi ligada;
  - 1.2.17.10. Quantidade de vírus encontrados (contador) na máquina;
  - 1.2.17.11. Nome do computador;
  - 1.2.17.12. Domínio ou grupo de trabalho do computador;
  - 1.2.17.13. Data e horário da última atualização de vacinas;
  - 1.2.17.14. Sistema operacional com ServicePack;
  - 1.2.17.15. Quantidade de processadores;
  - 1.2.17.16. Quantidade de memória RAM;

- 1.2.17.17. Usuário(s) logado(s) naquele momento, com informações de contato (caso disponíveis no Active Directory);
- 1.2.17.18. Endereço IP;
- 1.2.18. Deve permitir bloquear as configurações do anti-virus instalado nas estações e servidores de maneira que o usuário não consiga alterá-las;
- 1.2.19. Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como:
  - 1.2.19.1. Mudança de gateway;
  - 1.2.19.2. Mudança de subnet DNS;
  - 1.2.19.3. Mudança de domínio;
  - 1.2.19.4. Mudança de servidor DHCP;
  - 1.2.19.5. Mudança de servidor DNS;
  - 1.2.19.6. Mudança de servidor WINS;
  - 1.2.19.7. Aparecimento de nova subnet;
- 1.2.20. Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet;
- 1.2.21. Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes;
- 1.2.22. Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de anti-virus;
- 1.2.23. Capacidade de herança de tarefas e políticas na estrutura hierarquica de servidores administrativos;
- 1.2.24. Capacidade de eleger qualquer computador cliente como repositório de vacinas e de pacotes de instalação, sem que seja necessária a instalação de um servidor administrativo completo, onde outras máquinas clientes irão atualizar-se e receber pacotes de instalação, a fim de otimizar tráfego da rede;
- 1.2.25. Capacidade de exportar relatórios para os seguintes tipos de arquivos: PDF, HTML e XML.
- 1.2.26. Capacidade de gerar traps SNMP para monitoramento de eventos;
- 1.2.27. Capacidade de enviar mensagens via NETSEND para máquina específicas em caso de algum evento;
- 1.2.28. Capacidade de enviar emails para contas específicas em caso de algum evento;
- 1.2.29. Deve possuir compatibilidade com Microsoft NAP, quando instalado em um Windows 2008 Server;
- 1.2.30. Deve possuir compatibilidade com Cisco Network Admission Control (NAC);
- 1.2.31. Deve possuir documentação da estrutura do banco de dados para geração de relatórios a partir de ferramentas específicas de consulta (Crystal Reports, por exemplo).
- 1.2.32. Capacidade de ligar máquinas via Wake on Lan para realização de tarefas (varredura, atualização, instalação, etc), inclusive de máquinas que estejam em subnets diferentes do servidor;
- 1.2.33. Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado intervalo de tempo);
- 1.2.34. Capacidade de realizar atualização incremental de vacinas nos computadores clientes;

## 2. Estações Windows

## 2.1.Compatibilidade:

- 2.1.1. Microsoft Windows 2000 Professional Service Pack 4 ou superior
- 2.1.2. Microsoft Windows XP Home Edition
- 2.1.3. Microsoft Windows XP Professional SP1 ou superior
- 2.1.4. Microsoft Windows XP Professional x64 Edition
- 2.1.5. Microsoft Windows Vista
- 2.1.6. Microsoft Windows Vista x64
- 2.1.7. Microsoft Windows Seven Professional/Enterprise/Ultimate
- 2.1.8. Microsoft Windows Seven Professional/Enterprise/Ultimate x64

## 2.2.Características:

- 2.2.1. Deve prover as seguintes proteções:
  - 2.2.1.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
  - 2.2.1.2. Antivírus de Web (módulo para verificação de sites e downloads contra vírus)
  - 2.2.1.3. Antivírus de Email (módulo para verificação de emails recebidos e enviados, assim como seus anexos)
  - 2.2.1.4. Anti-Spam (módulo de anti-spam pessoal)
  - 2.2.1.5. Firewall com IDS
  - 2.2.1.6. Auto-proteção (contra ataques aos serviços/processos do antivírus)
  - 2.2.1.7. Controle de dispositivos externos
- 2.2.2. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
- 2.2.3. As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independente do nível das ameaças encontradas no período (alta, média ou baixa).
- 2.2.4. Capacidade de automaticamente desabilitar o Firewall do Windows (caso exista) durante a instalação, para evitar incompatibilidade com o Firewall da solução;
- 2.2.5. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;
- 2.2.6. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: "Win32.Trojan.banker") para que qualquer objeto detectado com o veredicto escolhido seja ignorado;
- 2.2.7. Capacidade de adicionar aplicativos a uma lista de "aplicativos confiáveis", onde as atividades de rede, atividades de disco e acesso ao registro do Windows não serão monitoradas;
- 2.2.8. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);
- 2.2.9. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
- 2.2.10. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomá-la a partir da extensão do arquivo;
- 2.2.11. Capacidade de verificar somente arquivos novos e alterados;
- 2.2.12. Capacidade de verificar objetos usando heurística;

- 2.2.13. Capacidade de agendar uma pausa na verificação;
- 2.2.14. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;
- 2.2.15. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
  - 2.2.15.1. Perguntar o que fazer, ou;
  - 2.2.15.2. Bloquear acesso ao objeto;
    - 2.2.15.2.1. Apagar o objeto ou tentar desinfecção (de acordo com a configuração pré-estabelecida pelo administrador);
    - 2.2.15.2.2. Caso positivo de desinfecção:
      - 2.2.15.2.2.1. Restaurar o objeto para uso;
    - 2.2.15.2.3. Caso negativo de desinfecção:
      - 2.2.15.2.3.1. Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);
- 2.2.16. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto.
- 2.2.17. Capacidade de verificar emails recebidos e enviados nos protocolos POP3, IMAP, NNTP, e SMTP, assim como conexões criptografadas (SSL) para POP3 e IMAP (SSL);
- 2.2.18. Capacidade de verificar tráfego de ICQ e MSN contra vírus e links phishings;
- 2.2.19. Capacidade de verificar links inseridos em emails contra phishings;
- 2.2.20. Capacidade de verificar tráfego SSL nos browsers: Internet Explorer, Firefox e Opera;
- 2.2.21. Capacidade de verificação de corpo e anexos de emails usando heurística;
- 2.2.22. O antivírus de email, ao encontrar um objeto potencialmente perigoso, deve:
  - 2.2.22.1. Perguntar o que fazer, ou;
  - 2.2.22.2. Bloquear o email;
    - 2.2.22.2.1. Apagar o objeto ou tentar desinfecção (de acordo com a configuração pré-estabelecida pelo administrador);
    - 2.2.22.2.2. Caso positivo de desinfecção:
      - 2.2.22.2.2.1. Restaurar o email para o usuário;
    - 2.2.22.2.3. Caso negativo de desinfecção:
      - 2.2.22.2.3.1. Mover para quarentena ou apagar o objeto (de acordo com a configuração pré-estabelecida pelo administrador);
- 2.2.23. Caso o email conter código que parece ser, mas não é definitivamente malicioso, o mesmo deve ser mantido em quarentena.
- 2.2.24. Possibilidade de verificar somente emails recebidos ou recebidos e enviados.
- 2.2.25. Capacidade de filtrar anexos de email, apagando-os ou renomeando-os de acordo com a configuração feita pelo administrador, com a possibilidade de restauração de um anexo deletado;
- 2.2.26. Capacidade de verificação de tráfego HTTP e qualquer script do Windows Script Host (JavaScript, Visual Basic Script, etc), usando heurísticas;
- 2.2.27. Deve ter suporte total ao protocolo IPv6;
- 2.2.28. Capacidade de alterar as portas monitoradas pelos módulos de Web e Email;
- 2.2.29. Na verificação de tráfego web, caso encontrado código malicioso o programa deve:
  - 2.2.29.1. Perguntar o que fazer, ou;
  - 2.2.29.2. Bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio, ou;
  - 2.2.29.3. Permitir acesso ao objeto;

- 2.2.30. O antivírus de web deve realizar a verificação de, no mínimo, duas maneiras diferentes, sob escolha do administrador:
  - 2.2.30.1. Verificação *on-the-fly*, onde os dados são verificados enquanto são recebidos em tempo-real, ou;
  - 2.2.30.2. Verificação de *buffer*, onde os dados são recebidos e armazenados para posterior verificação. O administrador deve ter a capacidade de escolher quanto tempo de *buffer* o programa irá realizar.
- 2.2.31. Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus de web.
- 2.2.32. Deve possuir módulo que analise as ações de cada aplicação em execução no computador, gravando as ações executadas e comparando-as com seqüências características de atividades perigosas. Tais registros de seqüências devem ser atualizados juntamente com as vacinas.
- 2.2.33. Deve possuir módulo que analise cada macro de VBA executada, procurando por sinais de atividade maliciosa.
- 2.2.34. Deve possuir módulo que analise qualquer tentativa de edição, exclusão ou gravação do registro, de forma que seja possível escolher chaves específicas para serem monitoradas e/ou bloqueadas.
- 2.2.35. Deve possuir módulo de bloqueio de *Phishing*, com atualizações incluídas nas vacinas, obtidas pelo *Anti-Phishing Working Group* (<http://www.antiphishing.org/>).
- 2.2.36. Deve possuir módulo de bloqueio de *Banners* e *Popups* de propagandas não-solicitadas, com opção de lista de exclusão;
- 2.2.37. Deve possuir módulo de proteção de atividades do modem, possibilitando a criação de uma lista de números que podem ser discados;
- 2.2.38. Capacidade de distinguir diferentes sub-nets e conceder opção de ativar ou não o firewall para uma sub-net específica;
- 2.2.39. Deve possuir módulo IDS (*Intrusion Detection System*) para proteção contra *port scans* e exploração de vulnerabilidades de softwares. A base de dados de análise deve ser atualizada juntamente com as vacinas.
- 2.2.40. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:
  - 2.2.40.1. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;
  - 2.2.40.2. Filtragem por aplicação: onde o administrador poderá escolher qual aplicação terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.
- 2.2.41. Deve possuir módulo de anti-spam, que utilize tecnologias PDB (análise de cabeçalho), GSG (análise de elementos gráficos), tecnologia baseada no teorema de Bayes ([http://pt.wikipedia.org/wiki/Filtro\\_bayesiano](http://pt.wikipedia.org/wiki/Filtro_bayesiano)) além de *White* e *Black Lists* e algoritmo de reconhecimento de frases comuns de spams.
- 2.2.42. Deve possuir módulo que habilite ou não o funcionamento dos seguintes dispositivos externos, no mínimo:
  - 2.2.42.1. Dispositivos de comunicação USB (modems, telefones, etc.)
  - 2.2.42.2. Impressoras USB
  - 2.2.42.3. Dispositivos de armazenamento USB
  - 2.2.42.4. Drives de CD/DVD-ROM
  - 2.2.42.5. Drives de disquete
  - 2.2.42.6. Dispositivos IEEE 1394 (Firewire)
  - 2.2.42.7. Modems

- 2.2.42.8. Dispositivos PCMCIA
- 2.2.42.9. Dispositivos COM e LPT
- 2.2.42.10. Drives de fita
- 2.2.42.11. Dispositivos 1284 Dot4
- 2.2.42.12. Impressoras 1284 Dot4
- 2.2.42.13. Dispositivos Infra-vermelhos (IRDA)
- 2.2.42.14. Leitores de cartões (SD, MemoryStick, etc)
- 2.2.42.15. Dispositivos de sincronização via ActiveSync (Windows CE, Windows Mobile, etc)
- 2.2.42.16. Dispositivos Bluetooth
- 2.2.43. Deve ter capacidade para desabilitar o autoplay em todos os dispositivos (drives de cd, usb, rede, etc)
- 2.2.44. Deve ter capacidade para desabilitar o processamento de arquivos autorun.inf sem desabilitar o autoplay por completo.

### 3. Estações de trabalho Linux

#### 3.1. Compatibilidade:

##### 3.1.1. Plataforma 32-bits:

- 3.1.1.1. Red Hat Enterprise Linux 5.2 Desktop (kernel 2.6.18-92)
- 3.1.1.2. Fedora 9 (kernel 2.6.25)
- 3.1.1.3. SUSE Linux Enterprise Desktop 10 SP2 (kernel 2.6.16.60-0.21)
- 3.1.1.4. openSUSE Linux 11.0 (kernel 2.6.25)
- 3.1.1.5. Debian GNU/Linux 4.0 r4 (kernel 2.6.24)
- 3.1.1.6. Mandriva Corporate Desktop 4 (kernel 2.6.12)
- 3.1.1.7. Ubuntu 8.04.1 Desktop Edition (kernel 2.6.25)
- 3.1.1.8. Linux XP Enterprise Desktop 2008 (2.6.25.10-47.3.lxp2008)

##### 3.1.2. Plataforma 64-bits:

- 3.1.2.1. Red Hat Enterprise Linux 5.2 Desktop (kernel 2.6.18-92)
- 3.1.2.2. Fedora 9 (kernel 2.6.25)
- 3.1.2.3. SUSE Linux Enterprise Desktop 10 SP2 (kernel 2.6.16.60-0.21)
- 3.1.2.4. openSUSE Linux 11.0 (kernel 2.6.25)

#### 3.2. Características:

##### 3.2.1. Deve prover as seguintes proteções:

- 3.2.1.1. Antivírus de arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
- 3.2.1.2. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora.

##### 3.2.2. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

- 3.2.2.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
- 3.2.2.2. Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfetar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;
- 3.2.2.3. Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;

- 3.2.2.4. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados.
- 3.2.3. Em caso erros, deve ter capacidade de criar *logs* automaticamente, sem necessidade de outros softwares;
- 3.2.4. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
- 3.2.5. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomá-la a partir da extensão do arquivo;
- 3.2.6. Capacidade de verificar objetos usando heurística;
- 3.2.7. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena
- 3.2.8. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados
- 3.2.9. Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).

#### 4. Servidores Windows

##### 4.1. Compatibilidade:

- 4.1.1. Microsoft Windows 2000 Server Service Pack 4 + Update Rollup 1 ou superior
- 4.1.2. Microsoft Windows 2000 Advanced Server Service Pack 4 + Update Rollup 1 ou superior
- 4.1.3. Microsoft Windows Server 2003 Web/Standard/Enterprise/DataCenter Edition Service Pack 1 ou superior
- 4.1.4. Microsoft Windows Server 2003 Web/Standard/Enterprise/DataCenter Edition x64
- 4.1.5. Microsoft Windows Server 2003 R2 Standard/Enterprise/DataCenter Edition
- 4.1.6. Microsoft Windows Server 2003 R2 Standard/Enterprise/DataCenter Edition x64
- 4.1.7. Microsoft Windows Storage Server 2003 R2
- 4.1.8. Microsoft Windows Server 2008 Standard/Enterprise/DataCenter Edition
- 4.1.9. Microsoft Windows Server 2008 Standard/Enterprise/DataCenter Edition x64
- 4.1.10. Microsoft Windows Server 2008 Core Standard/Enterprise/DataCenter Edition
- 4.1.11. Microsoft Windows Server 2008 Core Standard/Enterprise/DataCenter Edition x64
- 4.1.12. Microsoft Terminal baseado em Windows 2000 Server
- 4.1.13. Microsoft Windows Small Business Server 2003
- 4.1.14. Microsoft Windows Small Business Server 2008
- 4.1.15. Windows Essential Business Server 2008
- 4.1.16. Microsoft Terminal baseado em Windows 2003 Server
- 4.1.17. Microsoft Terminal baseado em Windows 2008 Server

##### 4.2. Características:

- 4.2.1. Deve prover as seguintes proteções:
  - 4.2.1.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
  - 4.2.1.2. Auto-proteção contra ataques aos serviços/processos do antivírus
- 4.2.2. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;

- 4.2.3. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora.
- 4.2.4. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
  - 4.2.4.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
  - 4.2.4.2. Gerenciamento de tarefa (criar ou excluir tarefas de verificação)
  - 4.2.4.3. Leitura de configurações
  - 4.2.4.4. Modificação de configurações
  - 4.2.4.5. Gerenciamento de Backup e Quarentena
  - 4.2.4.6. Visualização de relatórios
  - 4.2.4.7. Gerenciamento de relatórios
  - 4.2.4.8. Gerenciamento de chaves de licença
  - 4.2.4.9. Gerenciamento de permissões (adicionar/excluir permissões acima)
- 4.2.5. Capacidade de separadamente selecionar o número de processos que irão executar funções de varredura em tempo real, o número de processos que executarão a varredura sob-demanda e o número máximo de processos que podem ser executados no total.
- 4.2.6. Capacidade de resumir automaticamente tarefas de verificação que tenham sido paradas por anormalidades (queda de energia, erros, etc)
- 4.2.7. Capacidade de automaticamente pausar e não iniciar tarefas agendadas caso o servidor esteja em rodando com fonte ininterrupta de energia (*uninterruptible Power supply – UPS*)
- 4.2.8. Em caso erros, deve ter capacidade de criar *logs* e *traces* automaticamente, sem necessidade de outros softwares;
- 4.2.9. Capacidade de configurar níveis de verificação diferentes para cada pasta, grupo de pastas ou arquivos do servidor.
- 4.2.10. Capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado nos servidor.
- 4.2.11. Capacidade de criar uma lista de máquina que nunca serão bloqueadas mesmo quando infectadas.
- 4.2.12. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;
- 4.2.13. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: "Win32.Trojan.banker") para que qualquer objeto detectado com o veredicto escolhido seja ignorado;
- 4.2.14. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
- 4.2.15. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomá-la a partir da extensão do arquivo;
- 4.2.16. Capacidade de verificar somente arquivos novos e alterados;
- 4.2.17. Capacidade de escolher qual tipo de objeto composto será verificado (ex: arquivos comprimidos, arquivos auto-descompressores, .PST, arquivos compactados por compactadores binários, etc)
- 4.2.18. Capacidade de verificar objetos usando heurística;

- 4.2.19. Capacidade de configurar diferentes ações para diferentes tipos de ameaças;
- 4.2.20. Capacidade de agendar uma pausa na verificação;
- 4.2.21. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;
- 4.2.22. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
  - 4.2.22.1. Perguntar o que fazer, ou;
  - 4.2.22.2. Bloquear acesso ao objeto;
    - 4.2.22.2.1. Apagar o objeto ou tentar desinfecção (de acordo com a configuração pré-estabelecida pelo administrador);
    - 4.2.22.2.2. Caso positivo de desinfecção:
      - 4.2.22.2.2.1. Restaurar o objeto para uso;
    - 4.2.22.2.3. Caso negativo de desinfecção:
      - 4.2.22.2.3.1. Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);
- 4.2.23. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto.
- 4.2.24. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena
- 4.2.25. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados
- 4.2.26. Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa.

## 5. Servidores Linux

### 5.1. Compatibilidade:

#### 5.1.1. Plataforma 32-bits:

- 5.1.1.1. Red Hat Enterprise Linux 5.2 Server (kernel 2.6.18-92)
- 5.1.1.2. Fedora 9 (kernel 2.6.25)
- 5.1.1.3. SUSE Linux Enterprise Server 10 SP2 (kernel 2.6.16.60-0.21)
- 5.1.1.4. Novel Open Enterprise Server 2 (kernel 2.6.16.46-0.12)
- 5.1.1.5. openSUSE Linux 11.0 (kernel 2.6.25)
- 5.1.1.6. Debian GNU/Linux 4.0 r4 (kernel 2.6.24)
- 5.1.1.7. Mandriva Corporate Server 4 (kernel 2.6.12)
- 5.1.1.8. Ubuntu 8.04.1 Server Edition (kernel 2.6.25)

#### 5.1.2. Plataforma 64-bits:

- 5.1.2.1. Red Hat Enterprise Linux 5.2 Server (kernel 2.6.18-92)
- 5.1.2.2. Fedora 9 (kernel 2.6.25)
- 5.1.2.3. SUSE Linux Enterprise Server 10 SP2 (kernel 2.6.16.60-0.21)
- 5.1.2.4. openSUSE Linux 11.0 (kernel 2.6.25)

### 5.2. Características:

#### 5.2.1. Deve prover as seguintes proteções:

- 5.2.1.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
- 5.2.1.2. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora.

#### 5.2.2. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

- 5.2.2.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
  - 5.2.2.2. Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfetar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;
  - 5.2.2.3. Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;
  - 5.2.2.4. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados.
  - 5.2.3. Em caso erros, deve ter capacidade de criar *logs* automaticamente, sem necessidade de outros softwares;
  - 5.2.4. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
  - 5.2.5. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomá-la a partir da extensão do arquivo;
  - 5.2.6. Capacidade de verificar objetos usando heurística;
  - 5.2.7. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena
  - 5.2.8. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados
  - 5.2.9. Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux)
6. Smartphones
- 6.1. Compatibilidade:
    - 6.1.1. Symbian S60 9.1 – 9.4
    - 6.1.2. Windows Mobile 5.0 – 6.5
    - 6.1.3. BlackBerry 4.5 – 5.0
  - 6.2. Características:
    - 6.2.1. Deve prover as seguintes proteções:
      - 6.2.1.1. Proteção em tempo real do sistema de arquivos do dispositivo – interceptação e verificação de:
        - 6.2.1.1.1. Todos os objetos transmitidos usando conexões wireless (porta de infra-vermelho, Bluetooth) e mensagens EMS, durante sincronismo com PC e ao realizar download usando o browser.
        - 6.2.1.1.2. Arquivos abertos no smartphone
        - 6.2.1.1.3. Programas instalados usando a interface do smartphone
      - 6.2.1.2. Verificação dos objetos na memória interna do smartphone e nos cartões de expansão sob demanda do usuário e de acordo com um agendamento;
    - 6.2.2. Deverá isolar em área de quarentena os arquivos infectados;
    - 6.2.3. Deverá atualizar as bases de vacinas de modo agendado;
    - 6.2.4. Deverá bloquear spams de SMS através de Black lists;
    - 6.2.5. Deverá ter função de bloqueio do aparelho caso o SIM CARD for trocado para outro não autorizado;

- 6.2.6. Deverá ter função de limpeza de dados pessoais a distância, em caso de roubo, por exemplo.
    - 6.2.7. Deverá ter firewall pessoal;
    - 6.2.8. Possibilidade de instalação remota utilizando o Microsoft System Center Mobile.
7. Licenciamento
  - 7.1. A solução deve ser licenciada para 60 (sessenta) estações de trabalho e servidores, licenças válidas por 36(trinta e seis) meses, com possibilidade de renovação.
8. Implantação e Treinamento
  - 8.1. A contratada deverá possuir todos os recursos necessários para implantação da solução durante o período da migração, e, não obstante, agendar com a equipe de tecnologia de informação da Câmara Municipal de Anchieta, o início das atividades.
  - 8.2. O processo de migração deverá ser homologado no início dos trabalhos através da realização de um Piloto com um número de estações de trabalho e servidores a serem acordados com a equipe de tecnologia da informação da Câmara Municipal de Anchieta.
  - 8.3. Deverão ser criados grupos ou perfis para adequação da configuração das estações de trabalho e servidores de acordo com o seu perfil.
  - 8.4. Caso o produto ofertado seja de fabricante diferente do atual ou não possibilite a atualização automática desta será de responsabilidade da contratada a desinstalação do produto atual em todas as estações de trabalho e servidores.
  - 8.5. Deverá ser realizado um treinamento de no mínimo 08 horas, para capacitação de 1 (um) colaborador da equipe técnica da Câmara Municipal de Anchieta.
  - 8.6. O treinamento deverá ser realizado nas dependências da CMA ou outro local providenciado por esta.
9. Documentação
  - 9.1. A contratada deverá fornecer ao término do projeto a documentação da solução contendo:
    - a) Relatório de Implantação
    - b) Topologia Implantada
    - c) Configurações Realizadas
    - d) Procedimento de Recuperação de Desastre do Servidor.
  - 9.2. O fabricante deverá prover Assistência Técnica, em horário comercial e para todos os produtos ofertados, via telefone discagem gratuita (0800) ou suporte nível Brasil, por e-mail, chat e acesso remoto, comprovados por declaração do fabricante.
  - 9.3. Apresentar 02 (dois) atestados fornecidos por empresa pública ou privada comprovando que o licitante forneceu soluções semelhantes ao objeto deste edital (inclusive em quantitativos e serviços/treinamento) com no mínimo mesmo porte de ambiente computacional da CMA.

### **Item 03 - Implantação de soluções baseadas no MS Windows Server 2008**

- Instalação e implantação de um servidor WSUS baseado em Windows Server 2008, para atualização automática de todos os aplicativos Microsoft utilizados na Câmara Municipal de Anchieta.

- Replicação do AD (Active Directory) existente na CMA, para uma máquina virtual que funcionará como domínio secundário.
- A contratada deverá fornecer ao término do projeto a documentação das soluções implantadas.
- Deverá ser realizado um treinamento, para capacitação de 01 (um) colaborador da equipe técnica da Câmara Municipal de Anchieta.

## **LOTE 02 - SERVIDOR PARA RACK**

### **1. GABINETE**

- 1.1. Gabinete tipo rack com altura de, no máximo, 1U original do fabricante do equipamento;
- 1.2. Possuir, no mínimo, 4 (quatro) baias de 2,5" polegadas para disco rígido hot-puggable;
- 1.3. A ventilação deve ser adequada para a refrigeração do sistema interno do equipamento na sua configuração máxima e dentro dos limites de temperatura adequados para operação;
- 1.4. Fonte de alimentação com potência de no mínimo 350 Watts, suficiente para o funcionamento na sua configuração máxima;
- 1.5. As fontes de alimentação devem operar nas faixas de tensão de entrada de 100-240 VAC em 60 Hz;
- 1.6. Acompanhar cabos de alimentação para fonte de alimentação.

### **2. PROCESSADOR**

- 2.1. Possuir 01 (um) processador x86 com no mínimo quatro núcleos (quad-core), projetados para utilização em servidores.
- 2.2. Suportar operações em 32/64 bits;
- 2.3. Controladora de memória RAM integrada;
- 2.4. Memória cache L3 de 08 MB ou superior;
- 2.5. Frequência de clock de 2.4 GHz ou superior

### **3. MEMÓRIA**

- 3.1. Módulos de memória tipo DDR3 RDIMM (Registered DIMM) com tecnologia de correção ECC (Error Correcting Code) e barramento de, no mínimo, 1066 MHz;
- 3.2. Possuir 04 GB de memória RAM instalada;
- 3.3. O equipamento deve suportar escalabilidade de no mínimo 32 GB, através de no mínimo 06 slots de memória em módulos de memória RAM do tipo RDIMM (Registered DIMM).

### **4. CIRCUITOS INTEGRADOS (CHIPSET) E PLACA MÃE**

- 4.1. O chipset deve ser da mesma marca do fabricante dos processadores e suportar a velocidade de comunicação com os mesmos;

4.2. Placa mãe da mesma marca do fabricante do equipamento, desenvolvida especificamente para o modelo ofertado, não sendo essa de livre comercialização;

4.3. O equipamento deve possuir os seguintes slots de expansão:

- 02 (dois) slots PCI-Express x8 geração 2;
- 4.4. BIOS desenvolvida pelo mesmo fabricante do equipamento ou o fabricante deve ter direito copyright sobre essa BIOS, comprovado através de atestado fornecido pelo fabricante do equipamento. Não será aceito soluções de BIOS em regime OEM ou customizadas;
- 4.5. A BIOS deve possuir o número de série/serviço do equipamento e campo editável que permita inserir identificação de ativo podendo ser consultada por software de gerenciamento.

## **5. PORTAS DE COMUNICAÇÃO**

- 5.1. Todos os conectores das portas de entrada/saída de sinal são identificados pelos nomes ou símbolos;
- 5.2. Possuir no mínimo 06 (seis) portas USB versão 2.0, sendo 02 (duas) delas situadas na parte frontal do gabinete;
- 5.3. Possuir 01 (uma) porta serial (DB-9) integrada.

## **6. INTERFACES DE REDE**

- 6.1. Possuir 02 (duas) interfaces de rede padrão RJ-45;
- 6.2. As controladoras de rede devem ser padrão Gigabit Ethernet com tecnologia TOE (TCP/IP Offload Engine) e compatíveis com os padrões 10Base-T/100Base-TX/1000Base-T;
- 6.3. Suportar Receive Side Scaling (RSS), PXE e Virtual LANs.

## **7. CONTROLADORA RAID**

- 7.1. Controladora RAID da mesma marca do fabricante do equipamento, compatível com discos rígido padrão SAS e SATA;
- 7.2. Memória cachê de 128 MB ou superior;
- 7.3. Suporte nativo de RAID 0, 1, via hardware;
- 7.4. Possuir canais suficientes para controlar a quantidade de discos suportada pelo equipamento;

## **8. ARMAZENAMENTO**

- 8.1. Possuir 02 (dois) discos rígido SAS (Serial Attached SCSI) de 146 GB 10.000 rpm, hot pluggable;
- 8.2. Devem acompanhar todos os acessórios necessários para a função hot-pluggable dos discos rígido (trilhos, backplanes, etc.);
- 8.3. Possuir driver óptico DVD-ROM.

## **9. GERENCIAMENTO E INVENTÁRIO**

- 9.1. O equipamento ofertado deverá possuir recurso de gerenciamento compatível com o padrão IPMI 2.0 que possibilite o gerenciamento através de controladora de gerenciamento integrada com porta RJ-45 dedicada, não sendo essa nenhuma das interfaces de controladora de rede, e software de gerenciamento;

9.2.A controladora de gerenciamento integrada deve suportar as seguintes características:

- Compatível com os protocolos de criptografia SSL para acesso a console WEB e SSH para console CLI;
- Deve permitir controle remoto tipo virtual KVM mesmo quando o sistema operacional estiver inoperante;
- Deve informar o status do equipamento indicando componentes com falha e notificando via e-mail ou trap SNMP;
- Deve possuir emulação de mídia virtual possibilitando que drivers (CD/DVD, Floppy) localizado em estação de gerenciamento seja emulado no servidor gerenciado permitindo a inicialização (boot) através dessa mídia;
- Capacidade de monitorar o consumo de energia do servidor;
- Deve permitir desligar e reinicia do servidor através da console de gerenciamento, mesmo em condições de indisponibilidade do sistema operacional;

9.3. Software de gerenciamento centralizado com os seguintes recursos:

- Permitir o gerenciamento centralizado e individual de todos os servidores ofertados através de interface WEB;
- Realizar inventário de hardware, BIOS e firmware e possibilitar a geração de relatórios customizados;
- Emitir alertas de falha de hardware e permitir a criação de filtros de alertas isolados e notificação por e-mail;
- Agente compatível com os sistemas operacionais Windows Server 2003/2008, Red Hat Linux Enterprise 5 e Suse Linux Enterprise Server.

9.4. A controladora de gerenciamento integrada deve operar em conjunto com o software de gerenciamento, devendo ambos serem soluções proprietárias do fabricante dos equipamentos com a finalidade de garantir total compatibilidade e suporte único.

## **10. COMPATIBILIDADE COM SISTEMA OPERACIONAL**

- 10.1. O modelo do equipamento ofertado deve estar certificado para o sistema operacional Windows 2008 Server a ser comprovado através do *WindowsServer Catalog* da Microsoft;
- 10.2. O modelo do equipamento ofertado deve estar certificado para o sistema operacional Red Hat Enterprise Linux 5 ou posterior a ser comprovado através do HCL (Hardware Compatibility List) da Red Hat;
- 10.3. O modelo do equipamento ofertado deve estar certificado para o sistema operacional Suse Linux Enterprise Server 10 ou posterior a ser comprovado através do HCL (Hardware Compatibility List) da Novell;

## **11. SISTEMA OPERACIONAL**

- 11.1. Acompanhar licença do Sistema Operacional Microsoft Windows Server 2008 Standard R2 64 bits, versão em português do Brasil.
- 11.2. O sistema operacional Microsoft Windows Server 2008 deve estar pré-instalado, bem como, todos os drives de adaptadores internos necessário para seu funcionamento.

## **12. COMPONENTES E ACESSORIOS**

- 12.1. Acompanhar mídia de inicialização e configuração do equipamento contendo todos os drivers de dispositivos de forma a permitir a fácil instalação do equipamento. Não são aceitos para atendimento deste item, mídia contendo somente os drivers;
- 12.2. O fabricante do equipamento deve disponibilizar no seu respectivo web site, download gratuito de todos os Drivers, BIOS e Firmwares dos componentes que compõem este equipamento, a fim de permitindo atualizações necessárias;
- 12.3. Deverá ser fornecido kit de trilhos e braço organizador de cabos do mesmo fabricante do equipamento ofertado, para fixação dos equipamentos em rack 19 polegadas padrão EIA-310D;
- 12.4. Os trilhos devem permitir o deslizamento do equipamento a fim de facilitar a manutenção;
- 12.5. Deverão ser fornecidos manuais técnicos do usuário e de referência contendo todas as informações sobre os produtos com as instruções para instalação, configuração, operação e administração.

## **13. GARANTIA E SUPORTE**

- 13.1. Os equipamentos devem possuir garantia do fabricante por um período mínimo de 36 (trinta e seis) meses;
- 13.2. Os serviços de reparo dos equipamentos especificados devem ser executados no local onde se encontram instalados, ou seja, on-site;
- 13.3. Durante o prazo de garantia será substituída sem ônus para o contratante, a parte ou peça defeituosa, salva quando o defeito for provocado por uso inadequado dos equipamentos;
- 13.4. O serviço de suporte compreende a abertura de chamados 24x7, ou seja, vinte e quatro horas por dia em sete dias por semana;
- 13.5. O prazo máximo para atendimento e reparo/solução dos chamados abertos, contado a partir da abertura do chamado e dentro do período de disponibilidade para atendimento, é de 8 (oito) horas;
- 13.6. A contratada deve possuir Central de Atendimento tipo (0800) para abertura dos chamados de garantia, comprometendo-se à manter registros dos mesmos constando a descrição do problema;
- 13.7. Será considerado como período de disponibilidade para atendimento o intervalo de tempo disponibilizado para a manutenção dos equipamentos.

## **14. OUTRAS EXIGÊNCIAS**

- 14.1. Quando o Licitante não for o próprio fabricante dos equipamentos ofertados, deverá apresentar declaração do Fabricante, autorizando a empresa Licitante a comercializar e prestar os serviços de garantia exigidos;
- 14.2. Declaração de que o equipamento e todos os seus componentes são novos, de primeiro uso e estão em linha de fabricação na data de abertura das propostas;
- 14.3. Serviço de instalação física de todos os servidores ofertados em local indicado pela contratante.

**ANEXO II**  
**PLANILHA DE QUANTITATIVOS E ESTIMATIVA DE PREÇOS**

**LOTE 01**

<i>Item</i>	<i>Un</i>	<i>Qtde</i>	<i>Descrição</i>	<i>Preço Estimado</i>
01	Un	01	Aquisição e implantação de software de Gerenciamento de Backup	12.434,00

<i>Item</i>	<i>Un</i>	<i>Qtde</i>	<i>Descrição</i>	<i>Preço Estimado</i>
02	Un	01	Aquisição e implantação de nova Solução de Segurança (antivírus)	7.100,00

<i>Item</i>	<i>Un</i>	<i>Qtde</i>	<i>Descrição</i>	<i>Preço Estimado</i>
03	Un	01	Implantação de soluções baseadas no MS Windows Server 2008.	6.966,00

Valor total estimado do LOTE 01, obtido após media dos orçamentos recebidos .....R\$ 26.500,00

**LOTE 02**

<i>Item</i>	<i>Un</i>	<i>Qtde</i>	<i>Descrição</i>	<i>Preço Estimado</i>
01	Un	01	Aquisição de um servidor para rack	8.666,00

Valor total estimado do LOTE 02, obtido após media dos orçamentos recebidos .....R\$ 8.666,00

**VALOR TOTAL ESTIMADO DA LICITAÇÃO..... R\$ 35.166,00**

**ANEXO III**

**Modelo de Declaração (Item 8.1, alínea "a", do Edital)**

*(Papel timbrado ou carimbo da empresa)*

**DECLARAÇÃO**

A.....(Razão Social da empresa)....., CNPJ ....., com endereço à....., declara, em conformidade com o art. 32, parágrafo 2º, da Lei n. 8.666/93, que não existem fatos supervenientes ao seu cadastramento no **Sistema Integrado de Administração de Serviços Gerais - SIASG/SICAF** que sejam impeditivos de sua habilitação para este certame licitatório no Tribunal Regional do Trabalho da 23ª Região.

*Local e data,*

*(Assinatura e identificação do responsável pela empresa)*

**ANEXO IV**

**Modelo de Declaração (Item 8.1, alínea “b”, do Edital)**

*(Papel timbrado ou carimbo da empresa)*

**DECLARAÇÃO**

A.....(Razão Social da empresa)....., CNPJ ....., com endereço à....., declara, em atendimento ao previsto no item 8.1, alínea “b” do Edital **Pregão nº.\_\_\_\_\_/\_\_\_\_**, **que não possuímos** em nosso quadro de pessoal empregado(s) com menos de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre e de 16 (dezesseis) anos em qualquer trabalho, salvo na condição de aprendiz, se for o caso, nos termos do inciso XXXIII do art. 7º da Constituição República Federativa do Brasil.

*Local e data,*

*(Assinatura e identificação do responsável pela empresa)*

## ANEXO V

### Modelo de Carta de Representação

(Papel timbrado ou carimbo da empresa)

### CARTA DE REPRESENTAÇÃO

A.....(Razão Social da empresa)....., CNPJ ....., com endereço à....., através do seu ..... (proprietário, sócio-proprietário, presidente, gerente, diretor), .....(nacionalidade), .....(estado civil), portador do RG n ....., CPF n. ...., residente à ....., **CONSTITUI** como seu representante no certame licitatório – modalidade **Pregão n. \_\_\_\_\_/\_\_\_** a ser realizado pelo Tribunal Regional do Trabalho da 23ª Região, o Sr.(a) ....., (nacionalidade), .....(estado civil), portador do RG n ....., CPF n. ...., residente à ....., que poderá formular ofertas e lances de preço e praticar todos os demais atos pertinentes ao certame em nome da representada, inclusive renúncia ao direito de interpor e desistir de recursos.

Local e data,

(Assinatura e identificação do responsável pela empresa)

#### Obs:

- **Declaração com firma reconhecida (item 4.2 do edital)**

## Anexo VI

### Modelo de Minuta de Contrato

Contrato nº \_\_\_\_\_

Processo nº 87/2011

Pregão Presencial nº 03/2011

O Município de Anchieta, Poder Legislativo, Estado do Espírito Santo, pessoa jurídica de direito público interno, com sede à Rua Nancy Ramos Rosa, s/nº, Bairro Portal de Anchieta, inscrito no CNPJ-MF sob o nº 31.803.125/0001-83, neste ato representado por seu representante legal, XXX, inscrito no CPF n.ºxxxxx, doravante denominado CONTRATANTE, e a empresa \_\_\_\_\_, inscrita no CNPJ sob o nº \_\_\_\_\_ neste ato representado por seu representante legal o Sr(a). \_\_\_\_\_, portador do R.G. nº \_\_\_\_\_ -SSP/\_\_\_ e inscrito no CPF sob o nº \_\_\_\_\_, brasileiro(a), casado(A), comerciante, residente e domiciliado na Rua: \_\_\_\_\_ nº \_\_\_\_ Bairro: \_\_\_\_\_ Cidade: \_\_\_\_\_ Estado: \_\_\_\_\_, doravante denominado CONTRATADA, ajustam o presente CONTRATO ADMINISTRATIVO de prestação de serviços, nos termos da Lei nº 8.666/93 e suas alterações, conforme os termos do(s) Processo(s) de nº(s) 0XXX/20xx, e de acordo com as Cláusulas e condições seguintes:

#### CLÁUSULA PRIMEIRA - DO OBJETO:

1.1 - Constitui objeto do presente, a aquisição:

01	Aquisição e implantação de software de Gerenciamento de Backup
02	Aquisição e implantação de nova Solução de Segurança (Antivírus)
03	Aquisição de um servidor para rack.
04	Implantação de soluções baseadas no MS Windows Server 2008

#### CLÁUSULA SEGUNDA - DA VIGÊNCIA:

2.1- O presente contrato de prestação de serviços e entrega dos equipamentos terá a vigência a partir da data de sua assinatura, vigorando por 15(quinze) dias, prazo para execução do serviço, desde que publicado na forma da Lei, podendo ser rescindido por ambas as partes, a qualquer momento, desde que devidamente denunciado por escrito, com antecedência mínima de 30 (trinta) dias, podendo ser prorrogado na forma do artigo 57 da Lei nº 8.666/93.

#### CLÁUSULA TERCEIRA – DO VALOR

3 – O valor total do presente Contrato é de R\$ .....(.....), pagos através de medições mensais .

#### CLÁUSULA QUARTA – DO REAJUSTE DOS VALORES

4 - Os preços firmados entre os contratantes não serão passíveis de reajustes durante a vigência do contrato administrativo celebrado, resguardado a revisão para manter o equilíbrio econômico-financeiro, devidamente fundamentada.

#### **CLÁUSULA QUINTA - DA FORMA DE PAGAMENTO**

**5** - O pagamento será efetuado no prazo de até 20 (vinte) dias, através da Tesouraria do Contratante ou através de depósito em conta corrente do prestador do serviço, no Banco por ele indicado, contados da data da prestação dos serviços, constante no verso da Nota Fiscal/Fatura em 02 (duas) vias, juntamente com o Empenho, com o visto do funcionário competente, do setor responsável pela comprovação dos serviços.

**5.1** - Ocorrendo erro na apresentação das faturas, as mesmas serão devolvidas ao fornecedor para retificação, ficando estabelecido que o pagamento será efetuado após a apresentação da nova fatura devidamente retificada, correndo o mesmo prazo previsto no item 5.1;

**5.2** - É expressamente vedado ao prestador, cobrança ou desconto de duplicatas através de rede bancária ou de terceiros.

**5.3** - Os pagamentos serão efetuados somente após a comprovação da Regularidade Fiscal, mediante apresentação junto as Notas Fiscais/Faturas, de cópias autenticadas em Cartório, das certidões negativas de débitos com Tributos Federais, Fazenda Nacional, Estadual, Municipal, e com a Seguridade Social - INSS e FGTS.

**5.4** - **É vedada a antecipação de pagamentos sem a contraprestação dos serviços.**

#### **CLÁUSULA SEXTA - DOS RECURSOS ORÇAMENTÁRIOS**

**6** - As despesas decorrentes da execução deste contrato correrão à conta da dotação orçamentária , 333903900000 e 344905200000 da Câmara Municipal de Anchieta – ES.

#### **CLÁUSULA SETIMA - DO PRAZO DE EXECUÇÃO E DA FISCALIZAÇÃO**

**7** - O prazo de execução dos serviços será de 15 dias, sendo responsável pela fiscalização do referido contrato o Analista de Sistemas da Câmara de Anchieta, podendo ser prorrogado na forma prevista no artigo 57 da Lei nº 8.666/93 e suas alterações;

**7.2** - **O prazo máximo para início dos serviços fica fixado em 05 (cinco) dias úteis, contados a partir da data da assinatura do Contrato pela CONTRATADA.**

**7.3** – **A CONTRATADA, julgando insuficientes os elementos fornecidos , deverá solicitar por escrito , explicações e novos dados, dentro do prazo de 05 (cinco) dias contados do recebimento dos elementos da fiscalização. Nesse caso, o prazo de execução será contado a partir da data de recebimento dos esclarecimentos solicitados, se os mesmos impedirem o início dos serviços.**

#### **CLÁUSULA OITAVA - DAS PENALIDADES**

**8.1** - O não cumprimento pela CONTRATADA, de quaisquer das obrigações assumidas no presente contrato, facultará ao Contratante a aplicação das penalidades previstas no Edital e, quando o caso, a rescisão contratual.

#### **CLÁUSULA NONA - DA RESCISÃO**

**9.1** - O presente Contrato poderá ser rescindido nas hipóteses estabelecidas nos artigos. 77, 78 e 79 da Lei 8.666/93 e suas alterações.

**9.2** – Se o descumprimento deste Contrato gerar conseqüências graves para o Contratante, este poderá, além de rescindir o Contrato, aplicar uma das penalidades previstas no Edital.

## **CLÁUSULA DÉCIMA - DA RESPONSABILIDADE DAS PARTES**

**10.1** - Constituem obrigações da CONTRATANTE:

**10.1.1** - Efetuar à CONTRATADA o pagamento de preço ajustado na **Cláusula Terceira** e nos termos ali estabelecidos.

**10.1.2** - Designar servidor(es) responsável(eis) pelo acompanhamento e fiscalização do objeto deste Contrato.

**10.2** - Constituem obrigações da CONTRATADA:

**10.2.1** - Executar os serviços de acordo com o especificado na Cláusula Primeira deste Contrato, por intermédio exclusivo de seus empregados;

**10.2.2** – Fornecer material e equipamentos necessários à execução dos serviços especificados e proposta apresentada, que deverão ser de qualidade comprovada, competindo à CONTRATANTE a fiscalização e a verificação de tais condições durante toda a execução do contrato;

**10.2.3** – Responsabilizar-se por todos os consertos e ajustes que se fizerem necessários para a perfeita execução dos serviços;

**10.2.4** – Fornecer toda a mão de obra, ferramentas, instrumentos e equipamentos necessários à realização completa dos serviços;

**10.2.5** - Apresentar os documentos de cobrança, inclusive Nota(as) Fiscal(is) com a descrição completa dos serviços;

**10.2.6** – Deverá manter-se, durante toda a execução do contrato, compatível com as obrigações por ele assumidas, e em dia com as condições de habilitação e qualificação exigidas na licitação.

## **CLÁUSULA DÉCIMA PRIMEIRA - DOS RECURSOS PROCESSUAIS**

**11.1** - Dos atos de aplicação de penalidade prevista neste instrumento ou de sua rescisão, praticados pelo Contratante, cabe recurso no prazo de 02(dois) dias úteis, a contar da intimação do ato.

**Parágrafo Único:** Da decisão do responsável da Contratante que rescindir o presente contrato cabe, inicialmente, pedido de reconsideração, no prazo de 02(dois) dias úteis, a contar da intimação do ato.

## **CLÁUSULA DÉCIMA SEGUNDA - DAS DISPOSIÇÕES FINAIS**

**12.1** - O presente contrato será publicado na imprensa oficial na forma da Lei Orgânica, contados da data de sua assinatura.

**12.2** - Fazem parte deste Contrato, como se nele transcritas, todas as condições estabelecidas no Edital.

**12.3** - As partes elegem o foro da Comarca de Anchieta, Estado do Espírito Santo, com renúncia expressa de qualquer outro, para dirimir as questões oriundas do presente contrato, que não puderem ser resolvidas em comum acordo.

**12.4** - E, por estarem justas e contratadas, firmam o presente instrumento em 02(duas) vias de

igual teor e forma, na presença das testemunhas abaixo assinadas.

Anchieta(ES), \_\_\_\_ de \_\_\_\_\_ de 2.011.

XXXX  
**Presidente da Câmara Municipal de  
Anchieta  
CONTRATANTE**

XXX  
**CONTRATADA**

Testemunhas: 1- \_\_\_\_\_ 2- \_\_\_\_\_