RECIBO

A Empresa_____ CNPJ n.º _____, retirou este Edital de licitação e deseja ser informada de qualquer alteração pelo telefone_____ celular_____ ou por e-mail.

Nome legível e Assinatura

OBS.: Este Recibo deverá ser remetido à Prefeitura de Pouso Alegre - MG para o e-mail recursosmateriais@pousoalegre.mg.gov.br ou cpd@pousoalegre.mg.gov.br

A PREFEITURA MUNICIPAL DE POUSO ALEGRE - MG não se responsabiliza por comunicações à empresa que não encaminhar este recibo ou prestar informações incorretas no mesmo.

Do(a) Pregoeiro(a)

Para Assessoria

Estamos remetendo o presente referente ao Pregão a ser instaurado, com a minuta do edital e seus anexos para analise e parecer de Vossas Senhorias.

Pouso Alegre, 17 de outubro de 2017

Daniela Luiza Zanatta
Pregoeiro(a)

Declaro a abertura da Licitação na modalidade própria

Na qualidade de ordenador de despesa, declaramos que o presente gasto, dispõe de suficiente dotação e de firme e consistente expectativa de suporte de caixa, conformando-se as orientações do Plano Plurianual (PPA) e da Lei de Diretrizes Orçamentárias (LDO).

Pouso Alegre, 17 de outubro de 2017.

Julio César da Silva Tavares
Secretário de Administração e Finanças

Rinaldo Lima Oliveira
Secretário de Planejamento

PREAMBULO

PREGÃO PRESENCIAL Nº 70/2017
MODALIDADE: PREGÃO PRESENCIAL
TIPO: MENOR PREÇO
ÓRGÃO REQUISITANTE: SECRETARIA MUNICIPAL DE ADMINISTRAÇÃO E FINANÇAS.

DATA DE ABERTURA: 06/11/2017
HORÁRIO: 9:00 horas

I - OBJETO

1.1 Constitui objeto deste PREGÃO PRESENCIAL a CONTRATAÇÃO DE EMPRESA PARA a aquisição de LICENÇA DE ANTIVIRUS, de acordo com memorial descritivo e demais disposições constantes do edital e dos respectivos anexos.

1.2 A empresa vencedora se obrigará ao atendimento de todos os pedidos efetuados durante a sua vigência, ainda que o término da entrega dos objetos esteja previsto para data posterior a de seu termo final.

II - PRAZO DE EXECUÇÃO DOS SERVIÇOS

2.1 O Contrato terá a duração de 12 meses a partir de sua assinatura.

III - DOTAÇÃO ORÇAMENTÁRIA

No exercício de 2017, as despesas correrão à conta da dotação orçamentária:

n.º 02.08.04.122.0017.2066.3.3.90.39.00 – Ficha 495

Caso necessário, no exercício seguinte, as despesas correrão à conta de dotação orçamentária própria, consignada no respectivo Orçamento-Programa, ficando a Administração obrigada a apresentar, no início de cada exercício, a respectiva Nota de Empenho estimativa e, havendo necessidade, emitir Nota de Empenho complementar, respeitadas as mesmas classificações orçamentárias.

Pouso Alegre, 17 de outubro de 2017

Daniela Luiza Zanatta
Pregoeiro(a)

EDITAL

PREFEITURA MUNICIPAL DE POUSO ALEGRE - MG

PREGÃO PRESENCIAL Nº 70/2017

(Processo Administrativo n° 226/2017)

Torna-se público, para conhecimento dos interessados, que o MUNICÍPIO DE POUSO ALEGRE - MG, por meio do(a) Pregoeiro(a) Sr(a) Daniela Luiza Zanatta, sediada na Rua Carijós, 45, Bairro Centro, Pouso Alegre - MG, realizará licitação, na modalidade PREGÃO, na forma PRESENCIAL, do tipo menor preço, de acordo com as disposições constantes do edital e dos respectivos anexos. O certame deverá ser processado e julgado em conformidade com o Decreto Municipal nº 2.545/02, com a Lei Federal nº 10520, de 17 de Julho de 2002 e subsidiariamente com a Lei Federal nº 8666/93 e suas alterações e demais normas complementares e disposições deste instrumento.

Data da sessão: 06/11/2017
Horário: 9:00 horas
Local: Sala de Licitações

1. DO OBJETO

1.1 O objeto da presente licitação é a escolha da proposta mais vantajosa para a aquisição de LICENÇA PARA ANTIVIRUS, com finalidade de melhoria no desenvolvimento de ações nos diversos departamentos da Administração Municipal, atendendo à solicitação da Secretaria Municipal de Administração e Finanças, conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.

2. A LICITAÇÃO SERÁ MENOR PREÇO, CONFORME TERMO DE REFERÊNCIA

3. DOS RECURSOS ORÇAMENTÁRIOS

3.1 As despesas para atender a esta licitação estão programadas em dotação orçamentária própria, prevista no orçamento do Município de Pouso Alegre - MG para o exercício de 2017.

4. DO CREDENCIAMENTO

4.1 Todos os interessados do ramo de atividade pertinente ao objeto da contratação poderão participar deste certame, desde que preencham as condições de credenciamento constantes deste Edital:

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

b) tratando-se de procurador, a procuração por instrumento público ou particular, da qual constem poderes específicos para formular lances, negociar preço, interpor recursos e desistir de sua interposição e praticar todos os demais atos pertinentes ao certame, acompanhado do correspondente documento.

4.2 O representante legal ou o procurador deverão identificar-se exibindo documento oficial de identificação que contenha foto.

4.3 Será admitido apenas 01 (um) representante para cada licitante credenciada, sendo que cada um deles poderá representar apenas uma credenciada.

4.4 Se o licitante não credenciar um representante estará abdicando do direito de fazer lance e, principalmente, de recorrer dos atos do(a) Pregoeiro(a).

4.5 Para que sejam beneficiadas pela Lei Complementar nº 123/06, as microempresas e as empresas de pequeno porte deverão apresentar certidão expedida pela Junta Comercial do Estado onde fique demonstrada e comprovada sua atual condição de microempresa ou empresa de pequeno porte, conforme art.8º da Instrução Normativa nº 103/2007 do DNRC. A certidão deverá ser expedida em até 06 (seis) meses antes da data da abertura da licitação.

4.6 Os documentos apresentados através de cópia produzida por qualquer processo de reprodução deverão ser autenticados por cartório competente ou pela Comissão Permanente de Licitação mediante apresentação dos originais.

5. DA PARTICIPAÇÃO NO PREGÃO

5.1 Poderão participar deste Pregão os interessados pertencentes ao ramo de atividade relacionado ao objeto da licitação, conforme disposto nos respectivos atos constitutivos, que atenderem a todas as exigências, inclusive quanto à documentação, constantes deste Edital e seus Anexos.

5.2 Não poderão participar desta licitação os interessados:

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

5.2.2 Estrangeiros que não tenham representação legal no Brasil com poderes expressos para receber citação e responder administrativa ou judicialmente;

5.2.3 Que se enquadrem nas vedações previstas no artigo 9º da Lei nº 8.666, de 1993;

5.2.4 Que estejam sob falência, em recuperação judicial ou extrajudicial, concurso de credores, concordata ou insolvência, em processo de dissolução ou liquidação;

5.2.5 Entidades empresariais que estejam reunidas em consórcio;

5.3. Como condição para participação no Pregão, a licitante deverá firmar as seguintes declarações:

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

5.3.2 Que está ciente e concorda com as condições contidas no Edital e seus anexos, bem como de que cumpre plenamente os requisitos de habilitação definidos no Edital;

5.3.3 Que inexistem fatos impeditivos para sua habilitação no certame, ciente da obrigatoriedade de declarar ocorrências posteriores;

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

6. ENVIO DAS PROPOSTAS

6.1 As licitantes deverão apresentar suas propostas sem cotações alternativas, emendas, rasuras ou entrelinhas. Suas folhas devem estar rubricadas, numeradas e a última assinada pelo representante legal da empresa ou pela pessoa física participante, devendo nela constar:

a) identificação (individual ou social), a razão social, endereço, telefone/FAX, e-mail comercial se houver, número do CNPJ/MF, Banco, agência, número da conta corrente e praça de pagamento para facilitar o contato e o pagamento;

b) proposta definitiva de preços, especificando detalhadamente o item ofertado, discriminando, ainda, a marca dos produtos e o valor unitário e total, em moeda corrente nacional, sendo admitidas apenas duas casas após a vírgula;

c) a validade da proposta não poderá ser inferior a 60 (sessenta) dias, a contar da data da sessão de abertura desta licitação;

d) declaração expressa de que todos os tributos, custos e demais despesas correm por conta da proponente.

6.2 A proposta deverá atender todas as condições exigidas no Edital e nos Anexos. As licitantes poderão utilizar o Anexo I deste Edital para a formulação de sua proposta, complementando as informações, caso necessário.

6.3 A falta de data e/ou rubrica da proposta somente poderá ser suprida pelo representante legal presente na sessão de abertura do envelope de Proposta e com poderes para esse fim.

6.4 Em nenhuma hipótese poderá ser alterado o conteúdo da proposta apresentada, seja com relação a preço, pagamento, prazo ou qualquer condição que importe a modificação dos termos originais, ressalvadas apenas aquelas destinadas a sanar evidentes erros materiais, alterações essas que serão avaliadas pelo(a) Pregoeiro(a).

6.5 Caso o prazo estabelecido para validade da proposta não seja indicado na proposta, será considerado aceito pela licitante o prazo estabelecido neste edital para efeitos de julgamento.

6.6 Serão desclassificadas as propostas que não atenderem às exigências do presente Edital e seus Anexos sejam omissas ou apresentem irregularidades, ou defeitos capazes de dificultar o julgamento.

6.7 Fica reservado ao Município de Pouso Alegre - MG o direito de verificar, sempre que julgar necessário, se os preços praticados pela licitante vencedora estão compatíveis com os de mercado.

6.8 Todos os documentos que integram as propostas da licitante deverão estar embalados em envelopes lacrados, não transparentes e denominados:

Envelope nº. 01 "PROPOSTA COMERCIAL"

A Pregoeira da Prefeitura do Município de Pouso Alegre/MG
Pregão n.º 70/2017
Objeto: Registro de Preços – AQUISIÇÃO DE LICENÇA DE ANTIVIRUS PARA ATENDER AS NECESSIDADES DA PREFEITURA MUNICIPAL DE POUSO ALEGRE.
Licitante: .....

Envelope nº. 02 "DOCUMENTOS DE HABILITAÇÃO"

A Pregoeira da Prefeitura do Município de Pouso Alegre/MG
Pregão n.º 70/2017

Objeto: Registro de Preços – AQUISIÇÃO DE LICENÇA DE ANTIVIRUS PARA ATENDER AS NECESSIDADES DA PREFEITURA MUNICIPAL DE POUSO ALEGRE.
Licitante: .....

7. DAS PROPOSTAS E FORMULAÇÃO DE LANCES

7.1 A abertura da presente licitação dar-se-á em sessão pública, na data, horário e local indicados neste Edital.

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

7.2.1 A desclassificação será sempre fundamentada e registrada em ata.

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

7.3. As propostas serão classificadas, sendo que somente estas participarão da fase de lances.

7.4 Iniciada a etapa competitiva, os licitantes deverão formular lances, sendo imediatamente lançados na ata de registro.

7.4.1 O lance deverá ser ofertado pelo valor total do item.

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

7.6 O licitante somente poderá oferecer lance inferior ao último por ele ofertado e registrado em ata.

7.7 Não serão aceitos dois ou mais lances de mesmo valor.

7.8 A etapa de lances da sessão pública será encerrada por decisão do(a) Pregoeiro(a).

7.9 Caso o licitante não apresente lances, concorrerá com o valor de sua proposta e, na hipótese de desistência de apresentar outros lances, valerá o último lance por ele ofertado, para efeito de ordenação das propostas.

8. DA ACEITABILIDADE DA PROPOSTA VENCEDORA

8.1 Encerrada a etapa de lances, o(a) Pregoeiro(a) examinará a proposta classificada em primeiro lugar quanto ao preço, a sua exequibilidade, bem como quanto ao cumprimento das especificações do objeto.

8.2 Será desclassificada a proposta ou o lance vencedor com valor superior ao preço máximo fixado ou que apresentar preço manifestamente inexequível.

8.2.1 Considera-se inexequível a proposta que apresente preço por item, irrisórios ou de valor zero, incompatíveis com so preços dos insumos e salários de mercado, acrescidos dos respectivos encargos, ainda que o ato convocatório da licitação não tenha estabelecido limites mínimos, exceto quando se referirem a materiais e instalações de propriedade do próprio licitante, para os quais ele renuncie a parcela ou à totalidade da remuneração.

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

8.4 O(a) Pregoeiro(a0 poderá encaminhar contraproposta ao licitante que apresentou o lance mais vantajoso, com o fim de negociar a obtenção de melhor preço, vedada a negociação em condições diversas das previstas neste Edital.

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

8.5 A negociação será realizada de forma presencial.

9. DA HABILITAÇÃO

9.1 Como condição prévia ao exame da documentação de habilitação do licitante detentor da proposta classificada em primeiro lugar, o(a) Pregoeiro(a) verificará o eventual descumprimento das condições de participação, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, deverão apresentar a seguinte documentação relativa à Habilitação Jurídica, Regularidade Fiscal e trabalhista:

9.2 Habilitação jurídica:

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

9.2.2 No caso de sociedade empresária ou empresa individual de responsabilidade limitada - EIRELI: ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado na Junta Comercial da respectiva sede, acompanhado de documento comprobatório de seus administradores;

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

9.2.4 No caso de microempresa ou empresa de pequeno porte: certidão expedida pela Junta Comercial ou pelo Registro Civil das Pessoas Jurídicas, conforme o caso, que comprove a condição de microempresa ou empresa de pequeno porte, nos termos do artigo 8° da Instrução Normativa n° 103, de 30/04/2007, do Departamento Nacional de Registro do Comércio - DNRC;

9.2.5 No caso de cooperativa: ata de fundação e estatuto social em vigor, com a ata da assembléia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, bem como o registro de que trata o art. 107 da Lei nº 5.764, de 1971;

9.2.6 Os documentos acima deverão estar acompanhados de todas as alterações ou da consolidação respectiva;

9.3 Regularidade fiscal e trabalhista:

9.3.1 prova de inscrição no Cadastro Nacional de Pessoas Jurídicas;

9.3.2 prova de regularidade com a Fazenda Nacional (certidão conjunta, emitida pela Secretaria da Receita Federal do Brasil e Procuradoria-Geral da Fazenda Nacional, quanto aos demais tributos federais e a Divida Ativa da União, por elas administrados, conforme art. 1º, inciso I, do Decreto nº 6.106/07);

9.3.3 prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

9.3.4 prova de regularidade com a fazenda Estadual e Municipal;

9.3.5 prova de inexistência de débitos inadimplidos perante a justiça do trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da consolidação das leis do trabalho, aprovada pelo decreto-lei nº 5.452, de 1º de maio de 1943;

9.4 As empresas deverão comprovar, ainda, a qualificação técnica, por meio de:

9.4.1 Certidão negativa de pedido de falência, recuperação judicial ou extrajudicial.

9.4.2 Atestado de Capacidade Técnica da empresa, fornecido por Pessoa Jurídica de Direito Público ou Privado, em papel timbrado, comprovando a execução dos serviços, compatíveis com a complexidade dos serviços a serem realizados no Município de Pouso Alegre

9.5 Os documentos exigidos para habilitação relacionados nos subitens acima, deverão ser apresentados pelos licitantes, após solicitação do(a) Pregoeiro(a).

9.5.1 Não serão aceitos documentos com indicação de CNPJ diferentes, salvo aqueles legalmente permitidos.

9.6 Havendo alguma restrição no que tange à regularidade fiscal, o licitante será convocado para, no prazo de 05 (cinco) dias úteis, após solicitação do(a) Pregoeiro(a), comprovar a regularização. O prazo poderá ser prorrogado por igual período.

9.6.1 A não regularização fiscal no prazo previsto no subitem anterior acarretará a inabilitação do licitante, sem prejuízo das sanções previstas neste Edital, sendo facultada a convocação dos licitantes remanescentes, na ordem de classificação, para os quais será concedido o mesmo prazo especial para a regularização da situação fiscal.

9.7 Havendo necessidade de analisar minuciosamente os documentos exigidos, o(a) Pregoeiro(a) suspenderá a sessão, informando a nova data e horário para a continuidade da mesma.

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

10. DO ENCAMINHAMENTO DA PROPOSTA VENCEDORA

10.1 A proposta final deverá ser documentada nos autos e será levada em consideração no decorrer da execução do contrato e aplicação de eventual sanção à Contratada, se for o caso.

10.2 Todas as especificações do objeto contidas na proposta, tais como marca, modelo, tipo, fabricante e procedência, vinculam a Contratada.

11. DOS RECURSOS

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

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

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

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

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

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

11.4 Os autos do processo permanecerão com vista franqueada aos interessados, no endereço constante neste Edital.

12. DA ADJUDICAÇÃO E HOMOLOGAÇÃO

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

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

13. DO TERMO DE CONTRATO OU INSTRUMENTO EQUIVALENTE

13.1 Após a homologação da licitação será firmado Termo de Contrato ou aceito instrumento equivalente (Nota de Empenho/Carta Contrato/Autorização). O prazo de vigência da contratação é de 12 (doze) meses, contados da data de homologação, prorrogável na forma do art. 57, § 1°, da Lei n° 8.666/93.

13.2 Previamente à contratação será realizada consulta aos órgãos fiscais, pela contratante, para identificar possível regularidade junto aos poderes públicos.

13.2.1 O adjudicatário terá o prazo de 05 (cinco) dias úteis, contados a partir da data de sua convocação, para assinar o Termo de Contrato ou aceitar o instrumento equivalente, conforme o caso, sob pena de decair do direito à contratação, sem prejuízo das sanções previstas neste Edital.

13.2.2 Alternativamente à convocação para comparecer perante o órgão ou entidade para a assinatura do Termo de Contrato ou aceite do instrumento equivalente, a Administração

poderá encaminhá-lo para assinatura ou aceite do adjudicatário, mediante correspondência postal com aviso de recebimento (AR) ou meio eletrônico, para que seja assinado ou aceito no prazo de 05(cinco) dias, a contar da data de seu recebimento.

13.3 O prazo previsto no subitem anterior poderá ser prorrogado, por igual período, por solicitação justificada do adjudicatário e aceita pela Administração.

13.4 Antes da assinatura do Termo de Contrato ou aceite do instrumento equivalente, a Administração realizará consulta nos cadastros fiscais, cujos resultados serão anexados aos autos do processo.

13.4.1 Na hipótese de irregularidade, o contratado deverá regularizar a sua situação perante o cadastro no prazo de até 05 (cinco) dias, sob pena de aplicação das penalidades previstas no edital e anexo.

13.5 Se o adjudicatário, no ato da assinatura do Termo de Contrato ou aceite do instrumento equivalente, não comprovar que mantém as mesmas condições de habilitação, ou quando, injustificadamente, recusar-se à assinatura ou aceite, poderá ser convocado outro licitante, desde que respeitada a ordem de classificação, para, após a verificação da aceitabilidade da proposta, negociação e comprovados os requisitos de habilitação, celebrar a contratação, sem prejuízo das sanções previstas neste Edital e das demais cominações legais.

14. DO PREÇO

14.1 Os preços são fixos e irreajustáveis.

15. DA ENTREGA E DO RECEBIMENTO DO OBJETO E DA FISCALIZAÇÃO

15.1 Os critérios de recebimento e aceitação do objeto e de fiscalização estão previstos no Termo de Referência.

16. DAS OBRIGAÇÕES DA CONTRATANTE E DA CONTRATADA

16.1 As obrigações da Contratante e da Contratada são as estabelecidas no Termo de Referência.

17. DO PAGAMENTO

17.1 O pagamento será realizado no prazo máximo de até 30 (trinta) dias, contados a partir da data final do período de adimplemento a que se referir, através de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo contratado.

17.2 Os pagamentos decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 24 da Lei 8.666, de 1993, deverão ser efetuados no prazo de até

05 (cinco) dias úteis, contados da data da apresentação da Nota Fiscal, nos termos do art. 5º, § 3º, da Lei nº 8.666, de 1993.

17.3 O pagamento somente será autorizado depois de efetuado o “atesto” pelo servidor competente na nota fiscal apresentada.

17.4 Havendo erro na apresentação da Nota Fiscal ou dos documentos pertinentes à contratação, ou, ainda, circunstância que impeça a liquidação da despesa, como, por exemplo, obrigação financeira pendente, decorrente de penalidade imposta ou inadimplência, o pagamento ficará sobrestado até que a Contratada providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para a Contratante.

17.5 Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

17.6 Antes de cada pagamento à contratada será realizada consulta aos órgãos fiscais para verificar a manutenção das condições de habilitação exigidas no edital.

17.7 Constatando-se, a situação de irregularidade da contratada, será providenciada sua advertência, por escrito, para que, no prazo de 05 (cinco) dias, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da contratante.

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

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

17.10 Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso a contratada não regularize sua situação junto aos órgãos fiscais.

17.11 Somente por motivo de economicidade, segurança nacional ou outro interesse público de alta relevância, devidamente justificado, em qualquer caso, pela máxima autoridade da contratante, não será rescindido o contrato em execução com a contratada inadimplente nos órgãos.

17.12 Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

17.12.1 A Contratada regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

18. DAS SANÇÕES ADMINISTRATIVAS

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

18.1.1 Não aceitar/retirar a nota de empenho, ou não assinar o termo de contrato, quando convocado dentro do prazo de validade da proposta;

18.1.2 Apresentar documentação falsa;

18.1.3 Deixar de entregar os documentos exigidos no certame;

18.1.4 Ensejar o retardamento da execução do objeto;

18.1.5 Não mantiver a proposta

18.1.6 Cometer fraude fiscal;

18.1.7 Comportar-se de modo inidôneo;

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

18.3 O licitante/adjudicatário que cometer qualquer das infrações discriminadas no subitem anterior ficará sujeito, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

18.3.1 Multa de 0,3% (zero vírgula três por cento), por dia de atraso na execução do objeto, ou por dia de atraso no cumprimento de obrigação contratual ou legal, até o 30º (trigésimo) dia, calculados sobre o valor do contrato, por ocorrência, sobre o valor estimado do(s) item(s) prejudicado(s) pela conduta do licitante;

18.3.2 Multa de 10% (dez por cento) sobre o valor do contrato, no caso de atraso superior a 30 (trinta) dias na execução do objeto ou no cumprimento de obrigação contratual ou legal, que poderá ser aplicado com rescisão contratual;

18.3.3 Multa de 20% (vinte por cento) sobre o valor contrato, na hipótese de o contratado, de modo injustificado, desistir do contrato ou der causa à sua rescisão, bem como nos demais casos de descumprimento contratual, quando o Município em face de menor gravidade do fato e mediante motivação da autoridade superior do Município, poderá reduzir o percentual da multa a ser aplicada.

18.3.4 Impedimento de licitar e de contratar com o Município, pelo prazo de até cinco anos;

18.4 A penalidade de multa pode ser aplicada cumulativamente com a sanção de impedimento.

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

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

18.7 As penalidades serão obrigatoriamente registradas, para conhecimento da Comissão de Licitação.

18.8 As sanções por atos praticados no decorrer da contratação estão previstas no Termo de Referência.

19. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

19.1 Qualquer pessoa, física ou jurídica, é parte legítima para solicitar esclarecimentos ou providências em relação ao presente **PREGÃO**, ou ainda, para impugnar este edital, desde que o faça com antecedência de até dois dias úteis da data fixada para recebimento das propostas, observado o disposto no § 2º do art. 41 da Lei Federal n.º 8.666/93 e suas alterações.

19.2 O(a) Pregoeiro(a) deverá decidir sobre a impugnação, se possível, antes da abertura do certame.

19.3 Quando o acolhimento da impugnação implicar em alteração do edital, capaz de afetar a formulação das propostas, será designado nova data para a realização deste **PREGÃO.**

19.4 A impugnação feita tempestivamente pela licitante, não a impedirá de participar deste **PREGÃO** até o trânsito em julgado da decisão

19.5 Acolhida à impugnação será definida e publicada nova data para a realização do certame.

19.6 Os pedidos de esclarecimentos referentes a este processo licitatório deverão ser enviados ao(a) Pregoeiro(a), até 03 (três) dias úteis anteriores à data designada para abertura da sessão pública, exclusivamente por meio eletrônico (e-mail) licitapamg@gmail.com ou cpd@pousoalegre.mg.com.br

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

19.8 As respostas às impugnações e os esclarecimentos prestados pelo(a) Pregoeiro(a) serão entranhados nos autos do processo licitatório e estarão disponíveis para consulta por qualquer interessado.

19.9. Não serão aceitas impugnações encaminhadas por e-mail.

20. DAS DISPOSIÇÕES GERAIS

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

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

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

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

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

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

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

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

20.9 O Edital está disponibilizado, na íntegra, no endereço eletrônico: www.pousoalegre.mg.gov.br na janela *"Licitações"* e também poderão ser lidos e/ou obtidos no endereço Rua Carijós, nº 45, Bairro Centro, Pouso Alegre - MG, nos dias úteis, no horário das 13h00min às 18h00min, mesmo endereço e período no qual os autos do processo administrativo permanecerão com vista franqueada aos interessados.

20.10. Nos casos omissos aplicar-se-ão as disposições constantes nos dispositivos legais: Lei nº 10.520, de 2002, Decreto 2.545 de 2002, Decreto nº 2.754 de 2005, Decreto nº 3.272 de 2009, Lei nº 8.078, de 1990 - Código de Defesa do Consumidor Lei Complementar nº 123 de 2006, e Lei nº 8.666 de 1993, subsidiariamente.

20.11. O foro para dirimir questões relativas ao presente Edital será o da Comarca de Pouso Alegre - MG, com exclusão de qualquer outro.

20.12 Integram este Edital, para todos os fins e efeitos, os seguintes anexos:

Constituem anexos deste edital:

ANEXO I – MODELO DE INSTRUMENTO DE CREDENCIAMENTO DE REPRESENTANTES
ANEXO II – TERMO DE REFERÊNCIA
ANEXO III - MODELO PADRÃO DE PROPOSTA COMERCIAL
ANEXO IV – MODELO DE DECLARAÇÃO
ANEXO V - MINUTA DO TERMO DE CONTRATO
ANEXO VI – MODELO DE DECLARAÇÃO DE EPP OU ME

Pouso Alegre/MG, 17 de novembro de 2017.

Daniela Luiza Zanatta
Pregoeira

ANEXO I

MODELO DE INSTRUMENTO DE CREDENCIAMENTO DE REPRESENTANTES

(A ser elaborado em papel timbrado da licitante)

Pelo presente instrumento, a empresa....., inscrita no CNPJ/MF sob o nº ....., com sede na ....., através de seu representante legal infra-assinado, **credencia** o Sr.(a) ....., portador(a) da Cédula de Identidade RG nº ..... e inscrito no CPF/MF sob o nº ....., outorgando-lhe plenos poderes para representá-la na sessão pública do **PREGÃO**, em especial para formular lances verbais e para interpor recursos ou deles desistir.

Por oportuno, a outorgante declara, sob as penas da lei, estar cumprindo plenamente os requisitos de habilitação, através dos documentos de habilitação, de acordo com as exigências constantes do Edital**.**

(nome completo, cargo ou função e assinatura do representante legal)

OBS.: APRESENTAR CÓPIA DO CONTRATO SOCIAL (AUTENTICADA) JUNTAMENTE COM ESTE CREDENCIAMENTO.

ANEXO II

TERMO DE REFERÊNCIA

1. DO OBJETO

A presente licitação tem como objeto aquisição de LICENÇA DE ANTIVIRUS, na modalidade Registro de Preços, para atender as necessidades da Prefeitura Municipal de Pouso Alegre - MG localizada a Rua Carijós, 45 Bairro Centro, n° 723, Pouso Alegre - MG CEP: 37.550-000, conforme especificado no ANEXO I (Termo de Referência) deste Edital.

Descrição	Quantidade
Software de Antivírus para Servidor e Desktops. O servidor deve ter capacidade de Gerenciar Remotamente através de Agentes de Software instalados nos Computadores Desktops	1000

Quantidade de desktops estimados no pertencentes ao Domínio: 970 computadores.

2-CONDIÇÕES DE ENTREGA OU FORNECIMENTO:

O prazo de entrega será de até 10 dias após a assinatura do contrato.

3. ESPECIFICAÇÕES TÉCNICA DO OBJETO

DA ESPECIFICAÇÃO DO ANTIVÍRUS

Servidor de Administração e Console Administrativa

3.1 Compatibilidade:

3.1.1 Microsoft Windows Server 2003 SP2 (todas edições);

3.1.2 Microsoft Windows Server 2003 x64 SP2 (todas edições);
3.1.3. Microsoft Windows Server 2008 (todas edições);
3.1.4 Microsoft Windows Server 2008 x64 SP1 (todas edições);

3.1.5 Microsoft Windows Server 2008 R2 (todas edições);

3.1.6 Microsoft Windows Server 2012 (todas edições);

3.1.7 Microsoft Windows Server 2012 R2 (todas edições);
3.1.8 Microsoft Windows Small Business Server 2003 SP2 (todas edições);

3.1.9 Microsoft Windows Small Business Server 2008 (todas edições);

3.1.10 Microsoft Windows Small Business Server 2011 (todas edições);

3.1.11 Microsoft Windows XP Professional SP2 ou superior;

3.1.12 Microsoft Windows XP Professional x64 SP2ou superior;

3.1.13 Microsoft Windows Vista Business / Enterprise / Ultimate SP1 ou posterior;

3.1.14 Microsoft Windows Vista Business / Enterprise / Ultimate SP1 x64 ou posterior;

3.1.15 Microsoft Windows 7 Professional / Enterprise / Ultimate;

3.1.16 Microsoft Windows 7 Professional / Enterprise / Ultimate x64;

3.1.17 Microsoft Windows 8 Professional / Enterprise;

3.1.18 Microsoft Windows 8 Professional / Enterprise x64;

3.1.19 Microsoft Windows 8.1 Professional / Enterprise;

3.1.20 Microsoft Windows 8.1 Professional / Enterprise x64.

3.2. Suporta as seguintes plataformas virtuais:

3.2.1 VMware: Workstation 9.x, Workstation 10.x, ESX 4.x, ESXi 4.x, ESXi 5.5, ESXi 6.0;

3.2.2 Microsoft Hyper-V: 2008, 2008 R2, 2012, 2012 R2;

3.2.3 KVM integrado com: RHEL 5.4 e 5.x acima, SLES 11 SPx, Ubuntu 10.10 LTS;
3.2.4 Microsoft VirtualPC 6.0.156.0;

3.2.5 Parallels Desktop 7 e superior;

3.2.6 Oracle VM VirtualBox 4.0.4-70112 (somente logon como convidado);

3.2.7 Citrix XenServer 6.1, 6.2.

3.3. Características:

3.3.1 A console deve ser acessada via WEB (HTTPS) ou MMC;

3.3.2 Console deve ser baseada no modelo cliente/servidor;

3.3.3 Compatibilidade com Windows Failover Clustering ou outra solução de alta disponibilidade;

3.3.4 Deve permitir a atribuição de perfis para os administradores da Solução de Antivírus;

3.3.5 Console deve ser totalmente integrada com suas funções e módulos caso haja a necessidade no futuro de adicionar novas tecnologias tais como, criptografia, Patch management e MDM;

3.3.6 As licenças deverão ser perpétuas, ou seja, expirado a validade da mesma o produto deverá permanecer funcional para a proteção contra códigos maliciosos utilizando as definições até o momento da expiração da licença;

3.3.7 Capacidade de remover remotamente e automaticamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores;

3.3.8 Capacidade de instalar remotamente a solução de antivírus nas estações e servidores Windows, através de compartilhamento administrativo, login script e/ou GPO de Active Directory;

3.3.9 Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria;

3.3.10 A solução de gerencia deve permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas;

3.3.11 Através da solução de gerência, deve ser possível verificar qual licença está aplicada para determinado computador;

3.3.12 Capacidade de instalar remotamente a solução de segurança em smartphones e tablets de sistema iOS, Android e Windows;

3.3.13 Capacidade de instalar remotamente qualquer “app” em smartphones e tablets de sistema iOS;

3.3.14 A solução de gerência centralizada deve permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle;

3.3.15 Deverá ter a capacidade de criar regras para limitar o tráfego de comunicação cliente/servidor por subredecom os seguintes parâmetros: KB/s e horário;

3.3.16 Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux e Mac) protegidos pela solução antivírus;

3.3.17 Capacidade de gerenciar smartphones e tablets(Windows Phone,Android e iOS) protegidos pela solução de segurança;

3.3.18 Capacidade de gerar pacotes customizados (auto executáveis) contendo a licença e configurações do produto;

3.3.19 Capacidade de atualizar os pacotes de instalação com as últimas vacinas;

3.3.20 Capacidade de fazer distribuição remota de qualquer software, ou seja, deve ser capaz de remotamente enviar qualquer software pela estrutura de gerenciamento de antivírus para que seja instalado nas máquinas clientes;

3.3.21 A comunicação entre o cliente e o servidor de administração deve ser criptografada;

3.3.22 Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes;

3.3.23 Deve permitir a realocação de máquinas novas na rede para um determinado grupo sem ter um agente ou endpoint instalado utilizando os seguintes parâmetros:

3.3.23.1 Nome do computador;
3.3.23.2 Nome do domínio;
3.3.23.3 Range de IP;
3.3.23.4 Sistema Operacional;
3.3.23.5 Máquina virtual.

3.3.24 Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas;

3.3.25 Deve permitir, por meio da console de gerenciamento, extrair um artefato em quarentena de um cliente sem a necessidade de um servidor ou console de quarentena adicional;

3.3.26 Capacidade de monitorar diferentes subnets de rede a fim de encontrar máquinas novas para serem adicionadas à proteção;

3.3.27 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;

3.3.28 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 antivírus automaticamente;

3.3.29 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 últimos02 dias, etc.;

3.3.30 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;

3.3.31 Deve fornecer as seguintes informações dos computadores:

3.3.31.1 Se o antivírus está instalado;
3.3.31.2 Se o antivírus está iniciado;
3.3.31.3 Se o antivírus está atualizado;
3.3.31.4 Minutos/horas desde a última conexão da máquina com o servidor administrativo;
3.3.31.5 Minutos/horas desde a última atualização de vacinas;
3.3.31.6 Data e horário da última verificação executada na máquina;
3.3.31.7 Versão do antivírus instalado na máquina;
3.3.31.8 Se for necessário reiniciar o computador para aplicar mudanças;
3.3.31.9 Data e horário de quando a máquina foi ligada;
3.3.31.10 Quantidade de vírus encontrados (contador) na máquina;
3.3.31.11 Nome do computador;
3.3.31.12 Domínio ou grupo de trabalho do computador;
3.3.31.13 Data e horário da última atualização de vacinas;
3.3.31.14 Sistema operacional com Service Pack;
3.3.31.15 Quantidade de processadores;
3.3.31.16 Quantidade de memória RAM;
3.3.31.17 Usuário(s) logado(s) naquele momento, com informações de contato (caso disponíveis no Active Directory);
3.3.31.18 Endereço IP;
3.3.31.19 Aplicativos instalados, inclusive aplicativos de terceiros, com histórico de instalação,
contendo data e hora que o software foi instalado ou removido;

3.3.31.20 Atualizações do Windows Updates instaladas;
3.3.31.21 Informação completa de hardware contendo: processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de áudio, adaptadores de rede, monitores, drives de CD/DVD;
3.3.31.22 Vulnerabilidades de aplicativos instalados na máquina;

3.3.32 Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterá-las;

3.3.33 Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como:

3.3.33.1 Alteração de Gateway Padrão;
3.3.33.2 Alteração de subrede;
3.3.33.3 Alteração de domínio;
3.3.33.4 Alteração de servidor DHCP;
3.3.33.5 Alteração de servidor DNS;
3.3.33.6 Alteração de servidor WINS;
3.3.33.7 Alteração desubrede;
3.3.33.8 Resolução de Nome;
3.3.33.9 Disponibilidade de endereço de conexão SSL;

3.3.34 Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet;

3.3.35 Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes;

3.3.36 Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus;
3.3.37 Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos;

3.3.38 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;

3.3.39 Capacidade de fazer deste repositório de vacinas um gateway para conexão com o servidor de administração, para que outras máquinas que não consigam conectar-se diretamente ao servidor possam usar este gateway para receber e enviar informações ao servidor administrativo;

3.3.40 Capacidade de exportar relatórios para os seguintes tipos de arquivos: PDF, HTML e XML;

3.3.41 Capacidade de gerar traps SNMP para monitoramento de eventos;

3.3.42 Capacidade de enviar e-mails para contas específicas em caso de algum evento;

3.3.43 Deve possuir compatibilidade com Microsoft NAP, quando instalado em um Windows 2008 Server;

3.3.44 Deve possuir compatibilidade com Cisco Network Admission Control (NAC);

3.3.45 Deve possuir documentação da estrutura do banco de dados para geração de relatórios a partir de ferramentas específicas de consulta (Crystal Reports, por exemplo).

3.3.46 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;

3.3.47 Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede
(baseado em quantidade de vírus encontrados em determinado intervalo de tempo);

3.3.48 Capacidade de realizar atualização incremental de vacinas nos computadores clientes;
3.3.49 Deve armazenar localmente e enviar ao servidor de gerência a ocorrência de vírus com os seguintes dados, no mínimo:

3.3.49.1 Nome do vírus;
3.3.49.2 Nome do arquivo infectado;
3.3.49.3 Data e hora da detecção;
3.3.49.4 Nome da máquina ou endereço IP;
3.3.49.5 Ação realizada.

3.3.50 Capacidade de reportar vulnerabilidades de softwares presentes nos computadores;

3.3.51 Capacidade de realizar inventário de hardware de todas as máquinas clientes;

3.3.52 Capacidade de realizar inventário de aplicativos de todas as máquinas clientes;

3.3.53 Capacidade de diferenciar máquinas virtuais de máquinas físicas.

Estações Windows

3.4 Compatibilidade:

3.4.1 Microsoft Windows Embedded 8.0 Standard x64;

3.4.2 Microsoft Windows Embedded 8.1 Industry Pro x64;

3.4.3 Microsoft Windows Embedded Standard 7* x86 / x64 SP1;

3.4.4 Microsoft Windows Embedded POSReady 7* x86 / x64;

3.4.5 Microsoft Windows XP Professional x86 SP3 e superior;

3.4.6 Microsoft Windows Vista x86 / x64SP2 e posterior;

3.4.7 Microsoft Windows 7 Professional/Enterprise/Ultimate x86 / x64 e posterior;

3.4.8 Microsoft Windows 8 Professional/Enterprise x86 / x64;

3.4.9 Microsoft Windows 8.1 Pro / Enterprise x86 / x64;

3.4.10 Microsoft Windows 10 Pro / Enterprise x86 / x64.

3.5 Características:

3.5.1. Deve prover as seguintes proteções:

3.5.1.1 Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
3.5.1.2 Antivírus de Web (módulo para verificação de sites e downloads contra vírus);
3.5.1.3 Antivírus de E-mail (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos);
3.5.1.4 Antivírus de Mensagens Instantâneas (módulo para verificação de mensagens instantâneas, como ICQ, MSN, IRC, etc);
3.5.1.5 O Endpoint deve possuir opção para rastreamento por linha de comando, parametrizável, com opção de limpeza;
3.5.1.6 Firewall com IDS;
3.5.1.7 Auto proteção (contra-ataques aos serviços/processos do antivírus);
3.5.1.8 Controle de dispositivos externos;
3.5.1.9 Controle de acesso a sites por categoria;

3.5.1.10 Controle de acesso a sites por horário;
3.5.1.11 Controle de acesso a sites por usuários;
3.5.1.12 Controle de execução de aplicativos;
3.5.1.13 Controle de vulnerabilidades do Windows e dos aplicativos instalados;

3.5.2 Capacidade de escolher quais módulos serão instalados, tanto na instalação local quanto na instalação remota;

3.5.3 As vacinas devem ser atualizadas pelo fabricante e disponibilizadas aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa);

3.5.4 Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;

3.5.5 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;

3.5.6 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;

3.5.7 Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks)
3.5.8 Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;

3.5.9 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 tomar a partir da extensão do arquivo;

3.5.10 Capacidade de verificar somente arquivos novos e alterados;

3.5.11 Capacidade de verificar objetos usando heurística;

3.5.12 Capacidade de agendar uma pausa na verificação;

3.5.13 Deve permitir a filtragem de conteúdo de URL avançada efetuando a classificação dos sites em categorias;

3.5.14 Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;

3.5.15 O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

3.5.15.1 Perguntar o que fazer, ou;
3.5.15.2 Bloquear acesso ao objeto;
3.5.15.2.1 Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
3.5.15.2.2 Caso positivo de desinfecção:
3.5.15.2.2.1 Restaurar o objeto para uso;
3.5.15.2.3 Caso negativo de desinfecção:
3.5.15.2.3.1 Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);

3.5.16 Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;

3.5.17 Capacidade de verificar e-mails recebidos e enviados nos protocolos POP3, IMAP, NNTP, SMTP e MAPI, assim como conexões criptografadas (SSL) para POP3 e IMAP (SSL);

3.5.18 Capacidade de verificar tráfego de ICQ, MSN, AIM e IRC contra vírus e links phishings;

3.5.19 Capacidade de verificar links inseridos em e-mails contra phishings;

3.5.20 Capacidade de verificar tráfego nos browsers: Internet Explorer, Firefox e Opera;

3.5.21 Capacidade de verificação de corpo e anexos de e-mails usando heurística;

3.5.22 O antivírus de e-mail, ao encontrar um objeto potencialmente perigoso, deve:
3.5.22.1 Perguntar o que fazer, ou;
3.5.22.2 Bloquear o e-mail;
3.5.22.2.1 Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração preestabelecida pelo administrador);
3.5.22.2.2 Caso positivo de desinfecção:
3.5.22.2.2.1 Restaurar o e-mail para o usuário;
3.5.22.2.3. Caso negativo de desinfecção:
3.5.22.2.3.1 Mover para quarentena ou apagar o objeto (de acordo com a configuração pré-estabelecida pelo administrador);

3.5.23 Caso o e-mail conter código que parece ser, mas não é definitivamente malicioso, o mesmo deve ser mantido em quarentena;

3.5.24 Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados;

3.5.25 Capacidade de filtrar anexos de e-mail, apagando-os ou renomeando-os de acordo com a configuração feita pelo administrador;

3.5.26 Capacidade de verificação de tráfego HTTP e qualquer script do Windows Script Host
(JavaScript, Visual Basic Script, etc.), usando heurísticas;

3.5.27 Deve ter suporte total ao protocolo IPv6;

3.5.28 Capacidade de alterar as portas monitoradas pelos módulos de Web e e-mail;

3.5.29 Na verificação de tráfego web, caso encontrado código malicioso o programa deve:

3.5.29.1 Perguntar o que fazer, ou;
3.5.29.2 Bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio, ou;
3.5.29.3 Permitir acesso ao objeto;

3.5.30. O antivírus de web deve realizar a verificação de, no mínimo, duas maneiras diferentes, sob escolha do administrador:

3.5.30.1 Verificação on-the-fly, onde os dados são verificados enquanto são recebidos em tempo-real, ou
3.5.30.2 Verificação de buffer, onde os dados são recebidos e armazenados para posterior verificação;

3.5.31 Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus de web;

3.5.32 Deve possuir módulo que analise as ações de cada aplicação em execução no computador, gravando as ações executadas e comparando-as com sequências características de atividades perigosas. Tais registros de sequências devem ser atualizados juntamente com as vacinas;

3.5.33 Deve possuir módulo que analise cada macro de VBA executada, procurando por sinais de atividade maliciosa;

3.5.34 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;

3.5.35 Deve possuir módulo de bloqueio de Phishing, com atualizações incluídas nas vacinas, obtidas pelo Anti-PhishingWorkingGroup (http://www.antiphishing.org/);

3.5.36 Capacidade de distinguir diferentes subnets e conceder opção de ativar ou não o firewall para uma subnet específica;

3.5.37 Deve possuir módulo IDS (IntrusionDetection System) para proteção contra portscans e exploração de vulnerabilidades de softwares. A base de dados de análise deve ser atualizada juntamente com as vacinas;
3.5.38 O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:

3.5.38.1 Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;

3.5.38.2 Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.

3.5.39 Deve possuir módulo que habilite ou não o funcionamento dos seguintes dispositivos externos, no mínimo:

3.5.39.1 Discos de armazenamento locais;
3.5.39.2 Armazenamento removível;
3.5.39.3 Impressoras;
3.5.39.4 CD/DVD;
3.5.39.5 Drives de disquete;
3.5.39.6 Modems;
3.5.39.7 Dispositivos de fita;
3.5.39.8 Dispositivos multifuncionais;
3.5.39.9 Leitores de smartcard;
3.5.39.10 Dispositivos de sincronização via ActiveSync (Windows CE, Windows Mobile, etc);
3.5.39.11 Wi-Fi;
3.5.39.12 Adaptadores de rede externos;
3.5.39.13 Dispositivos MP3 ou smartphones;
3.5.39.14 Dispositivo Bluetooth;
3.5.39.15 Câmeras e Scanners.

3.5.40 Capacidade de liberar acesso a um dispositivo e usuários por um período de tempo específico, sem a necessidade de desabilitar a proteção e o gerenciamento central ou de intervenção local do administrador na máquina do usuário;

3.5.41 Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por usuário;

3.5.42 Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por agendamento;

3.5.43 Capacidade de configurar novos dispositivos por Class ID/Hardware ID;

3.5.44 Capacidade de limitar o acesso a sites da internet por categoria, por conteúdo (vídeo, áudio, etc.), com possibilidade de configuração por usuário ou grupos de usuários e agendamento;

3.5.45 Capacidade de limitar a execução de aplicativos por hash MD5, nome do arquivo, versão do arquivo, nome do aplicativo, versão do aplicativo, fabricante/desenvolvedor, categoria (ex: navegadores, gerenciador de download, jogos, aplicação de acesso remoto, etc);

3.5.46 Capacidade de bloquear execução de aplicativo que está em armazenamento externo;

3.5.47 Capacidade de limitar o acesso dos aplicativos a recursos do sistema, como chaves do registro e pastas/arquivos do sistema, por categoria, fabricante ou nível de confiança do aplicativo;

3.5.48 Capacidade de, em caso de epidemia, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web;

3.5.49 Capacidade de, caso o computador cliente saia da rede corporativa, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web.
Estações Mac OS X

3.6 Compatibilidade:

3.6.1 Mac OS X 10.11 (El Capitan);

3.6.2 Mac OS X 10.10 (Yosemite);

3.6.3 Mac OS X 10.9 (Mavericks).

3.6.4 Mac OS X 10.8 (Mountain Lion)

3.6.5 Mac OS X 10.7 (Lion)

3.7 Características:

3.7.1 Deve prover proteção residente para arquivos (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;

3.7.2 Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;

3.7.3 A instalação e primeira execução do produto devem ser feita sem necessidade de reinicializarão do computador, de modo que o produto funcione com toda sua capacidade;

3.7.4 Deve possuir suportes a notificações utilizando o Growl;

3.7.5 As vacinas devem ser atualizadas pelo fabricante e disponibilizadas aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças

3.7.6 Capacidade de voltar para a base de dados de vacina anterior;

3.7.7 Capacidade de varrer a quarentena automaticamente após cada atualização de vacinas;

3.7.8 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;

3.7.9 Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);

3.7.10 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 tomar a partir da extensão do arquivo;

3.7.11 Capacidade de verificar somente arquivos novos e alterados;

3.7.12 Capacidade de verificar objetos usando heurística;

3.7.13 Capacidade de agendar uma pausa na verificação;

3.7.14 O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

3.7.14.1 Perguntar o que fazer, ou;
3.7.14.2 Bloquear acesso ao objeto;
3.7.14.2.1 Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração preestabelecida pelo administrador);
3.7.14.2.2 Caso positivo de desinfecção:
3.7.14.2.2.1 Restaurar o objeto para uso;
3.7.14.2.3 Caso negativo de desinfecção:
3.7.14.2.3.1 Mover para quarentena ou apagar (de acordo com a configuração preestabelecida pelo administrador);

3.7.15 Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
3.7.16 Capacidade de verificar arquivos de formato de email;

3.7.17 Possibilidade de trabalhar com o produto pela linha de comando, com no mínimo opções para atualizar as vacinas, iniciar uma varredura, para o antivírus e iniciar o antivírus pela linha de comando;

3.7.18 Capacidade de ser instalado, removido e administrado pela mesma console central de gerenciamento.
Estações de trabalho Linux

3.8 Compatibilidade:

3.8.1. Plataforma 32-bits:

3.8.1.1 Canaima 3;
3.8.1.2 RedFlag Desktop 6.0 SP2;
3.8.1.3 Red Hat Enterprise Linux 5.8 Desktop;
3.8.1.4 Red Hat Enterprise Linux 6.2 Desktop;
3.8.1.5 Fedora 16;
3.8.1.6 CentOS-6.2;
3.8.1.7 SUSE Linux Enterprise Desktop 10 SP4;
3.8.1.8 SUSE Linux Enterprise Desktop 11 SP2;
3.8.1.9 openSUSE Linux 12.1;
3.8.1.10 openSUSE Linux 12.2;
3.8.1.11 Debian GNU/Linux 6.0.5;
3.8.1.12 Mandriva Linux 2011;
3.8.1.13 Ubuntu 10.04 LTS;

3.8.1.14 Ubuntu 12.04 LTS.

3.8.2 Plataforma 64-bits:

3.8.2.1 Canaima 3;
3.8.2.2 RedFlag Desktop 6.0 SP2;
3.8.2.3 Red Hat Enterprise Linux 5.8;
3.8.2.4 Red Hat Enterprise Linux 6.2 Desktop;
3.8.2.5 Fedora 16;
3.8.2.6 CentOS-6.2;
3.8.2.7 SUSE Linux Enterprise Desktop 10 SP4;
3.8.2.8 SUSE Linux Enterprise Desktop 11 SP2;
3.8.2.9 openSUSE Linux 12.1;
3.8.2.10 openSUSE Linux 12.2;
3.8.2.11 Debian GNU/Linux 6.0.5;
3.8.2.12 Ubuntu 10.04 LTS;
3.8.2.13 Ubuntu 12.04 LTS.

3.9 Características:

3.9.1 Deve prover as seguintes proteções:

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

3.9.2 Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
3.9.2.1 Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
3.9.2.2 Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;
3.9.2.3 Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;
3.9.2.4 Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados.

3.9.3 Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares;

3.9.4 Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;

3.9.5 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 tomar a partir da extensão do arquivo;

3.9.6 Capacidade de verificar objetos usando heurística;

3.9.7 Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;

3.9.8 Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;

3.9.9 Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin
(ferramenta nativa GNU-Linux).
Servidores Windows

3.10 Compatibilidade:

3.10.1. Plataforma 32-bits:

3.10.1.1 Microsoft Windows Server 2003 Standard / Enterprise (SP2);
3.10.1.2 Microsoft Windows Server 2003 R2 Standard / Enterprise (SP2);
3.10.1.3 Microsoft Windows Server 2008 Standard / Enterprise / DataCenter (SP1 ou posterior);
3.10.1.4 Microsoft Windows Server 2008 Core Standard / Enterprise / DataCenter (SP1 ou posterior).

3.11 Compatibilidade

3.11.1. Plataforma 64-bits:

3.11.1.1 Microsoft Windows Server 2003 Standard / Enterprise (SP2);
3.11.1.2 Microsoft Windows Server 2003 R2 Standard / Enterprise (SP2);
3.11.1.3 Microsoft Windows Server 2008 Standard / Enterprise / DataCenter (SP1 ou posterior);
3.11.1.4 Microsoft Windows Server 2008 Core Standard / Enterprise / DataCenter (SP1 ou posterior);
3.11.1.5 Microsoft Windows Server 2008 R2 Standard / Enterprise / DataCenter (SP1 ou posterior);

3.11.1.6 Microsoft Windows Server 2008 R2 Core Standard / Enterprise / DataCenter (SP1 ou posterior);
3.11.1.7 Microsoft Windows Storage Server 2008 R2;
3.11.1.8 Microsoft Windows Hyper-V Server 2008 R2 (SP1 ou posterior);
3.11.1.9 Microsoft Windows Server 2012 Essentials / Standard / Foundation / Datacenter;
3.11.1.10 Microsoft Windows Server 2012 R2 Essentials / Standard / Foundation / Datacenter;
3.11.1.11 Microsoft Windows Server 2012 Core Essentials / Standard / Foundation / Datacenter;
3.11.1.12 Microsoft Windows Server 2012 R2 Core Essentials / Standard / Foundation /Datacenter;
3.11.1.13 Microsoft Windows Storage Server 2012 (todas as edições);
3.11.1.14 Microsoft Windows Storage Server 2012 R2 (todas as edições);
3.11.1.15 Microsoft Windows Hyper-V Server 2012;
3.11.1.16 Microsoft Windows Hyper-V Server 2012 R2.

3.12 Características:

3.12.1 Deve prover as seguintes proteções:

3.12.1.1 Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
3.12.1.2 Auto-proteção contra-ataques aos serviços/processos do antivírus;
3.12.1.3 Firewall com IDS;
3.12.1.4 Controle de vulnerabilidades do Windows e dos aplicativos instalados;

3.12.2 Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;

3.12.3 As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;

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

3.12.4.1 Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
3.12.4.2 Gerenciamento de tarefa (criar ou excluir tarefas de verificação);
3.12.4.3 Leitura de configurações;
3.12.4.4 Modificação de configurações;
3.12.4.5 Gerenciamento de Backup e Quarentena;
3.12.4.6 Visualização de relatórios;

3.12.4.7 Gerenciamento de relatórios;
3.12.4.8 Gerenciamento de chaves de licença;
3.12.4.9 Gerenciamento de permissões (adicionar/excluir permissões acima);

3.12.5 O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:

3.12.5.1 Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;
3.12.5.2 Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.

3.12.6 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;

3.12.7 Capacidade de resumir automaticamente tarefas de verificação que tenham sido paradas por anormalidades (queda de energia, erros, etc);

3.12.8 Capacidade de automaticamente pausar e não iniciar tarefas agendadas caso o servidor esteja em rodando com fonte ininterrupta de energia (uninterruptible Power supply – UPS);

3.12.9 Em caso de erros, deve ter capacidade de criar logs e traces automaticamente, sem necessidade de outros softwares;

3.12.10 Capacidade de configurar níveis de verificação diferentes para cada pasta, grupo de pastas ou arquivos do servidor;

3.12.11 Capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado no servidor;

3.12.12 Capacidade de criar uma lista de máquina que nunca serão bloqueadas mesmo quando infectadas;

3.12.13 Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;

3.12.14 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;

3.12.15 Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;

3.12.16 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 tomar a partir da extensão do arquivo;

3.12.17 Capacidade de verificar somente arquivos novos e alterados;

3.12.18 Capacidade de escolher qual tipo de objeto composto será verificado (ex: arquivos comprimidos, arquivos auto descompressores, .PST, arquivos compactados por compactadores binários, etc.);

3.12.19 Capacidade de verificar objetos usando heurística;

3.12.20 Capacidade de configurar diferentes ações para diferentes tipos de ameaças;

3.12.21 Capacidade de agendar uma pausa na verificação;

3.12.22 Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;

3.12.23 O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

3.12.23.1 Perguntar o que fazer, ou;
3.12.23.2 Bloquear acesso ao objeto;
3.12.23.2.1 Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração preestabelecida pelo administrador);
3.12.23.2.2 Caso positivo de desinfecção:
3.12.23.2.2.1 Restaurar o objeto para uso;
3.12.23.2.3. Caso negativo de desinfecção:
3.12.23.2.3.1 Mover para quarentena ou apagar (de acordo com a configuração preestabelecida pelo administrador);

3.12.24 Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;

3.12.25 Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;

3.12.26 Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;

3.12.27 Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa. Servidores Linux

3.13 Compatibilidade:

3.13.1 Plataforma 32-bits:

3.13.1.1 Red Hat Enterprise Linux Server 5.x;
3.13.1.2 Red Hat® Enterprise Linux® Server 6.x (6.0 - 6.6);
3.13.1.3 CentOS 6.x (6.0 - 6.6);
3.13.1.4 SUSE® Linux Enterprise Server 11 SP3;
3.13.1.5 Ubuntu Server 12.04 LTS;
3.13.1.6 Ubuntu Server 14.04 LTS;
3.13.1.7 Ubuntu Server 14.10;
3.13.1.8 Oracle Linux 6.5;
3.13.1.9. Debian GNU/Linux 7.5, 7.6, 7.7;
3.13.1.10 openSUSE

3.13.2 Plataforma 64-bits:

3.13.3 Red Hat Enterprise Linux Server 5.x;

3.13.4 Red Hat Enterprise Linux Server 6.x (6.0 - 6.6);

3.13.5 Red Hat Enterprise Linux Server 7;

3.13.6 CentOS-6.x (6.0 - 6.6);

3.13.7 CentOS-7.0;

3.13.8 SUSE Linux Enterprise Server 11 SP3;

3.13.9 SUSE Linux Enterprise Server 12;

3.13.10 Novell Open Enterprise Server 11 SP1;

3.13.11 Novell Open Enterprise Server 11 SP2;

3.13.12 Ubuntu Server 12.04 LTS;

3.13.13 Ubuntu Server 14.04 LTS;

3.13.14 Ubuntu Server 14.10;

3.13.15 Oracle Linux 6.5;

3.13.16 Oracle Linux 7.0;

3.13.17 Debian GNU/Linux 7.5, 7.6, 7.7;
3.13.18 openSUSE®

3.14 Características:

3.14.1 Deve prover as seguintes proteções:

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

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

3.14.2.1 Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
3.14.2.2 Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;
3.14.2.3 Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;
3.14.2.4 Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados;

3.14.3 Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares;

3.14.4 Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;

3.14.5 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 tomar a partir da extensão do arquivo;

3.14.6 Capacidade de verificar objetos usando heurística;

3.14.7 Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;

3.14.8 Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;

3.14.9 Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).

Servidores Novell Netware,
Compatibilidade:

3.14.10 Novell Netware 5.x Support Pack 6 ou superior;

3.14.11 Novell Netware 6.0 Support Pack 3 ou superior;

3.14.12 Novell Netware 6.5 Support Pack 3ou superior.

3.15 Características:

3.15.1 Deve possuir proteção em tempo real para arquivos acessados, criados ou modificados;

3.15.2 Deve possuir verificação manual e agendada de acordo com a configuração do administrador;

3.15.3 Capacidade de realizar update de maneira automatica, via internet ou LAN;

3.15.4 Capacidade de fazer um rollback das vacinas;

3.15.5 Capacidade de mover arquivos suspeitos ou infectados para área de quarentena;

3.15.6 Capacidade de criar logs detalhados e salvar resultados das verificações agendadas;

3.15.7 Capacidade de salvar um backup de todos os objetos infectados e suspeitos tratados;

3.15.8 Capacidade de notificar o administrador de varreduras concluidas e sobre objetos maliciosos encontrados no servidor, utilizando a rede Novell ou e-mail.

3.16 Compatibilidade Smartphones e tablets:

3.16.1 Apple iOS 7.0 – 8.X;
3.16.2 Windows Phone 8.1;

3.16.3 Android OS 2.3 – 5.1.

3.17 Características:

3.17.1 Deve prover as seguintes proteções:

3.17.1.1 Proteção em tempo real do sistema de arquivos do dispositivo – interceptação e verificação de:

3.17.1.1.1 Todos os objetos transmitidos usando conexões wireless (porta de infravermelho, Bluetooth) e mensagens EMS, durante sincronismo com PC e ao realizar download usando o browser;

3.17.1.1.2 Arquivos abertos no smartphone;

3.17.1.1.3 Programas instalados usando a interface do smartphone

3.17.1.2 Verificação dos objetos na memória interna do smartphone e nos cartões de expansão sob demanda do usuário e de acordo com um agendamento;

3.17.2 Deverá isolar em área de quarentena os arquivos infectados;

3.17.3 Deverá atualizar as bases de vacinas de modo agendado;

3.17.4 Deverá bloquear spams de SMS através de Black lists;

3.17.5 Deverá ter função de bloqueio do aparelho caso o SIM CARD for trocado para outro não autorizado;

3.17.6 Capacidade de desativar por política:

3.17.6.1 Wi-fi;
3.17.6.2 Câmera;
3.17.6.3 Bluetooth.

3.17.7 Deverá ter função de limpeza de dados pessoais a distância, em caso de roubo, por exemplo;

3.17.8 Capacidade de requerer uma senha para desbloquear o dispositivo e personalizar a quantidade de caracteres para esta senha;

3.17.9 Deverá ter firewall pessoal (Android);

3.17.10 Capacidade de tirar fotos quando a senha for inserida incorretamente;

3.17.11 Possibilidade de instalação remota utilizando o Microsoft System Center Mobile Device

Manager 2008 SP1;

3.17.12 Capacidade de enviar comandos remotamente de:

3.17.12.1 Localizar;
3.17.12.2 Bloquear.

3.17.13 Capacidade de detectar Jailbreak em dispositivos iOS;

3.17.14 Capacidade de bloquear o acesso a site por categoria em dispositivos;

3.17.15 Capacidade de bloquear o acesso a sites phishing ou malicioso;

3.17.16 Capacidade de criar containers de aplicativos, separando dados corporativos de dados pessoais;

3.17.17 Capacidade de bloquear o dispositivo quando o cartão “SIM” for substituído;

3.17.18 Capacidade de configurar White e blacklist de aplicativos;

3.17.19 Capacidade de localizar o dispositivo quando necessário;

3.17.20 Permitir atualização das definições quando estiver em “roaming”;

3.17.21 Capacidade de selecionar endereço do servidor para buscar a definição de vírus;

3.17.22. Capacidade de enviar URL de instalação por e-mail;

3.17.23 Capacidade de fazer a instalação através de um link QRCode;

3.17.24 Capacidade de executar as seguintes ações caso a desinfecção falhe:

3.17.24.1 Deletar;
3.17.24.2 Ignorar;
3.17.24.3 Quarentenar;
3.17.24.4 Perguntar ao usuário.

3.18 Compatibilidade Gerenciamento de dispositivos móveis (MDM)

3.18.1 Dispositivos conectados através do Microsoft Exchange ActiveSync:

3.18.1.1 Apple iOS;
3.18.1.2 Windows Phone;
3.18.1.3 Android.

3.18.2 Dispositivos com suporte ao Apple PushNotification (APNs).

3.18.2.1 Apple iOS 5.0 ou superior.

3.19 Características:

3.19.1 Capacidade de aplicar políticas de ActiveSync através do servidor Microsoft Exchange;

3.19.2 Capacidade de ajustar as configurações de:
3.19.2.1 Sincronização de e-mail;
3.19.2.2 Uso de aplicativos;
3.19.2.3 Senha do usuário;
3.19.2.4 Criptografia de dados;
3.19.2.5 Conexão de mídia removível.

3.19.3 Capacidade de instalar certificados digitais em dispositivos móveis;

3.19.4 Capacidade de, remotamente, resetar a senha de dispositivos iOS;

3.19.5 Capacidade de, remotamente, apagar todos os dados de dispositivos iOS;

3.19.6 Capacidade de, remotamente, bloquear um dispositivo iOS.

Criptografia

3.20 Compatibilidade:

3.20.1 Microsoft Windows XP Professional SP3 ou superior;

3.20.2 Microsoft Windows Vista Business/Enterprise/Ultimate SP2;

3.20.3 Microsoft Windows Vista Business/Enterprise/Ultimate x64 SP2;
3.20.4 Microsoft Windows 7 Professional/Enterprise/Ultimate;

3.20.5 Microsoft Windows 7 Professional/Enterprise/Ultimate x64;

3.20.6 Microsoft Windows 8 Professional/Enterprise;

3.20.7 Microsoft Windows 8 Professional/Enterprise x64;

3.20.8 Microsoft Windows 8.1 Professional / Enterprise;

3.20.9 Microsoft Windows 8.1 Professional / Enterprise x64;

3.20.10 Microsoft Windows 10 Pro x86 / x64;

3.20.11 Microsoft Windows 10 Enterprise x86 /x64.

3.21. Características:

3.21.1 O acesso ao recurso criptografado (arquivo, pasta ou disco) deve ser garantido mesmo em caso o usuário tenha esquecido a senha, através de procedimentos de recuperação;

3.21.2 Utilizar, no mínimo, algoritmo AES com chave de 256 bits;

3.21.3 Capacidade de criptografar completamente o disco rígido da máquina, adicionando um ambiente de pré-boot para autenticação do usuário;

3.21.4 Capacidade de utilizar Single Sign-On para a autenticação de pré-boot;

3.21.5 Permitir criar vários usuários de autenticação pré-boot;

3.21.6 Capacidade de criar um usuário de autenticação pré-boot comum com uma senha igual para todas as máquinas a partir da console de gerenciamento;

3.21.7 Capacidade de criptografar drives removíveis de acordo com regra criada pelo administrador, com as opções:

3.21.7.1 Criptografar somente os arquivos novos que forem copiados para o disco removível, sem modificar os arquivos já existentes;

3.21.7.2 Criptografar todos os arquivos individualmente;

3.21.7.3 Criptografar o dispositivo inteiro, de maneira que não seja possível listar os arquivos e pastas armazenadas;

3.21.7.4 Criptografar o dispositivo em modo portátil, permitindo acessar os arquivos em máquinas de terceiros através de uma senha;

3.21.8 Capacidade de selecionar pastas e arquivos (por tipo, ou extensão) para serem criptografados automaticamente. Nesta modalidade, os arquivos devem estar acessíveis para todas as máquinas gerenciadas pela mesma console de maneira transparente para os usuários;

3.21.9 Capacidade de criar regras de exclusões para que certos arquivos ou pastas nunca sejam criptografados;

3.21.10 Capacidade de selecionar aplicações que podem ou não ter acesso aos arquivos criptografados;

3.21.11 Verifica compatibilidade de hardware antes de aplicar a criptografia;

3.21.12 Possibilita estabelecer parâmetros para a senha de criptografia;

3.21.13 Bloqueia o reuso de senhas;

3.21.14 Bloqueia a senha após um número de tentativas pré-estabelecidas;

3.21.15 Capacidade de permitir o usuário solicitar permissão a determinado arquivo criptografado para o administrador mediante templates customizados;

3.21.16 Permite criar exclusões para não criptografar determinados “discos rígidos” através de uma busca por nome do computador ou nome do dispositivo

3.21.17 Permite criptografar as seguintes pastas pré-definidas: “meus documentos”, “Favoritos”, “Desktop”, “Arquivos temporários” e “Arquivos do outlook”;

3.21.18 Permite utilizar variáveis de ambiente para criptografar pastas customizadas;

3.21.19 Capacidade de criptografar arquivos por grupos de extensão, tais como: Documentos do office, Document, arquivos de audio, etc;

3.21.20 Permite criar um grupo de extensões de arquivos a serem criptografados;

3.21.21 Capacidade de criar regra de criptografia para arquivos gerados por aplicações;

3.21.22 Permite criptografia de dispositivos móveis mesmo quando o endpoint não possuir comunicação com o console de gerenciamento.
Gerenciamento de Sistemas

3.22 Capacidade de criar imagens de sistema operacional remotamente e distribuir essas imagens para computadores gerenciados pela solução e para computadores bare-metal;

3.23 Capacidade de detectar softwares de terceiros vulneráveis, criando assim um relatório de softwares vulneráveis;

3.24 Capacidade de corrigir as vulnerabilidades de softwares, fazendo o download centralizado da correção ou atualização e aplicando essa correção ou atualização nas máquinas gerenciadas de maneira transparente para os usuários;

3.25 Possuir tecnologia de Controle de Admissão de Rede (NAC), com a possibilidade de criar regras de quais tipos de dispositivos podem ter acessos a recursos da rede;

3.26 Capacidade de gerenciar licenças de softwares de terceiros;

3.27 Capacidade de registrar mudanças de hardware nas máquinas gerenciadas;

3.28 Capacidade de gerenciar um inventário de hardware, com a possibilidade de cadastro de dispositivos (ex: router, switch, projetor, acessório, etc), informando data de compra, local onde se encontra servicetag, número de identificação e outros;

3.29 Possibilita fazer distribuição de software de forma manual e agendada;

3.30 Suporta modo de instalação silenciosa;

3.31 Suporte a pacotes MSI, exe, bat, cmd e outros padrões de arquivos executáveis;

3.32 Possibilita fazer a distribuição através de agentes de atualização;

3.33 Utiliza tecnologiamulticast para evitar tráfego na rede;

3.34 Possibilita criar um inventário centralizado de imagens;

3.35 Capacidade de atualizar o sistema operacional direto da imagem mantendo os dados do usuário;

3.36 Suporte a WakeOnLan para deploy de imagens;

3.37 Capacidade de atuar como servidor de atualização do Windows podendo fazer deploy de patches;

3.38 Suporta modo de teste, podendo atribuir alguns computadores para receberem as atualizações de forma automática para avaliação de alterações no comportamento;

3.39 Capacidade de gerar relatórios de vulnerabilidades e patches;

3.40 Possibilita criar exclusões para aplicação de patch por tipo de sistema operacional, Estação de trabalho e Servidor ou por grupo de administração;

3.41 Permite iniciar instalação de patch e correções de vulnerabilidades ao reiniciar ou desligar o computador;

3.42 Permite baixar atualizações para o computador sem efetuar a instalação

3.43 Permite o administrador instalar somente atualizações aprovadas, instalar todas as atualizações (exceto as bloqueadas) ou instalar todas as atualizações incluindo as bloqueadas;

3.44 Capacidade de instalar correções de vulnerabilidades de acordo com a severidade;

3.45 Permite selecionar produtos a serem atualizados pela console de gerenciamento;

3.46 Permite selecionar categorias de atualizações para serem baixadas e instaladas, tais como: atualizações de segurança, ferramentas, drivers, etc.

4 - LOCAL DE SERVIÇO:

Rua Carijós, 45 – Centro

5 - DOTAÇÃO ORÇAMENTÁRIA

No exercício de 2017, as despesas correrão à conta da dotação orçamentária:

n.º - 0208 04.122.0017.2066 33903900 – Ficha 495

Caso necessário, no exercício seguinte, as despesas correrão à conta de dotação orçamentária própria, consignada no respectivo Orçamento-Programa, ficando a Administração obrigada a apresentar, no início de cada exercício, a respectiva Nota de Empenho estimativa e, havendo necessidade, emitir Nota de Empenho complementar, respeitadas as mesmas classificações orçamentárias.

6- PAGAMENTO

O pagamento será efetuado em até 30 dias após emissão da nota fiscal, respeitando-se o prazo de tramitação do empenho.

7- CRITÉRIOS DE JULGAMENTO

Menor Preço

8- JUSTIFICATIVA

A aquisição deste software de Antivírus visa proteger nossa rede de computadores contra ameaças cibernéticas tais como vírus, malwares, spams, rootkits, hackers e outros. O software irá proteger todos os computadores e os servidores da Prefeitura Municipal de Pouso Alegre – MG.

A presente proposição de contratação tomou como base o princípio da teoria de livre mercado, no qual os fornecedores concorrem na busca de oferecer o menor preço, sem com isso, comprometer a qualidade, a confiabilidade, a continuidade de serviço. Tal princípio trará benefícios e economia substanciais ao serviço público, cujas políticas e diretrizes devem estar orientadas para garantir e maximizar a qualidade e a quantidade da prestação de seus serviços à população, ao menor preço possível.

_____

Leandro Gomes Silveira

Gerente de Tecnologia da Informação

Secretaria de Administração e Finanças

_____

Júlio Cesar da Silva Tavares

Secretário de Administração e Finanças

ANEXO III

MODELO PADRÃO DE PROPOSTA COMERCIAL

A empresa ....., estabelecida na ....., inscrita no CNPJ/MF sob o nº ....., propõe fornecer à Prefeitura do Município de Pouso Alegre, em estrito cumprimento ao quanto previsto no edital da licitação em epígrafe, os itens relacionados abaixo:

Descrição	Quantidade	Preço Unitário	Preço total
Software de Antivírus para Servidor e Desktops. O servidor deve ter capacidade de Gerenciar Remotamente através de Agentes de Software instalados nos Computadores Desktops	1000		

Validade da Proposta: 60 dias

Pouso Alegre/MG ....., de ..... de 2017.

(Nome e assinatura do representante legal da licitante)

Banco.....

Agencia.....

Conta Corrente.....

ANEXO IV

MODELO - DECLARAÇÃO

....., inscrita no CNPJ/MF o nº ....., por intermédio de seu representante legal, o(a) Sr.(a)....., portador(a) da Carteira de Identidade RG nº ..... e inscrito no CPF/MF sob o nº ....., DECLARA, para fins do disposto no inciso V do art. 27 da Lei Federal nº 8.666, de 21 de Outubro de 1.993, acrescido pela Lei nº 9.854, de 27 de outubro de 1.999, que não emprega menor de dezoito anos em trabalho noturno, perigoso ou insalubre e não emprega menor de dezesseis anos.

Ressalva: emprega menor, a partir de quatorze anos, na condição de aprendiz ( ).

.....

(local e data)

.....

(representante legal)

(Obs.: em caso afirmativo, assinalar a ressalva acima)

ANEXO V

MINUTA DO CONTRATO

TERMO DE CONTRATO N° XX/2017

PROCESSO DE COMPRA: 226/2017

PREGÃO Nº 70/2017

CONTRATANTE: PREFEITURA MUNICIPAL DE POUSO ALEGRE/MG

CONTRATADA:

Aos ..... dias do mês de ..... do ano de 2017 (dois mil e dezessete), nesta cidade de Pouso Alegre, Estado de Minas Gerais, as partes de um lado a **PREFEITURA MUNICIPAL DE POUSO ALEGRE/MG,** pessoa jurídica de direito público interno, sediada na Rua Carijós, nº 45, centro, cadastrada junto ao Cadastro Nacional de Pessoa Jurídica do Ministério da Fazenda (CNPJ/MF) sob nº ....., neste ato representado pelo Secretário Municipal de Administração e Finanças **Sr**....., brasileiro, casado, portador da Cédula de Identidade RG. nº ....., devidamente inscrito junto ao Cadastro de Pessoas Físicas do Ministério da Fazenda (CPF/MF) sob o nº ....., doravante denominados **CONTRATANTE,** e, de outro lado, a empresa **.....**, pessoa jurídica de direito privado, sediada na ....., no Município de ....., Estado de ....., cadastrada junto ao Cadastro Nacional de Pessoa Jurídica do Ministério da Fazenda - CNPJ/MF sob o nº ....., com Inscrição Estadual registrada sob nº ....., neste ato representada por ....., ..., ..., ..., portador da Cédula de Identidade RG nº ....., inscrita no Cadastro de Pessoas Físicas do Ministério da Fazenda - CPF/MF sob o nº ....., doravante denominada **CONTRATADA**, têm entre si justo e acordado celebrar o presente contrato, em face do resultado do **Pregão,** que se regerá pela Lei nº 8666, de 21 de junho de 1993, bem como o Edital referido, a proposta da **CONTRATADA**, e as cláusulas seguintes:

CLÁUSULA PRIMEIRA – OBJETO e PRAZOS

O objeto do presente contrato consiste na **AQUISIÇÃO DE LICENÇA DE ANTIVIRUS, PARA ATENDER AS NECESSIDADES DA PREFEITURA MUNICIPAL DE POUSO ALEGRE – MG,** de acordo com Termo de Referência e demais disposições constantes do edital e dos respectivos anexos.

A entrega do objeto será efetuada nos prazos e condições descritos no Termo de Referência.

A **CONTRATADA** somente entregará o objeto mediante a ordem de fornecimento emitido pela secretaria requisitante.

CLÁUSULA SEGUNDA - DOTAÇÃO ORÇAMENTÁRIA

2.1. No exercício de 2017, as despesas correrão à conta da seguinte dotação orçamentária: 02.08.04.122.0017.2066.3.3.90.39.00 – FICHA 495.

CLÁUSULA TERCEIRA - PRAZOS

3.1. O prazo de vigência, objeto deste contrato, será de 12 meses a contar da sua data de assinatura.

3.2. Quaisquer atrasos no cumprimento dos prazos estabelecidos no presente Termo de Contrato somente serão justificados, e não serão considerados como inadimplemento contratual, se provocados por atos ou fatos imprevisíveis não imputáveis à **CONTRATADA** e devidamente aceitos pela **CONTRATANTE**.

CLÁUSULA QUARTA – DO VALOR

4.1. O valor deste contrato é de R$ ..... (.....) .

CLÁUSULA QUINTA – DAS CONDIÇÕES DE PAGAMENTO

5.1. A **CONTRATANTE** efetuará o pagamento em até 30 (trinta) dias após a emissão das Notas Fiscais, obedecendo à tramitação interna dos empenhos e desde que atendidas às condições previstas neste edital e no Termo de Referência.

CLÁUSULA SEXTA - DO REAJUSTE

6.1. Os preços propostos serão fixos e irreajustáveis.

CLÁUSULA SÉTIMA - RESPONSABILIDADES DA CONTRATANTE

7.1. Cabe a **CONTRATANTE** efetuar os pagamentos devidos, na forma e condições ora estipuladas.

7.2. Prestar todos os esclarecimentos necessários para a entrega do objeto.

CLÁUSULA OITAVA - RESPONSABILIDADES DA CONTRATADA

8.1. **Entregar o objeto,** conforme solicitação da Secretaria requisitante, obedecendo aos critérios detalhados no Anexo II – Termo de Referência, em total conformidade com o Edital e seus Anexos.

8.2. Ficar responsável por qualquer erro na Proposta apresentada, obrigando-se a entregar o objeto conforme exigido no edital e em seus anexos.

8.3. Obriga-se a **CONTRATADA** a manter durante toda a execução da obrigação, em compatibilidade com as obrigações por ela assumidas, todas as condições de habilitação e qualificação exigidas na licitação.

8.4. Paralisar, por determinação do Município de Pouso Alegre/MG, a entrega do objeto que não esteja de acordo com edital e seus anexos.

8.5. Arcar com todas as despesas relativas ao seu ramo de atividade, e necessárias ao cumprimento do objeto e todos os tributos incidentes sobre o objeto do contrato, devendo efetuar os respectivos pagamentos na forma e nos prazos previstos em lei.

CLÁUSULA NONA – DAS PENALIDADES

9.1. São aplicáveis as sanções previstas no Capítulo IV da Lei Federal nº 8.666/93 na Lei Federal nº 10.520/02 e demais normas pertinentes.

9.2. Se a **CONTRATADA** não mantiver a proposta, comportar-se de modo inidôneo ou fizer declaração falsa, estará sujeita à pena de suspensão de seu direito de licitar e contratar com a Administração, pelo prazo de até 02 (dois) anos.

9.3. Salvo ocorrência de caso fortuito ou de força maior devidamente justificada, e comprovada, ao não cumprimento, por parte da **CONTRATADA**, das obrigações assumidas, ou a infringência de preceitos legais pertinentes, será aplicada, segundo a gravidade da falta, nos termos dos artigos 86 e 87 da Lei Federal nº 8.666/93 e suas alterações, as seguintes penalidades:

I - advertência, sempre que for constatada irregularidade de pouca gravidade, para a qual tenha a **CONTRATADA** concorrida diretamente, ocorrência que será registrada no Cadastro de Fornecedores da Prefeitura Municipal de Pouso Alegre/MG.

II – multa de 1% (um por cento) por dia de atraso na entrega do objeto, calculada sobre o valor da nota de empenho ou instrumento equivalente, até o 10º (décimo) dia, após o que, aplicar-se-á, multa prevista na alínea “III” desta cláusula.

III – multa de 30% (trinta por cento) sobre o valor da nota de empenho ou instrumento equivalente, na hipótese do não cumprimento de qualquer das obrigações assumidas.

IV – na hipótese de rescisão do instrumento equivalente ao contrato, além da aplicação da multa correspondente, aplicar-se-á suspensão ao direito de licitar com a Prefeitura de Pouso Alegre/MG, bem como o impedimento de com ela contratar, pelo prazo de 12 (doze) meses.

V – declaração de inidoneidade, quando a proponente vencedora deixar de cumprir com as obrigações assumidas, praticando falta grave, dolosa ou culposa.
Parágrafo Primeiro - As multas serão, após regular processo administrativo, cobradas administrativa ou judicialmente.

Parágrafo Segundo - As penalidades previstas nesta cláusula têm caráter de sanção administrativa, conseqüentemente a sua aplicação não exime a(s) proponente(s) vencedora(s) de reparar os eventuais prejuízos que seu ato venha a acarretar ao Município de Pouso Alegre/MG.

9.5. As sanções são independentes e a aplicação de uma não exclui a aplicação das outras.

CLÁUSULA DÉCIMA - DA RESCISÃO CONTRATUAL

10.1. Poderão ser motivo de rescisão contratual as hipóteses elencadas nos artigos 77 e 78 da Lei n 8.666/93.

10.2. Caso a **CONTRATANTE** não se utilize da prerrogativa de rescindir o contrato, o seu exclusivo critério, poderá suspender a sua execução e/ou sustar o pagamento das faturas, até que a **CONTRATADA** cumpra integralmente a condição contratual infringida, sem

prejuízo da incidência das sanções previstas no Edital, na Lei nº 10.520 de 17.07.02, no Código de Defesa do Consumidor (Lei n 8.078/90).

10.3. A rescisão poderá ser unilateral, amigável (resilição) ou judicial, nos termos e condições previstas no art. 79 da Lei n° 8.666/93.

10.4. A **CONTRATADA** reconhece os direitos do MUNICÍPIO nos casos de rescisão previstas nos artigos 77 a 80 da Lei nº 8.666/93.

CLÁUSULA DÉCIMA PRIMEIRA - TRANSMISSÃO DE DOCUMENTOS

11.1. A troca eventual de documentos e cartas entre a **CONTRATANTE** e a **CONTRATADA** será feita através de protocolo. Nenhuma outra forma será considerada como prova de execução de documentos ou cartas.

CLÁUSULA DÉCIMA SEGUNDA - ALTERAÇÃO

12.1. A alteração de qualquer das disposições estabelecidas neste Termo de Contrato somente se reputará válida se tomadas expressamente em Instrumento Aditivo, que ao presente se aderirá, passando a dele fazer parte.

CLÁUSULA DÉCIMA TERCEIRA - LEGISLAÇÃO APLICÁVEL

13.1. O presente Termo de Contrato rege-se pelas disposições expressas na Lei nº 8.666, de 21 de junho de 1993, Lei Federal nº 10.520/02 e pelos preceitos de direito público, aplicando-se, supletivamente, os princípios da Teoria Geral dos Contratos e as disposições de direito privado.

CLÁUSULA DÉCIMA QUARTA - CONDIÇÕES GERAIS

14.1. Todos os encargos sociais e trabalhistas, bem como tributos de qualquer espécie, que venham a ser devidos em decorrência do presente Termo de Contrato correrão por conta da **CONTRATADA**.

CLÁUSULA DÉCIMA QUINTA - DIREITO DAS PARTES

15.1. Os direitos das partes contraentes encontram-se inseridos na Lei nº 8.666, de 21/06/93 e Lei nº 8.078 - Código de Defesa do Consumidor, e supletivamente no Código Civil Brasileiro.

CLÁUSULA DÉCIMA SEXTA - FORO

16.1. Fica eleito o Foro da Comarca de Pouso Alegre/MG, como competente para dirimir quaisquer questões oriundas do presente Termo de Contrato;

16.2. E por estarem justos e contratados, assinam o presente, por si e seus sucessores, em 03 (três) vias iguais e rubricadas para todos os fins de direito, na presença das testemunhas abaixo arroladas.

Pouso Alegre/MG, ... de ..... de 2017.

SECRETÁRIO MUNICIPAL DE ADMINISTRAÇÃO E FINANÇAS
CONTRATANTE

EMPRESA CONTRATADA

ANEXO VI

DECLARAÇÃO DE MICROEMPRESA OU EMPRESA DE PEQUENO PORTE

DECLARO, sob as penas da lei, sem prejuízo das sanções e multas previstas neste ato convocatório, que a empresa

_____(denominação da pessoa jurídica), CNPJ nº _____é microempresa ou empresa de pequeno porte, nos termos do enquadramento previsto na Lei Complementar nº 123, de 14 de dezembro de 2006, cujos termos declaro conhecer na íntegra, estando apta, portanto, a exercer o direito de preferência como critério de desempate no procedimento licitatório do **Pregão.**

Pouso Alegre, xx de xxxxxxx de 2017.

_____

Assinatura do representante

Nome:

RG nº: