CÂMARA MUNICIPAL DE
SANTO ANDRÉ

CONTRATO Nº 26, DE 2020

CONTRATO PARA AQUISIÇÃO DE SOFTWARES, QUE ENTRE SI CELEBRAM A CÂMARA MUNICIPAL DE SANTO ANDRÉ E A EMPRESA BRASOFTWARE INFORMÁTICA LTDA

PREÂMBULO

Aos dezesseis dias do mês de novembro de 2020, a CÂMARA MUNICIPAL DE SANTO ANDRÉ, inscrita no CNPJ sob nº 43.307.008/0001-08, situada na Praça IV Centenário, 2, Centro, Santo André – SP, CEP 09040-905, doravante denominada "CONTRATANTE", neste ato representada por seu Presidente, Vereador Pedro Luiz Mattos Canhassi Botaro, portador da Cédula de Identidade R.G. nº 29.775.799-4, emitida pela Secretaria de Segurança Pública do Estado de São Paulo (SSP/SP), e do C.P.F./MF n.º 312.568.618-04, e a empresa BRASOFTWARE INFORMÁTICA LTDA, inscrita no CNPJ sob nº 57.142.978/0001-05, com sede na Rua Marina La Regina, 227 – 3º andar, salas 11 a 15, Centro – Poá/SP, CEP 08550-210, doravante denominada "CONTRATADA", representada pela Sra. Fernanda Esteves Simoni, portadora da Cédula de Identidade RG nº 43.444.082-6 emitida pela Secretaria de Segurança Pública do Estado de São Paulo (SSP/SP), e do CPF/MF nº 299.707.828-86, perante as testemunhas ao final firmadas, assinam o presente contrato, cuja celebração foi autorizada pelo despacho de fls. 460 e 461 do Processo Acessório Licitatório vinculado ao **Processo Administrativo Principal nº 6533/2019,** que se regerá pela Lei Federal 10.520/02 e subsidiariamente pela Lei Federal 8.666/93, atendidas as cláusulas e condições que se enunciam a seguir:

FUNDAMENTO DO CONTRATO

Este contrato decorre da autorização do Senhor Presidente da Câmara Municipal de Santo André ao homologar a licitação na modalidade PREGÃO, do tipo MENOR PREÇO POR ITEM, aberta sob nº 12/2020 consoante se verifica nos autos do Processo Administrativo CM nº 6533/2019.

ESPECIFICAÇÃO DO OBJETO E CONDIÇÕES DA EXECUÇÃO

I - OBJETO DO CONTRATO

1. O presente contrato tem como objeto a AQUISIÇÃO DE SOFTWARES, conforme especificação do Anexo I do Edital de Pregão que antecedeu a presente contratação.

2. Nos termos do art. 55, inciso XI, da Lei Federal nº 8.666/93, fazem parte integrante do presente contrato o edital, seus anexos e a proposta vencedora.

II - FORMA DE EXECUÇÃO

1. O objeto da licitação será executado de acordo com as normas, especificações e demais elementos técnicos fornecidos pela CONTRATANTE e em conformidade com a proposta apresentada pela CONTRATADA, os quais ficam fazendo parte integrante deste contrato, independentemente de transcrições.

III – EXIGÊNCIAS A SEREM OBSERVADAS - Na execução, a CONTRATADA deverá observar e cumprir as exigências seguintes:

a) Assumir integral responsabilidade pela boa e eficiente execução do objeto, de acordo com o estabelecido nas normas do Pregão que regeu a licitação, bem como pelos eventuais danos que possam ser provocados por seus empregados por ocasião do fornecimento;

b) Cumprir as normas de segurança do trabalho, devendo fornecer aos seus funcionários os equipamentos de proteção individual e exigir-lhes o uso.

c) Substituir, em até 24 (vinte e quatro) horas, a contar de notificação, formulada por escrito, todo produto que for rejeitado pela CONTRATANTE, sob pena de multa diária por dia de atraso sobre o valor da entrega, a partir da notificação.

c.1) Trocar, às suas expensas, os produtos que vierem a ser recusados, sendo que o ato de recebimento não importará aceitação.

d) Assumir inteira responsabilidade pela entrega que efetuar, de acordo com as especificações constantes no presente Edital e seus Anexos, bem como da respectiva proposta, obedecendo ao Código de Defesa do Consumidor e à legislação pertinente vigente, quanto às condições dos produtos entregues.

IV – RESPONSABILIDADES - A CONTRATADA será única responsável pelos encargos sociais, trabalhistas, previdenciários, fiscais e comerciais resultantes da execução do contrato, bem como por todas as despesas necessárias incluindo transporte, mão-de-obra e demais despesas indiretas.

V - PRAZOS

1. PRAZO DE ENTREGA: Até 15 (quinze) dias contados a partir da assinatura do contrato.

2. PRAZO DE VIGÊNCIA DO CONTRATO: O prazo de vigência será de 30 dias ou por perda de objeto, o que ocorrer primeiro.

3. PRAZO DE GARANTIA: Cada licença deverá possuir garantia e atualizações por, no mínimo 3 anos, e telefone e e-mail para suporte técnico, se necessário, a contar da data do seu recebimento.

3.1. Não haverá prazo para substituição de itens fora da especificação ou com eventuais defeitos devido às características do objeto deste ajuste.

VI – PREPOSTO E FISCAL

1. A CONTRATADA designa o Sr. Luiz Phelipe da Silva, a quem outorga poderes legais para representá-la na execução do contrato e que servirá ainda de elemento permanente de ligação com o Fiscal da CONTRATANTE, devendo atendê-lo em horário comercial, de segunda a sexta-feira, sem ônus adicional para o CONTRATANTE.

2. A CONTRATANTE designa o(a) Senhor(a) Diretor de Apoio Tecnológico para os itens 2, 3, 4 e 5, e o (a) Senhor(a) Gerente de Comunicações Institucionais para o item 1, como fiscais para representá-la na execução do presente contrato, garantindo a qualidade e a excelência do objeto contratado, fiscalização essa que, em nenhuma hipótese, eximirá nem reduzirá as responsabilidades legais e contratuais da CONTRATADA.

VII - PREÇOS E PAGAMENTO

1. Nos preços acham-se computados e diluídos todos os ônus decorrentes de despesas diretas e indiretas (mão-de-obra, encargos sociais e quaisquer outras despesas necessárias), mesmo que não tenham sido apontadas expressamente pela CONTRATANTE, desde que tenham relação com o objeto contratado.

2. O pagamento será efetuado até o 5º (quinto) dia útil após o recebimento do objeto, por meio de depósito em conta corrente, através de ordem bancária, após a apresentação da respectiva nota fiscal/fatura, devidamente discriminada e atestada pelos(as) fiscais designados(as) na cláusula VI, sub cláusula 2.

2.1. O não pagamento da nota fiscal/fatura, apresentada nas condições previstas, ensejará a incidência da necessária compensação financeira, a ser procedida nos termos da Lei Civil.

3. SUSTAÇÃO DE PAGAMENTO - Nenhum pagamento será efetuado à CONTRATADA enquanto pendente de liquidação de qualquer obrigação financeira que lhe for imposta, em virtude de penalidade ou inadimplência, a qual poderá ser compensada com o pagamento pendente, sem que isso gere direito a acréscimos de qualquer natureza.

4. REAJUSTES - Tendo em vista a periodicidade adotada, não haverá reajustamento do preço pactuado.

VIII – DO VALOR DO CONTRATO

1. O valor total deste contrato para cobrir as despesas é de R$ 292.262,91 (duzentos e noventa e dois mil duzentos e sessenta e dois reais e noventa e um centavos), distribuído da seguinte forma:

1.1. Item 1 – R$ 62.686,75 (sessenta e dois mil seiscentos e oitenta e seis reais e setenta e cinco centavos);

1.2. Item 2 – R$ 32.369,25 (trinta e dois mil trezentos e sessenta e nove reais e vinte e cinco centavos);

1.3. Item 3 – R$ 65.828,40 (sessenta e cinco mil oitocentos e vinte e oito reais e quarenta centavos);

1.4. Item 4 – R$ 59.754,40 (cinquenta e nove mil setecentos e cinquenta e quatro reais e quarenta centavos);

1.5. Item 5 – R$ 71.624,11 (setenta e um mil seiscentos e vinte e quatro reais e onze centavos).

IX – DA DESPESA

1. A despesa com este contrato, no corrente exercício, no montante de R$ 292.262,91 (duzentos e noventa e dois mil duzentos e sessenta e dois reais e noventa e um centavos), correrá à conta da Nota de Empenho nº 610/2020, de 13/11/2020, devidamente apropriada no elemento de despesa 1.000.3.3.90.40 – SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO E INFORMAÇÃO - PJ, vinculado à atividade 2002 – Manutenção das Atividades Legislativas, da vigente Lei Orçamentária Anual.

X – GARANTIA CONTRATUAL

1. GARANTIA - Como garantia pelo cumprimento deste contrato, a CONTRATADA forneceu à CONTRATANTE garantia no valor de R$ 14.613,14 (quatorze mil seiscentos e treze reais e quatorze centavos), correspondente a 5% (cinco por cento) do valor contratual, na modalidade seguro garantia, conforme § 1°, artigo 56 da Lei Federal 8.666/93.

2. A CONTRATADA obriga-se a substituir ou prorrogar o prazo de garantia oferecida, caso o mesmo venha a vencer no decorrer do cumprimento das obrigações ajustadas.

3. DEVOLUÇÃO DA GARANTIA - A garantia oferecida pela CONTRATADA ser-lhe-á restituída, mediante requerimento da mesma, após o total cumprimento das obrigações ajustadas, inclusive períodos de garantia.

XI – PENALIDADES - As penalidades estão previstas nas Leis Federais nº 8.666/93 e 10.520/02, e os procedimentos relativos à aplicação de multas e outras sanções decorrentes da inexecução total ou parcial do contrato, no âmbito da Câmara Municipal de Santo André, estão previstos no Ato nº 4, de 22 de março de 2005, Anexo II, do presente ajuste.

XII – RESCISÃO - Haverá rescisão contratual na ocorrência de qualquer dos motivos elencados no artigo 78, na forma estabelecida no artigo 79, com as consequências previstas no artigo 80, todos da Lei Federal n.º 8.666/93, sem prejuízo das sanções enumeradas no artigo 87.

XIII - DISPOSIÇÕES GERAIS

1. ACRÉSCIMOS OU SUPRESSÕES - A CONTRATADA ficará obrigada a aceitar, nas mesmas condições contratuais, acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato, obedecido ao disposto no § 1º do artigo 65 da Lei Federal nº 8.666/93.

2. MANTENÇA DAS CONDIÇÕES HABILITATÓRIAS - A CONTRATADA obriga-se a manter, durante toda a execução contratual, em compatibilidade com as obrigações por ela assumidas, as condições habilitatórias e de qualificação exigidas na respectiva licitação.

3. FORO - Fica eleito o Foro da Comarca de Santo André, com exclusão de qualquer outro, por mais privilegiado que seja, para dirimir qualquer questão oriunda da execução deste contrato.

4. PUBLICIDADE – A Administração efetivará a publicação resumida deste instrumento de contrato na imprensa oficial, nos termos do Art. 61, parágrafo único, da Lei nº 8.666/93.

E, para firmeza e validade do que aqui ficou estipulado, foi lavrado o presente contrato, em 3 (três) vias de igual teor, que, depois de lido e achado conforme, é assinado pelas partes contratantes e pelas testemunhas abaixo.

Câmara Municipal de Santo André, 16 de novembro de 2020, 467º ano da fundação da cidade.

PEDRO LUIZ MATTOS CANHASSI BOTARO - Presidente	**FERNANDA ESTEVES SIMONI**
p/ Contratante	**p/ Contratada**

Testemunha 1:	**Testemunha 2:**
Nome: _____	Nome: _____
RG nº: _____	RG nº: _____
Ass.: _____	Ass.: _____

CÂMARA MUNICIPAL DE
SANTO ANDRÉ

ANEXO I

TERMO DE REFERÊNCIA

1. Objeto: Aquisição de Softwares, a seguir, especificados.

1.1. Os softwares solicitados deverão estar disponíveis para download, pelo período da vigência do contrato inicial de 12 meses, com possibilidade de prorrogação até 48 meses.

Operacionalização: Após a assinatura do contrato, as licenças de cada software deverão ser entregue através dos e-mail: dti@Câmarandre.sp.gov.br e informática@Câmarandre.sp.gov.br, em até 15 (quinze) dias corridos.

1.2. A licitante declarada vencedora deverá fornecer os produtos em conformidade com as especificações técnicas constantes neste Termo de Referência, bem como estar de acordo com todas as cláusulas editalícias;

1.3. Caso não possa ser oferecido produto com as mesmas especificações deste Termo, por motivo de atualização tecnológica ou alterações nos modelos fabricados pelo Fabricante, esta Casa se reserva o direito de suspender esta Licitação, para fins de adequação do objeto.

2. DAS ESPECIFICAÇÕES:

2.1. Pacote ADOBE Creative Cloud With Stock

O presente termo tem como objeto: Contratação de 2 licenças de uso do **pacote ADOBE Creative Cloud with Stock**, onde necessariamente precisa conter as ferramentas abaixo, entre as demais que o pacote contempla:
a) Aplicativo profissional para edição de fotografias e imagens diversas;
b) Aplicativo gráfico profissional para produção de desenhos;
c) Aplicativo profissional para diagramação e produção de layout;
d) Aplicativo profissional para organização, catalogação, armazenamento e busca de fotos digitais;
e) Aplicativo profissional para criação de arquivos PDF (Portable Document Format);
f) **Banco de Imagens.**

2.2. Pacote ADOBE Creative Cloud

O presente termo tem como objeto: Contratação de 1 licenças de uso do **pacote ADOBE Creative Cloud**, onde necessariamente precisa conter as ferramentas abaixo, entre as demais que o pacote contempla:
a) Aplicativo profissional para edição de fotografias e imagens diversas;
b) Aplicativo gráfico profissional para produção de desenhos;
c) Aplicativo profissional para diagramação e produção de layout;
d) Aplicativo profissional para organização, catalogação, armazenamento e busca de fotos digitais;
e) Aplicativo profissional para criação de arquivos PDF (Portable Document Format);

2.2.1 Em virtude de a CÂMARA dispor do **Software Adobe Collection CS6**, em alguns departamentos, destacamos os seguintes pontos:
a) Para seguir o padrão já existente dos arquivos criados, dentro de alguns departamentos da CÂMARA, onde temos instalado o **Pacote ADOBE Master Collection CS6**, que hoje contempla todas as ferramentas que estes departamentos necessitam para exercer os trabalhos exigidos por estas áreas.
Não temos como cotar um produto que não seja equivalente aos documentos já elaborados por esta ferramenta, por motivo de incompatibilidade.

b) Necessidade de adotar a padronização dos trabalhos já realizados com estas ferramentas e que já são utilizados pelos diversos departamentos da CÂMARA e produzidos em Gráfica

c) Integrar as soluções propostas neste documento com o ambiente em produção da CÂMARA;

d) Preservar os investimentos realizados no passado com cursos e produtos da ADOBE;

e) Utilizar o "know how" (conhecimento prático) adquirido pelos profissionais (técnicos e usuários) em produtos ADOBE.

f) Integração total com o ambiente Windows e trabalhos já realizados no passado e atualmente. Isso significa que as principais funcionalidades são estabelecidas nativamente, dispensando pesadas configurações e sendo, em sua maioria, transparentes para os usuários. Essa integração nativa, significa menores custos de implementação e, por não envolver outras soluções de contorno, menores custos com o suporte ao longo do tempo.

2.2.2 Os softwares não poderão ter sua vigência inferior a 3 (três) anos.

2.3. Software para acesso Remoto

Visa o atendimento e suporte ao usuário remotamente, inclusive porque temos áreas da Câmara que não estão dentro do prédio e também usuários que prestam serviço de tele trabalho., software de acesso remoto e suporte via internet, conforme as especificações e detalhamentos:

2.3.1. O software a ser contratado deverá ter a licença por subscrição de 12 meses (totalizando o prazo de 36 meses), garantindo o direito de uso da subscrição, sem qualquer custo adicional, devendo ser entregue em sua versão mais recente.

2.3.2. Software de acesso remoto deve dar suporte via internet para as plataformas Windows, Linux e Mac;

2.3.3. Apresentar uma solução livre de configurações na infraestrutura de rede da Contratante, isto é, configurações de roteamento, NAT;

2.3.4. O software deverá gerar um código e uma senha aleatórios para efetivar a conexão, sendo que a cada execução do software a senha deverá ser alterada;

2.3.5. Fornece suporte ad-hoc sem a obrigatoriedade de instalação nos computadores; Pregão nº 12/2020 20

2.3.6. Acesso à área de trabalho do computador destino permitindo o acesso a qualquer dado na máquina destino;

2.3.7. Proteger o acesso através de conexões criptografadas, bloqueando os acessos não autorizados, sempre por conexões seguras e protegidas por senha;

2.3.8. A solução deve possibilitar a transferência de arquivos entre os computadores, sem a necessidade de configurações extra;

2.3.9. A solução deve informar aos envolvidos o momento de abertura e finalização da sessão; Permitir o acesso remoto sem a necessidade de criação de conta e gerenciamento dos contatos.

2.3.10 – A solução devera permitir até 3 conexões simultâneas;

2.4. Licença Microsoft Office 365 E1

Para seguir o padrão já existente dentro da **CÂMARA**, onde todos os nossos equipamentos são da plataforma Microsoft, bem como o pacote Office; desta forma, não temos como cotar um produto que não seja equivalente aos documentos elaborados nesta Casa.
O presente termo tem como objeto: Contratação de licenças de uso de softwares Microsoft, para atualização tecnológica da plataforma de ferramentas de apoio ao escritório por meio dos serviços de Office 365, com suporte e garantia.

Em virtude de a CÂMARA dispor da Plataforma Microsoft nas estações de trabalho e servidores com sistemas operacionais Windows e aplicativos de escritórios - Pacotes Office, destacam-se os seguintes motivos que ratificam esta aquisição:

a. Adotar a padronização da plataforma de software com vistas a manter a compatibilidade com os produtos Microsoft que já se encontram em operação;

b. Integrar as soluções propostas neste documento com o ambiente em produção da CÂMARA;

c. Preservar os investimentos realizados no passado com cursos e produtos da Microsoft;

d. Utilizar o "know how" (conhecimento prático) adquirido pelos profissionais (técnicos e usuários) em produtos Microsoft.

e. Integração total com o ambiente Windows. Isso significa que as principais funcionalidades são estabelecidas nativamente, dispensando pesadas configurações e sendo, em sua maioria, transparentes para os usuários.
Essa integração nativa significa menores custos de implementação e, por não envolver outras soluções de contorno, menores custos com o suporte ao longo do tempo.

Considerando o modelo de licenciamento do software na modalidade como serviço em nuvem, uma de suas principais características é a flexibilização nos quantitativos de assinaturas.

Especificações

a- Licença de software de serviços de comunicação e colaboração online com hospedagem em nuvem
conta de e-mail com capacidade de armazenamento de pelo menos 50 gbytes;
b- Capacidade de envio de mensagens instantâneas;
c- Funcionalidade de bate-papo por texto, voz e vídeo;
d- Funcionalidade de pesquisa da caixa de email;
e- Capacidade de compartilhamento de contatos entre usuários;
f- Acesso e compartilhamento de documentos do texto, planilha eletrônica e apresentação armazenados na nuvem com gerenciamento de permissões de compartilhamento, definidos pelo usuário proprietário do documento, permitindo a edição simultânea e a recuperação de versões anteriores. o ambiente deve ter uma ferramenta de busca de informação.
g- Deve possibilitar a criação e edição de arquivos em formatos word, excel, powerpoint, em um navegador internet;
h- Unidade de disco virtual na nuvem com capacidade mínima de 25 gbytes não compartilhado com o correio eletrônico. a solução deve permitir a instalação de agente no computador que permita o acesso aos arquivos emulando uma unidade de disco local. os arquivos armazenados na unidade virtual podem ser compartilhados pelo seu proprietário a outros usuários. o ambiente deve ter uma ferramenta de busca de informação;
i- Capacidade de criação de grupos de usuários em fóruns de discussão e blogs; para as telas de leitura, criação e edição de mensagens de e-mail, mensagens instantâneas e agenda de compromissos, as interfaces deverão estar disponíveis no idioma português do Brasil;
j- Deverá existir telas com conteúdo da ajuda para usuários em português;
k- Suporte aos protocolos pop, imap;
l- Suporte a dispositivos móveis compatíveis com o activesync;
m- Suporte a smtps.

O softwares terá sua vigência por 12 meses. (Prorrogável por até 48 meses)

2.5. Windows 10 PRO

Para padronização e compatibilidade com todos os sistemas hoje existentes na CÂMARA, e porque utilizamos nossos Servidores com Sistemas Operacionais Microsoft, fazendo com que seja obrigatória a instalação do Windows 10 Pro, para acesso a nossa rede de computadores.

Atualmente a CAMARA possui suas licenças na modalidade OEM, dificultando assim uma gestão centralizada

a- Características Necessárias:

A ativação ocorrerá por meio de disponibilização de chave de acesso pela Contratada, que permitirá o acesso ao Portal Volume Lincensing Service Center – VLSC do Fabricante Microsoft.

A Contratante após o recebimento da chave de acesso citada anteriormente, conseguirá então efetuar a ativação dentro do Portal de acesso as licenças de softwares informadas neste Termo de Referência.

b- Qualificação técnica

c- Declarações de que se compromete a apresentar, no ato da assinatura do contrato:

- Declaração da Licitante – afirmando que atende os requisitos necessários para fornecer licenças para GOVERNO, ou seja, empresas LSP (Large Solution Partner), uma vez que apenas organizações com tal qualificação estão aptas a fornecer licenças nas modalidades de licenciamento contempladas nesse certame;
- Declaração da Microsoft – Declaração emitida pela Microsoft de que a empresa é revenda autorizada a fornecer licenciamento por volume para instituições governamentais na categoria "Government Partner", estando autorizada a comercializar o objeto da presente licitação na forma e modalidade de contratação prevista no termo de Referência deste edital.

As declarações deverão ser formalizadas em papel timbrado, data de emissão e assinatura do responsável com firma reconhecida

2. 6. Antivírus

No caso das licenças de Antivírus, estamos solicitando a compra também do Suporte, implementação e treinamento, por uma única empresa, que é a solução de Proteção para Endpoints, Implantação e Garantia Técnica de 36 meses.

2.6.1. Funcionalidades da solução e número de licenças

2.6.1.1. A solução a ser contratada deverá possuir os itens descritos abaixo, juntamente com a quantidade de licenças indicadas, sendo que todos os módulos devem ser fornecidos pelo mesmo fabricante.

2.6.2. Instalação, configuração e acompanhamento operacional.

2.6.2.1. Caso a solução a ser fornecida, seja diferente do software de antivírus atualmente instalado na CAMARA MUNICIPAL DE SANTO ANDRÉ, a contratada deverá providenciar a desinstalação automática de todas as cópias instaladas do software em estações e servidores e a instalação do novo software de antivírus em um único processo;

2.6.2.2. A instalação deverá ser realizada por técnicos qualificados e certificados pelo fabricante para a solução ofertada;

2.6.2.3. Caso a solução seja a mesma já existente, a mesma deve ser atualizada para a última versão disponível e todas as configurações revisadas, com as devidas correções ou melhorias implementadas;

2.6.2.4. Deverão ser instalados e configurados:

- Console de gerenciamento da solução ofertada;
- Software de antivírus nas estações de trabalho;
- Tarefas para verificação e geração de relatórios de vulnerabilidades de todo o parque computacional;
- Relatórios que serão enviados por e-mail de forma automática pela console, para os responsáveis na CÂMARA MUNICIPAL DE SANTO ANDRÉ;

2.6.2.5. Independentemente de a solução ofertada ser a de corrente uso na CÂMARA MUNICIPAL DE SANTO ANDRÉ, deverá ser fornecido acompanhamento operacional de 01 (um) técnico on-site por no mínimo 10 (dez) dias. Este acompanhamento operacional deverá ser realizado no prédio executivo da CÂMARA MUNICIPAL DE SANTO ANDRÉ, sito a Praça IV Centenário nº 02 – Diretoria de Apoio Tecnológico. Este acompanhamento deve ser feito por técnico qualificado e certificado pelo fabricante da solução ofertada;

2.6.2.6. Deverão ser executadas as seguintes tarefas em relação a este acompanhamento:

- Resolução de dúvidas sobre o produto;
- Discussão de melhorias na configuração;
- Resolução de problemas.

2.6.3. Da solução de proteção para endpoints

2.6.3.1. Proteção para endpoints – Windows

2.6.3.2. O módulo de proteção Anti-Malware deve ter a capacidade de:

a) Realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais:

- Windows Server 2003 sp2 (32/64-bit);
- Windows Server 2008 (32/64-bit) e Windows Server 2008 r2 (32/64-bit);
- Windows Server 2012;
- Windows Server 2016;
- Windows XP sp3 (x86/x64);
- Windows vista (x86/x64);
- Windows 7 (x86/x64);
- Windows 8 e 8.1 (x86/x64);
- Windows 10;

b) Detectar, analisar e eliminar programas maliciosos, tais como vírus, spyware, worms, cavalos de tróia, key loggers, programas de propaganda, rootkits, phishing, dentre outros;

c) Detectar, analisar e eliminar, automaticamente e em tempo real, programas maliciosos em:

- Processos em execução em memória principal (RAM);
- Arquivos executados, criados, copiados, renomeados, movidos ou modificados, inclusive em sessões de linha de comando (DOS ou Shell);
- Arquivos compactados automaticamente, em pelo menos nos seguintes formatos: zip, exe, arj, mime/uu, Microsoft cab.
- Arquivos recebidos por meio de programas de comunicação instantânea;
- Detectar e proteger em tempo real a estação de trabalho contra vulnerabilidades e ações maliciosas executadas em navegadores web por meio de scripts em linguagens tais como javascript, vbscript/Activex;
- Detectar variantes de malwares que possam ser geradas em tempo real na memória da estação de Trabalho ou notebook, permitindo que seja tomada ação de quarentenar a ameaça;
- Disponibilizar evidências de varredura em todas as estações de trabalho, identificando as atualizações de sucesso e as ações de insucesso visando o monitoramento de tais casos para futura tomada de ações pontuais;
- Aferir a reputação das URLs acessadas pelas estações de trabalho e notebooks, sem a necessidade de utilização de qualquer tipo de programa adicional ou plug-in ao navegador web, de forma a proteger o usuário independente da maneira de como a URL está sendo acessada;

d) O módulo de proteção Anti-Malware deve permitir:

- Configurar o consumo de CPU que será utilizada para uma varredura manual ou agendada;
- Diferentes configurações de detecção tanto no modo varredura como no modo rastreamento, sendo as onfigurações disponíveis:
- Em tempo real de arquivos acessados pelo usuário;
- Em tempo real dos processos em memória, para a captura de programas maliciosos executados em memória, sem a necessidade de escrita de arquivo;
- Manual, imediato ou programável, com interface gráfica em janelas, personalizável, com opção de limpeza;
- Por linha-de-comando, parametrizável, com opção de limpeza;
- Automáticos do sistema com as seguintes opções:

Escopo: todos os discos locais, discos específicos, pastas específicas ou arquivos específicos;

Ação: somente alertas, limpar automaticamente, apagar automaticamente, renomear automaticamente, ou mover automaticamente para área de segurança (quarentena);

Frequência: horária, diária, semanal e mensal;

Exclusões: pastas ou arquivos (por nome e/ou extensão) que não devem ser rastreados;
A restauração de maneira granular de arquivos quarentemados, sob suspeita de representarem risco de segurança;

e) A solução deve possuir:

- Detecção heurística de vírus desconhecidos;
- Mecanismo de cachê de informações dos arquivos já escaneados;
- Cachê persistente dos arquivos já escaneados para que nos eventos de desligamento e reinicialização das estações de trabalho e notebooks, a cache não seja descartada;
- Ferramenta de alterações de parâmetros de comunicação entre o cliente antivírus e o servidor de gerenciamento da solução de antivírus;

2.6.3.3. Proteção para endpoints - Linux

a) Compatibilidade:

1. Plataforma 32-bits:

- Ubuntu 14.04.5 LTS;
- Ubuntu 16.04.4 LTS;
- Ubuntu 17.10.1;
- Red Hat® Enterprise Linux® 6.9;
- CentOS-6.9;
- Debian GNU/Linux 8.10;
- Debian GNU/Linux 9.4;

Plataforma 64-bits:

- Ubuntu 14.04.5 LTS;
- Ubuntu 16.04.4 LTS;
- Ubuntu 17.10.1;
- Ubuntu 18.04; 4.2.1.2.5. Red Hat® Enterprise Linux® 6.9;
- Red Hat® Enterprise Linux® 7.4;
- CentOS-6.9;
- CentOS-7.4;
- Debian GNU/Linux 8.10;
- Debian GNU/Linux 9.4;
- OracleLinux 7.4;
- SUSE® Linux Enterprise Server 12 SP3;
- OpenSUSE® 42.3;

2.6.4. Características:

2.6.4.1 Deve prover as seguintes proteções:
2.6.4.2 Antivírus de arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;

2.6.4.3 As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora; 3.2.2.2. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
2.6.4.4 Capacidade de criar exclusões por local, máscara e nome da ameaça;
2.6.4.5 Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
2.6.4.6. 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;
2.6.4.7. Detectar aplicações que possam ser utilizadas como vetor de ataque por hackers; 3.2.2.5. Fazer detecções através de heurística utilizando no mínimo as seguintes opções de nível:
2.6.4.8. Alta;
2.6.4.9. Média;
2.6.4.10. Baixa;
2.6.4.11. Recomendado;
2.6.4.12. Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;
2.6.4.13. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados;
2.6.4.14. Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares;
2.6.4.15. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
2.6.4.16. 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;
2.6.4.17. Capacidade de verificar objetos usando heurística;
2.6.4.18. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;
2.6.4.19. Deve possuir módulo de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados, de administração remota através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).

2.6.5. Proteção para Estações de Trabalho – Funcionalidades de Atualização

As funcionalidades de atualização da solução devem incluir a capacidade de permitir:

1. A programação de atualizações automáticas das listas de definições de vírus, a partir de local predefinido da rede, ou de site seguro da internet, com frequência (no mínimo diária) e horários definidos pelo administrador da solução;
2. A atualização incremental da lista de definições de vírus;
3. A atualização automática do engine do programa de proteção a partir de localização na rede local ou na internet, a partir de fonte autenticável;
4. O rollback das atualizações das listas de definições de vírus e engines;

5. A indicação de agentes para efetuar a função de replicador de atualizações e configurações, de forma que outros agentes possam utilizá-los como fonte de atualizações e configurações, não sendo necessária a comunicação direta com o servidor de anti-malware para essas tarefas;
Deve permitir que os agentes de atualização possam replicar os componentes de vacinas, motores de escaneamento, versão de programas, hotfix e configurações específicas de domínios da árvore de gerenciamento;
6. O servidor da solução de anti-malware, deve ser capaz de gerar localmente versões incrementais das vacinas a serem replicadas com os agentes replicadores de atualizações e configurações, de maneira a reduzir o consumo de banda necessário para execução da tarefa de atualização;

O agente replicador de atualizações e configurações deve ser capaz de gerar localmente versões incrementais das vacinas a serem replicadas com os demais agentes locais, de maneira a reduzir o consumo de banda necessário para execução da tarefa de atualização;

2.6.6. Proteção para Estações de Trabalho – Console de Gerenciamento e Administração da Solução

2.6.6.1. A administração da solução se dará por console de gerenciamento, de modo que esta deverá:
2.6.6.2. Ser via web com gerenciamento por Internet Explorer, Firefox ou MMC;
2.6.6.3. Possuir dashboards customizáveis para monitoramento;
2.6.6.4. A customização deverá ser realizada pelo administrador da solução;
2.6.6.5. As variáveis customizáveis deverão ser “quantidade” e “período”;
2.6.6.6. O administrador deverá poder optar por janelas de monitoramento no dashboard a sua disposição e poderá livremente adicionar ou remover de acordo com sua necessidade de visualização;
2.6.6.7. O console de gerenciamento deverá possuir a capacidade de:
2.6.6.8. Atualizar as vacinas, engines, assinaturas e recursos de inspeção de conteúdo de forma agendada e automática;
2.6.6.9. Facilitar a busca por detecções via mecanismo;
2.6.6.10. Identificar ameaças evasivas em tempo real com o provimento de análise profunda e inteligência para identificar e prevenir ataques;
2.6.6.11. Correlacionar regras de detecção de conteúdo malicioso durante todas as fases de um ataque;
2.6.6.12. Adicionar e remover os diversos recursos de visualização de informações na tela principal de monitoramento da ferramenta;

3. A solução deve possuir funcionalidades que permitam:

3.1. A proteção das configurações da solução instalada na estação de trabalho através de senha ou controle de acesso, em ambos os casos, controlada por política gerenciada pela console de administração da solução completa;
3.2. O bloqueio por nome de arquivo;
3.3. O rastreamento e bloqueio de infecções;
3.4. A desinstalação através da console de gerenciamento da solução;
3.5. Exportar/importar configurações da solução através do console de gerenciamento;

3.6. Realização do backup da base de dados através de mapeamento de rede controlado por senha;
3.7. Deletar os arquivos quarentenados;
3.8. A remoção automática de clientes inativos por determinado período de tempo;
3.9. A utilização de consulta externa a base de reputação de sites integrada e gerenciada através da solução de anti-malware, com opção de configuração para estações dentro e fora da rede, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante;
3.10. A criação de subdomínios consecutivos dentro da árvore de gerenciamento;
3.11. A criação de usuários locais de administração da console de anti-malware;
3.12. A gerência de domínios separados para usuários previamente definidos;
3.13. O envio de notificações específicas aos respectivos administradores de cada domínio definido na console de administração;
3.14. Instalação "silenciosa";
3.15. Efetuar a instalação remota nas estações de trabalho, sem requerer outro software ou agente adicional, previamente instalado e sem necessidade de reiniciar a estação de trabalho;
3.16. Desinstalar automaticamente e remotamente a solução de antivírus atual, sem requerer outro software ou agente;
3.17. Backup da base de dados da solução através do console de gerenciamento;
3.18. Designação do local onde o backup automático será realizado;
3.19. Determinar a capacidade de armazenamento da área de quarentena;
3.20. Prover segurança através de SSL para as comunicações entre o servidor e a console de gerenciamento web;
3.21. Prover segurança através de SSL para as comunicações entre o servidor e os agentes de proteção;
3.22. Bloquear acessos indevidos a área de administração do agente que não estejam na tabela de políticas definidas pelo administrador;
3.23. Criar perfis de usuários customizáveis, concedendo acessos também customizáveis ao console de gerenciamento;
3.24. Registrar no sistema de monitoramento de eventos do console de anti-malware informações relativas ao usuário logado no sistema operacional;

4. As funcionalidades da solução devem possuir:

4.1. Mecanismo de detecção de ameaças baseado em comportamento de processos que estão sendo executados nas estações de trabalho e notebooks;
4.2. Solução de consulta do hash dos arquivos integrada e gerenciada através da solução de antivírus, cancelando o download ou execução do arquivo, de forma automática, baseado na resposta à consulta da base do fabricante;
4.3. Solução de reputação de sites local para sites já conhecidos como maliciosos integrada e gerenciada através da solução de antivírus, com opção de configuração para estações dentro e fora da rede, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante;
4.4. Mecanismo de autenticação da comunicação entre o servidor de administração e os agentes de proteção distribuídos nas estações de trabalho e notebooks.

5. A solução deverá prover ao administrador:

5.1. Relatórios de conformidade do status dos componentes, serviços, configurações das estações de trabalho e notebooks que fazem parte do escopo de gerenciamento da console de antivírus
5.2. Informações sobre quais estações de trabalho e notebooks fazem parte do escopo de gerenciamento da console de anti-malware não realizaram o escaneamento agendado ou o escaneamento demandado pelo administrador no período determinado de dias.
5.3. A solução deverá integrar-se ao Active Directory para:
5.4. Acesso ao console de gerenciamento para administração;
5.5. A solução deverá suportar múltiplas florestas e domínios confiáveis do Active Directory;
5.6. Identificar quais máquinas estão sem a solução de anti-malware instalada;
5.7. Permitir agrupamento automático de estações de trabalho e notebooks do console de gerenciamento baseando-se no escopo do Active Directory ou IP.
5.8. Proteção para Estações de Trabalho – Do Controle de Dispositivos
5.9. O controle de dispositivos deverá controlar:
5.9.1. Acesso a discos removíveis reconhecidos como dispositivos de armazenamento em massa através de interfaces USB e outras, com as seguintes opções: acesso total, leitura e escrita, leitura e execução, apenas leitura, e bloqueio total;
5.9.2. Acesso a drives de mídias de armazenamento como CD-Rom, DVD, e pendrives, com as opções de acesso total, leitura e escrita, leitura e execução, apenas leitura e bloqueio total.
5.10. Deve possuir módulo que habilite ou não o funcionamento dos seguintes dispositivos externos, no mínimo:
5.10.1. Discos de armazenamento locais;
5.10.2. Armazenamento removível;
5.10.3. Impressoras;
5.10.4. CD/DVD;
5.10.5. Drives de disquete;
5.10.6. Modems;
5.10.7. Dispositivos de fita;
5.10.8. Dispositivos multifuncionais;
5.10.9. Leitores de smart card;
5.10.10. Dispositivos de sincronização via ActiveSync (Windows CE, Windows Mobile, etc);
5.10.11. Wi-Fi;
5.10.12. Adaptadores de rede externos;
5.10.13. Dispositivos MP3 ou smartphones;
5.10.14. Dispositivos Bluetooth;
5.10.15. Câmeras e Scanners.
5.11. 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;
5.12. Capacidade de habilitar “logging” em dispositivos removíveis tais como Pendrive, Discos externos, etc.
5.13. Proteção para Estações de Trabalho – Da Autoproteção

5.14. A solução deverá possuir mecanismo de proteção contra uso não autorizado no qual o agente do antivírus deve ser protegido contra mudança do seu estado (não possibilitar que um administrador da estação de trabalho e notebook possa parar o serviço do antivírus) bem como mecanismo para restaurar seu estado normal;
5.15. Devem estar inclusas no mecanismo de autoproteção:
5.15.1. Proteção e verificação dos arquivos de assinatura;
5.15.2. Proteção dos processos do agente de segurança;
5.15.3. Proteção das chaves de registro do agente de segurança;
5.15.4. Proteção do diretório de instalação do agente de segurança;
5.16. Proteção para Estações de Trabalho – Características do Host Firewall
5.16.1. O host firewall deverá ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais:
5.16.1.1. Windows Server 2003 sp2 (32/64-bit);
5.16.1.2. Windows Server 2008 (32/64-bit) e Windows Server 2008 r2 (32/64-bit);
5.16.1.3. Windows Server 2012 (32/64-bit);
5.16.1.4. Windows XP sp2 / sp3 (x86/x64);
5.16.1.5. Windows vista (x86/x64);
5.16.1.6. Windows 7 (x86/x64);
5.16.1.7. Windows 8 e 8.1 (x86/x64).
5.16.2. O host firewall deverá permitir a criação de:
5.16.2.1. Políticas de segurança personalizadas;
5.16.2.2. Regras de firewall utilizando os seguintes protocolos:
5.16.2.3. Icmp, icmpv6, igmp, tcp, udp, tcp+udp;
5.16.2.4. Regras de firewall por origem de ip ou mac ou porta e destino de ip ou mac ou porta;
5.16.3. Grupos lógicos através de lista de ip, mac ou portas;
5.16.3.1. Contextos para a aplicação para criação de regras de firewall.
5.16.4. Devem ser funcionalidades do host firewall:
5.16.4.1. Ativação e desativação do produto sem a necessidade de remoção do mesmo;
5.16.4.2. Varredura de portas lógicas do sistema operacional para identificar quais estejam abertas, possibilitando também o tráfego de entrada e saída;
5.16.4.3. Emissão de alertas via smtp e snmp;
5.16.4.4. Configuração e manipulação de políticas de firewall através de prioridades.
5.17. A solução deverá permitir a criação de dashboards customizáveis:
5.17.1. Os dashboards serão compostos por blocos de informações (widgets), visualizados através de gráficos ou tabelas;
5.17.2. As informações pertencentes aos painéis personalizáveis devem permitir filtros personalizados para facilitar a visualização e gerenciamentos
5.17.3. A seleção de uma informação específica através de um clique, deve redirecionar ao log detalhado que gerou aquela informação;
5.17.4. Todas as regras das funcionalidades de firewall de host devem permitir apenas detecção (log) ou prevenção (bloqueio); 3.8.6. A solução deverá possuir módulo para proteção de vulnerabilidades com as funcionalidades de host firewall.
5.18. Proteção para Estações de Trabalho – Do Gerenciamento Centralizado dos Módulos

5.19. A solução de gerenciamento centralizado deve permitir a integração com a solução de segurança para proteção de estações de trabalho (desktops e notebooks), com todos os seus módulos e dispositivos móveis;
5.20. A instalação do servidor deverá ser na plataforma Windows 2003 Server ou superior, seja o servidor físico ou virtual;
5.21. O gerenciamento centralizado de módulos deverá:
5.21.1. Suportar base de dados sql;
5.21.2. Gerenciar logs das atividades e eventos gerados pela solução;
5.21.3. Integrar-se ao Microsoft ad – Active Directory;
5.21.4. Disponibilizar sua interface através dos protocolos http e https;
5.22. Possuir acompanhamento dos comandos administrativos em execução, tal como seu status de conclusão, alvo e usuário.
5.23. Os métodos de envio suportados devem incluir: e-mail, gravação de registros de eventos do Windows, SNMP e SYSlog;
5.24. A solução deverá permitir:
5.24.1. Atualização de todos os componentes de todos os módulos gerenciados;
5.24.2. Criação de planos de entrega das atualizações, com hora de início ou postergação da entrega após o download dos componentes;
5.24.3. Controle individual de cada componente a ser atualizado;
5.24.4. Definição de exceções por dias e horas para não realização de atualizações;
5.24.5. Ter como fonte de atualização um compartilhamento de rede no formato UNC;
5.24.6. Níveis de administração por usuários ou grupos de usuários;
5.24.7. Constituição de políticas genéricas aplicáveis a grupos de máquinas, ou aplicáveis a grupos de usuários;
5.24.8. Alteração das configurações das ferramentas ofertadas, de maneira remota;
5.24.9. Diferentes níveis de administração, de maneira independente do login da rede;
5.25. Pesquisas personalizadas para a consulta de eventos (logs) através de:
5.25.1. Categorias;
5.25.2. Critérios lógicos, com base em todos os campos pertencentes aos eventos consultados;
5.25.3. Configuração de/do:
5.25.4. Eventos administrativos ou de segurança que geram notificações, tal como o método de envio e o destinatário;
5.25.5. Intervalo de comunicação com os módulos gerenciados;
5.25.6. Intervalo de tempo necessário para que um módulo seja considerado fora do ar (off-line);
5.25.7. Informações que não são enviadas dos módulos à solução de gerenciamento centralizado;
5.25.8. Manutenção dos registros de eventos (logs), com base no intervalo de tempo que devem ser mantidos e no número máximo de registros, por tipo de evento;
5.25.9. Visualização de eventos de violação de segurança de todos os módulos gerenciados, agrupado por usuário numa linha de tempo, configurável;
5.25.10. Investigação de incidentes de vazamento de informação através de um número identificador de incidentes;
5.25.11. Gerencia dos módulos baseados no modelo de nuvem (cloud), quando existentes.
5.26. A solução deverá permitir a criação de políticas de segurança personalizadas;

5.27. As políticas de segurança devem permitir a seleção dos alvos baseados nos seguintes critérios:
5.27.1. Nome parcial ou completo das estações de trabalho, permitindo a utilização de caractere coringa para identificação do nome parcial da máquina;
5.27.2. Range de endereços IPS;
5.27.3. Sistema operacional;
5.27.4. Agrupamento lógico dos módulos;
5.27.5. As políticas de segurança devem permitir a combinação lógica dos critérios para identificação do(s) alvo(s) de cada política.
5.28. A solução deverá permitir a criação de modelos de relatórios customizáveis:
5.28.1. Relatórios e gráficos deverão ser parametrizáveis nos formatos HTML, PDF, XLS

6. Fornecimento de treinamento e capacitação

6.1. Deverão ser contemplados 1 (um) treinamento oficial on site para a capacitação de profissionais da CÂMARA MUNICIPAL DE SANTO ANDRÉ na solução ofertada, com carga horária conforme abaixo:
6.2. Treinamento: Solução de proteção para endpoint – no mínimo 20 horas – participação de 3 (três) profissionais;
6.3. O treinamento oferecido deverá conter, no mínimo:
6.3.1. Funcionalidades básicas;
6.3.2. Gerenciamento avançado;
6.3.3. Instalação e desinstalação do software cliente;
6.3.4. Instalação e desinstalação do software
6.3.5. O treinamento deverá ser realizado por instituição qualificada e certificada pelo fabricante da solução ofertada;
6.3.6. O treinamento deverá ser oficial e com material dos produtos ofertados.

7. RESUMO DOS ITENS:

ITEM	DESCRIÇÃO PRODUTO	QUANTIDADE
1	Creative Cloud All Apps with Stock – 36 Meses	2
	Creative Cloud All Apps – 36 Meses	1
2	Software Acesso remoto para suporte as estações de trabalho da CÂMARA	5
3	Pacote Office 365 - E1	40
4	Licenças Windows 10 Pro Upgrade	40
5	Solução de Proteção para Endpoints (estação de trabalho e servidores) - 36 meses	220
	Implementação das soluções de segurança de Endpoint e Servidores	1
	Treinamento para solução de proteção de Endpoints e Servidores – on site	1

CÂMARA MUNICIPAL DE
SANTO ANDRÉ

ANEXO II

ATO Nº 4, DE 22 DE MARÇO DE 2005

Dispõe sobre procedimentos administrativos relativos a aplicação de multas e outras sanções decorrentes da inexecução total ou parcial dos contratos assinados com a Câmara Municipal de Santo André, nos termos dos artigos 81, 86 e 87 da Lei Federal 8.666/93.

Art. 1º No âmbito da Câmara Municipal de Santo André, a aplicação de multas e outras sanções decorrentes de atraso no cumprimento de obrigações ou da inexecução total ou parcial dos contratos, obedecerá aos procedimentos estabelecidos por este Ato e às disposições da Lei Federal nº 8.666/93, em especial ao que dispõem os artigos 81, 86 e 87.

Art. 2º A recusa injustificada do adjudicatário em assinar o contrato, aceitar ou retirar instrumento equivalente, dentro do prazo estabelecido pelo edital ou carta-convite do certame, caracteriza o descumprimento total da obrigação assumida de que trata o artigo 81 da Lei Federal nº 8.666/93, sujeitando-o à multa de 20% (vinte por cento) sobre o valor contratado.

Art. 3º O atraso injustificado na execução do contrato cujo objeto seja a prestação de serviço, realização de obra ou entrega de bens adquiridos, sem prejuízo do disposto no § 1º do artigo 86 da Lei Federal nº 8.666/93, sujeitará a contratada à multa de mora, calculada por dia de atraso sobre o valor da obrigação não cumprida, a partir do primeiro dia útil seguinte ao término do prazo estipulado na proposta, no edital ou no contrato para cumprimento da obrigação, conforme o caso, nas seguintes proporções:

I - multa de 0,5% (meio por cento) ao dia, até o 15º (décimo quinto) dia de atraso;

II - multa de 1% (um por cento) ao dia a partir do 16º (décimo sexto) dia de atraso e até o 30º (trigésimo) dia;

III – após 30 (trinta) dias de atraso para cumprimento da obrigação, o contrato será considerado rescindido de pleno direito pela Administração, aplicando à contratada inadimplente as penalidades previstas no artigo 4º deste Ato.

§ 1º Os eventuais pedidos de prorrogação de prazo para entrega de materiais ou para execução de obras ou serviços contratados, somente serão apreciados e deliberados se apresentados por escrito e com a devida justificativa, dentro dos prazos fixados para entrega ou execução, estabelecidos na proposta, no edital ou no contrato, conforme o caso.

§ 2º Na hipótese de deferimento do pedido de que trata o parágrafo anterior, o prazo de prorrogação começará a fluir a partir do dia útil subsequente ao da comunicação da decisão do (a) Presidente (a) que autorizou a referida prorrogação.

§ 3º Ocorrendo o atraso de que trata o *caput* deste artigo, tal fato será certificado pelo setor competente da Câmara, devendo o processo ser remetido para o(a) Presidente(a) da Câmara para fins do disposto no artigo 6º deste Ato.

§ 4º O pedido para prorrogação de prazo ou a justificativa pelo atraso, somente serão aceitos pelo (a) Presidente(a) da Câmara quando forem fundamentados e provados o caso fortuito ou

força maior que impediu o cumprimento da obrigação pela contratada no prazo avençado.

Art. 4º Pela inexecução total ou parcial do contrato, qualquer que seja o seu objeto, fica a contratada sujeita às seguintes penalidades, a serem aplicadas de forma discricionária pela Administração Pública, observado o princípio da razoabilidade:

I - advertência;

II – multa de 20% (vinte por cento) sobre o valor da parcela inadimplente; ou

III – multa de 20% (vinte por cento) sobre o valor do contrato quando houver inexecução total da avença; ou

IV - suspensão temporária de participação em licitação e impedimento de contratação com a Administração por até 2 (dois) anos;

V - declaração de inidoneidade para licitar e contratar com a Administração.

Art. 5º Os bens, serviços e obras contratados, quando entregues em desacordo com a especificação inicial, não serão aceitos e deverão ser substituídos e/ou corrigidos no prazo máximo de até 15 (quinze) dias, a critério da Administração, contados do recebimento da notificação pela contratada, sob pena de incorrer o fornecedor em inadimplência contratual.

Parágrafo único. Quando a substituição e/ou correção referidas no *caput* deste artigo for impossível no prazo avençado por razões técnicas ou pela complexidade da matéria, tal situação deverá ser certificada pelo setor responsável pela gestão do contrato e devidamente comprovada no processo correspondente, assim como submetida à aprovação do (a) Presidente (a) da Câmara, que estipulará prazo razoável para cumprimento da obrigação.

Art. 6º Esgotados os contatos ordinários para resolver eventuais pendências contratuais, o setor competente enviará o processo, acompanhado de relatório circunstanciado sobre os fatos, ao (à) Presidente (a) da Câmara, para que este (a) decida, por despacho fundamentado, sobre a abertura dos procedimentos administrativos tendentes à aplicação das multas e outras sanções, por recusa do adjudicatário em assinar o contrato, atraso no cumprimento de obrigações, ou inexecução total ou parcial de qualquer contrato.

Art. 7º Nas hipóteses dos artigos 2º, 3º e 4º deste Ato, e após as providências do artigo 6º, a contratada será previamente notificada, por ofício, com aviso de recebimento juntado aos autos, para oferecer defesa prévia, por escrito, protocolizado no Setor de Protocolo e Arquivo, nos prazos abaixo estabelecidos:

I - no prazo de 5 (cinco) dias úteis, contados da juntada aos autos do comprovante de notificação da contratada, no caso dos incisos I, II, III e IV do artigo 4º;

II - no prazo de 10 (dez) dias, contados da juntada aos autos do comprovante de notificação da contratada, no caso do inciso V do artigo 4º.

§ 1º Na hipótese da contratada não atualizar o seu cadastro junto à Câmara Municipal, e ser ignorado, incerto e não sabido o seu endereço, a notificação e/ou intimação será realizada por edital, publicado no órgão responsável pela publicação dos atos oficiais do Município de Santo André, por 2 (duas) vezes consecutivas, contando-se o prazo para defesa a partir do primeiro dia útil seguinte ao da última publicação, cujas cópias dos editais serão juntadas ao processo.

§ 2º Decorrido o prazo, com ou sem defesa, o processo será remetido ao (à) Presidente(a) da Câmara, com relatório circunstanciado elaborado pelo setor competente, para decisão final.

Art. 8º Caberá ao (à) Presidente (a) da Câmara Municipal aplicar as sanções de que trata este Ato, qualquer que seja a forma de contratação.

Art. 9º Das decisões do (a) Presidente (a) que resultar na aplicação das penas de multa e outras sanções, caberá recurso dirigido à Mesa Diretora da CMSA, protocolizado no Setor de Protocolo e Arquivo:

I - no prazo de 5 (cinco) dias úteis, contados da juntada aos autos do comprovante de intimação da decisão, nas hipóteses dos artigos 2º, 3º e incisos I, II, III e IV do artigo 4º deste ato, podendo, em idêntico prazo, o (a) Presidente (a) da Câmara reconsiderar sua decisão ou fazê-lo subir, devidamente informado, à consideração da Mesa Diretora, devendo, neste caso, a decisão final ser proferida no prazo de 5 (cinco) dias úteis, contados do recebimento do recurso;

II - no prazo de 10 (dez) dias úteis, contados da juntada aos autos do comprovante de intimação da decisão, na hipótese do inciso V do artigo 4º deste Ato, podendo, em idêntico prazo, o (a) Presidente (a) da Câmara reconsiderar a sua decisão, ou fazê-lo subir, devidamente informado, à consideração da Mesa Diretora, devendo, neste caso, a decisão ser proferida no prazo de 10 (dez) dias úteis, contados do recebimento do recurso.

Parágrafo único. Os recursos obedecerão aos mesmos procedimentos estabelecidos no artigo 7º deste Ato.

Art. 10. Os valores das multas de que trata este Ato poderão ser cobrados mediante dedução de eventuais pagamentos devidos pela Câmara às contratadas, ou, na ausência destes, e a critério da Administração, deduzidos do valor da garantia prestada pelas contratadas.

§ 1º O prazo para o recolhimento das multas previstas neste Ato é de 15 (quinze) dias contados da notificação da contratada, podendo ser prorrogado, a juízo da Administração, por mais 15 (quinze) dias.

§ 2º A notificação de que trata o parágrafo anterior poderá ser feita por edital, nos termos do § 1º do artigo 7º deste Ato.

§ 3º Não sendo possível a cobrança das multas na forma prevista neste artigo, será a cobrança efetuada por meio de medidas administrativas ou judiciais, incidindo correção sobre o valor devido no período compreendido entre o dia imediatamente posterior à data final para liquidar a multa e aquele em que o pagamento efetivamente ocorrer.

§ 4º As multas serão calculadas também sobre os reajustamentos contratuais, se houver.

Art. 11. As multas e sanções aplicadas com base neste Ato são autônomas e não excluem a aplicação de outras sanções previstas em legislação esparsa.

Art. 12. Como índice de atualização será adotado, no âmbito da Câmara Municipal de Santo André, o FMP (Fator Monetário Padrão), devendo as multas aplicadas serem convertidas, na data da sua aplicação.

Art. 13. Este Ato deve ser parte integrante, como anexo obrigatório, de todos os editais de licitação, bem como dos contratos, inclusive daqueles oriundos de contratação direta.

Art. 14. A abertura do processo administrativo, bem como os atos de punição e decisão final serão proferidos na forma de portaria, expedida pelo (a) Presidente (a) ou pela Mesa Diretora, conforme o caso, nos termos do artigo 240 do Regimento Interno da Câmara Municipal de Santo André.

Art. 15. As disposições constantes deste Ato aplicam-se, no que couber, aos contratos vigentes, ressalvados os valores de multas anteriormente pactuados.

Art. 16. Este Ato entra em vigor na data de sua publicação.

Câmara Municipal de Santo André, 22 de março de 2005, 451º ano da fundação da cidade.

LUIZ ZACARIAS

Presidente

MARIA FERREIRA DE SOUZA - LOLÓ

1ª Secretária

DINAH ZEKCER

2ª Secretária

TRIBUNAL DE CONTAS DO ESTADO DE SÃO PAULO

ANEXO III

TERMO DE CIÊNCIA E DE NOTIFICAÇÃO

CONTRATANTE: CÂMARA MUNICIPAL DE SANTO ANDRÉ
CONTRATADO: BRASOFTWARE INFORMÁTICA LTDA
CONTRATO Nº (DE ORIGEM): 26/2020 - Processo CMSA 6533/2019 – Pregão 12/2020.
OBJETO: Aquisição de softwares.
ADVOGADO (S)/ Nº OAB: (*)_____

Pelo presente TERMO, nós, abaixo identificados:

1. Estamos CIENTES de que:

a) o ajuste acima referido estará sujeito a análise e julgamento pelo Tribunal de Contas do Estado de São Paulo, cujo trâmite processual ocorrerá pelo sistema eletrônico;
b) poderemos ter acesso ao processo, tendo vista e extraindo cópias das manifestações de interesse, Despachos e Decisões, mediante regular cadastramento no Sistema de Processo Eletrônico, conforme dados abaixo indicados, em consonância com o estabelecido na Resolução nº 01/2011 do TCESP;
c) além de disponíveis no processo eletrônico, todos os Despachos e Decisões que vierem a ser tomados, relativamente ao aludido processo, serão publicados no Diário Oficial do Estado, Caderno do Poder Legislativo, parte do Tribunal de Contas do Estado de São Paulo, em conformidade com o artigo 90 da Lei Complementar nº 709, de 14 de janeiro de 1993, iniciando-se, a partir de então, a contagem dos prazos processuais, conforme regras do Código de Processo Civil;
d) Qualquer alteração de endereço – residencial ou eletrônico – ou telefones de contato deverá ser comunicada pelo interessado, peticionando no processo.

2. Damo-nos por NOTIFICADOS para:

a) O acompanhamento dos atos do processo até seu julgamento final e consequente publicação;
b) Se for o caso e de nosso interesse, nos prazos e nas formas legais e regimentais, exercer o direito de defesa, interpor recursos e o que mais couber.

Santo André (SP), 16 de novembro de 2020.

GESTOR DO ÓRGÃO/ENTIDADE:
Nome: Pedro Luiz Mattos Canhassi Botaro
Cargo: Presidente da Câmara Municipal de Santo André
CPF: 312.568.618-04 - RG: 29.775.799-4 (SSP-SP)
Data de Nascimento: 25/7/1983
Endereço residencial completo: Rua Alzira, 413 – Vila Alzira, Santo André / SP, CEP 09030-200
E-mail institucional: gabinetedapresidencia@cmsandre.sp.gov.br
E-mail pessoal: pedrinhobotaro@yahoo.com.br
Telefone(s): (11) 3429-5883

Assinatura: _____

Responsáveis que assinaram o ajuste:
Pelo CONTRATANTE:
Nome: Pedro Luiz Mattos Canhassi Botaro
Cargo: Presidente da Câmara Municipal de Santo André
CPF: 312.568.618-04 - RG: 29.775.799-4 (SSP-SP)
Data de Nascimento: 25/7/1983
Endereço residencial completo: Rua Alzira, 413 – Vila Alzira, Santo André / SP, CEP 09030-200
E-mail institucional: gabinetedapresidencia@cmsandre.sp.gov.br
E-mail pessoal: pedrinhobotaro@yahoo.com.br
Telefone(s): (11) 3429-5883

Assinatura: _____

Pela CONTRATADA:
Nome: Fernanda Esteves Simoni
Cargo: Executiva de Contas Governo SP
CPF: 299.707.828-86 – RG: 43.444.082-6 (SSP-SP)
Data de Nascimento: 10/02/1982
Endereço residencial completo: Rua Ângelo Antônia Zago Botteghim, 63, Jardim Patente, São Paulo/SP, CEP: 04243-050
E-mail institucional: fernanda.esteves@brasoftware.com.br
E-mail pessoal: fe_cesteves@hotmail.com
Telefone(s): (11) 3179-6722

Assinatura: _____

Advogado:
(*) Facultativo. Indicar quando já constituído, informando, inclusive, o endereço eletrônico.