
SERVIÇO AUTÔNOMO DE ÁGUA E ESGOTO DE SÃO CARLOS

EDITAL DE PREGÃO ELETRÔNICO Nº 010/2018

- PARTICIPAÇÃO AMPLA -

PROCESSO LICITATÓRIO Nº 6141/2017

TIPO: "MENOR PREÇO"

O **SERVIÇO AUTÔNOMO DE ÁGUA E ESGOTO DE SÃO CARLOS**, pessoa jurídica de direito público interno, com sede nesta cidade de São Carlos - SP, na Avenida Getúlio Vargas, nº 1.500, Jardim São Paulo, inscrita no CNPJ sob nº 45.359.973/0001-50, I.E. nº 637.271.909.116, torna público para conhecimento de todos os interessados que no dia e hora abaixo indicados, será realizada licitação na modalidade **PREGÃO ELETRÔNICO**, do tipo **"MENOR PREÇO"**, que será regido pela Lei Federal nº 10.520/17/07/2002, pelo Decreto Municipal nº 151/2004, com aplicação subsidiária da Lei Federal nº 8.666/93 e suas alterações posteriores, Lei Complementar nº 123/06, e suas alterações posteriores, e, no que couber, pelo Decreto nº 5450/2005 e pelo Decreto Federal nº 8538/2015, além das demais disposições legais aplicáveis, e condições estabelecidas no presente Edital e seus Anexos.

O Pregão Eletrônico será realizado em sessão pública, por meio de sistema eletrônico de comunicação pela INTERNET. O sistema referido utiliza recursos de criptografia e de autenticação que asseguram condições adequadas de segurança em toda etapa do certame.

A informação dos dados para acesso deve ser feita na página inicial no site do Banco do Brasil S/A. www.bb.com.br, opção Licitações, ou diretamente em www.licitacoes-e.com.br.

O edital estará disponível gratuitamente nos sítios: www.saaesaocarlos.com.br e www.licitacoes-e.com.br.

ABERTURA DAS PROPOSTAS: às 09 horas do dia 27/02/2018.

INÍCIO DA SESSÃO DE DISPUTA DE PREÇOS: às 10 horas do dia 27/02/2018.

TEMPO DE DISPUTA NORMAL: 05 minutos, a etapa de lances da sessão pública será encerrada por decisão do Pregoeiro. Após o fechamento, transcorrerá período de tempo de 01 (um) segundo até 30 (trinta) minutos, aleatoriamente determinado pelo sistema eletrônico, findo o qual será automaticamente encerrada a recepção de lances.

FORMALIZAÇÃO DE CONSULTAS: Observando o prazo legal, o concorrente poderá formular pedidos de esclarecimento por mensagem eletrônica (e-mail), informando o número da licitação, até 03 (três) dias úteis anteriores à data fixada para abertura da sessão pública, através endereço eletrônico: pregoeiro@saaesaocarlos.com.br.

As consultas serão respondidas por e-mail, ou diretamente no site www.licitacoes-e.com.br, no campo "mensagens" no link correspondente a este pregão.

No campo "mensagens" serão disponibilizadas, além das respostas, outras informações que o Pregoeiro julgar importantes, razão pela qual os interessados no certame devem consultar o sítio com frequência.

REFERÊNCIA DE TEMPO: para todas as referências de tempo será considerado o horário de Brasília - DF.

Integram o presente Edital os seguintes anexos:

ANEXO I – TERMO DE REFERÊNCIA;

ANEXO II – MODELO DE PROPOSTA DE PREÇOS;

ANEXO III – DECLARAÇÃO DE ADEQUAÇÃO AO ARTIGO 7º – INCISO XXXIII DA CONSTITUIÇÃO FEDERAL;

ANEXO IV – DECLARAÇÃO DE INEXISTÊNCIA DE FATO IMPEDITIVO;

ANEXO V – DECLARAÇÃO DE MICROEMPRESA OU EMPRESA DE PEQUENO PORTE;

ANEXO VI – TERMO DE CIÊNCIA E NOTIFICAÇÃO.

1. DO OBJETO:

1.1. A presente licitação tem por objeto a aquisição de Solução de Software corporativo para proteção completa contra vírus e códigos maliciosos, conforme especificações, quantidades estimadas e condições estabelecidas no Anexo I do presente edital.

2. DO PROCEDIMENTO:

2.1. O Pregão Eletrônico será realizado em sessão pública, por meio da *INTERNET*, mediante condições de segurança - criptografia e autenticação - em todas as suas fases, com apoio técnico e operacional do Setor de Manutenção e Suporte Tecnológico do SAAE.

2.2. O certame será realizado através da utilização da opção "Licitações", do Portal Eletrônico do Banco do Brasil S/A, conforme acordo de cooperação técnica celebrada entre o BANCO DO BRASIL S/A e o SERVIÇO AUTÔNOMO DE ÁGUA E ESGOTO DE SÃO CARLOS.

2.3. Os trabalhos serão conduzidos pelo "Pregoeiro", com o suporte de sua equipe de apoio, os quais, juntamente com a autoridade competente do órgão promotor da licitação, formam o conjunto de operadores do sistema do Pregão Eletrônico.

3. CONDIÇÕES DE PARTICIPAÇÃO (PARTICIPAÇÃO AMPLA):

3.1. Poderão participar desta licitação os interessados que atendam a todas as exigências constantes neste Edital e seus anexos, inclusive, quanto à documentação, sendo vedada a participação sob a forma de consórcio.

3.2. Estarão impedidos de participar da presente licitação:

3.2.1. Os interessados suspensos do direito de licitar com a Administração Municipal de São Carlos, no prazo e nas condições do impedimento;

3.2.2. Os interessados que tenham sido declarados inidôneos pela Administração Municipal, Estadual ou Federal, o que abrange a administração direta e indireta, as entidades com personalidade jurídica de direito privado sob o seu controle e as fundações por ela instituída e mantida, enquanto perdurarem os motivos determinantes da punição ou até que seja reabilitado perante a autoridade que aplicou a penalidade;

3.2.3. Os interessados que estão em regime de falência, dissolução, liquidação ou concurso de credores;

3.2.4. Empresas em forma de consórcios.

4. DO CREDENCIAMENTO NO SISTEMA E EFETIVA PARTICIPAÇÃO:

4.1. Para acesso ao sistema eletrônico, os interessados em participar do Pregão Eletrônico deverão dispor de chave de identificação e senha pessoal e intransferível, obtida junto às Agências do Banco do Brasil S/A sediadas no País.

4.2. O credenciamento do concorrente vencedor e de seu representante legal junto ao sistema eletrônico implica na responsabilidade legal pelos atos praticados e a capacidade técnica para realização das transações inerentes ao pregão eletrônico.

4.3. A chave de identificação e a senha terão validade de 01 (um) ano e poderão ser utilizadas em qualquer pregão eletrônico, salvo quando canceladas por solicitação do credenciado ou por iniciativa do Banco, devidamente justificado.

4.4. É de exclusiva responsabilidade do usuário o sigilo da senha, bem como seu uso em qualquer transação efetuada diretamente ou por seu representante, não cabendo ao Banco do Brasil S/A, ao provedor do sistema ou ao órgão promotor da licitação responsabilidade por eventuais danos decorrentes de uso indevido da senha, ainda que por terceiros.

4.5. A participação no Pregão Eletrônico se dará por meio da digitação da senha pessoal e intransferível do representante credenciado e subsequente cadastramento da proposta de preços, exclusivamente por meio do sistema eletrônico, observados data e horário limite estabelecidos.

4.6. O encaminhamento de proposta pressupõe o pleno conhecimento e atendimento às exigências de habilitação previstas no Edital. O concorrente será responsável por todas as transações que forem efetuadas em seu nome no sistema eletrônico, assumindo como firmes e verdadeiras suas propostas e lances.

4.7. Caberá ao concorrente acompanhar as operações no sistema eletrônico durante a sessão pública do pregão, ficando responsável pelo ônus decorrente da perda de negócios diante da inobservância de quaisquer mensagens emitidas pelo sistema ou de sua desconexão.

5. DO RECEBIMENTO E ABERTURA DAS PROPOSTAS E FORMULAÇÃO DOS LANCES:

5.1. As propostas serão recebidas (cadastradas) até o horário previsto, após o que terá início a sessão pública do pregão eletrônico, com a divulgação das propostas de preços recebidas, passando o Pregoeiro a avaliar sua aceitabilidade.

5.2. Aberta a etapa competitiva, os representantes dos concorrentes deverão estar conectados ao sistema para participar da sessão de lances. A cada lance ofertado o concorrente será imediatamente informado de seu recebimento e respectivo horário de registro e valor.

5.3. O concorrente somente poderá oferecer lance inferior ao último por ele ofertado e registrado pelo sistema.

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

5.5. Durante o transcurso da sessão pública, os concorrentes serão informados, em tempo real, do valor do menor lance registrado. O sistema não identificará o autor dos lances aos demais concorrentes, tampouco ao pregoeiro.

5.6. No caso de desconexão com o Pregoeiro no decorrer da etapa competitiva do Pregão, o sistema eletrônico poderá permanecer acessível aos concorrentes para a recepção dos lances, retomando o Pregoeiro, quando possível, sua atuação no certame, sem prejuízos dos atos realizados.

5.6.1. Quando a desconexão persistir por tempo superior a 10 (dez) minutos, a sessão do Pregão Eletrônico será suspensa e terá reinício somente após comunicação expressa aos concorrentes, através de mensagem eletrônica, via sistema, divulgando data e hora da reabertura da sessão.

5.7. Na disputa normal, a etapa de lances da sessão pública será encerrada por decisão do pregoeiro mediante aviso de fechamento iminente da fase inicial de lances, emitido pelo sistema eletrônico, após transcorrer o período de tempo extra de 01 (um) segundo até 30 (trinta) minutos, aleatoriamente determinado pelo sistema eletrônico, findo o qual será automaticamente encerrada a recepção de lances.

5.8. Será permitido à Microempresa e Empresa de Pequeno Porte, o exercício de direito de preferência nos termos dos artigos 44, parágrafo segundo, combinado com o artigo 45, da Lei Complementar nº 123/2006, com oferecimento de proposta após o encerramento da disputa, exclusivamente por meio eletrônico previsto neste edital.

5.9. Após o encerramento da etapa de lances da sessão pública, o Pregoeiro poderá encaminhar pelo sistema eletrônico contraproposta ao concorrente que tenha apresentado lance mais vantajoso, para que seja obtida a melhor proposta, observado o critério de julgamento, não se admitindo negociar condições diferentes daquelas previstas no Edital. A negociação será realizada por meio do sistema, podendo ser acompanhada pelos demais concorrentes.

5.10. O sistema informará a proposta de menor preço imediatamente após o encerramento da etapa de lances, e será aberta automaticamente fase para considerações finais pelo pregoeiro, após a qual este encerrará o lote.

5.10.1. As etapas seguintes serão realizadas fora da sala de disputa, através de acesso identificado.

5.11. Caso não sejam apresentados lances, será verificada a conformidade entre a proposta de menor preço e valor estimado para a contratação.

5.11.1. Se houver duas ou mais propostas iniciais de mesmo valor, o sistema classificará como arrematante o concorrente que inseriu a proposta primeiro.

6. DA PROPOSTA:

6.1. A proposta deverá obedecer aos seguintes critérios:

6.1.1. Os preços deverão ser cotados em moeda corrente nacional, devendo o valor unitário proposto corresponder à unidade solicitada (Unidades de Medida constantes no Anexo I);

6.1.2. Excepcionalmente nos casos em que o valor unitário for inferior a um real, poderão ser aceitas propostas com 04 (quatro) casas decimais;

6.1.3. A proposta de preço contemplando o "valor global do lote" deverá ser cadastrada no sistema eletrônico até a data e hora marcada para abertura das propostas.

6.1.4. Após a sessão de disputa, deverá ser apresentada, pelo licitante classificado em primeiro lugar (arrematante do lote), proposta escrita atualizada, nos moldes estabelecidos no Anexo II, juntamente com a documentação de habilitação, conforme item 10 deste edital.

6.1.5. A marca/procedência da solução poderá ser especificada no envio da proposta junto ao site, em campo específico do site Licitações-e "Informações adicionais".

6.1.6. A marca/procedência da solução deverá ser obrigatoriamente especificada na proposta escrita.

6.1.7. Condições de pagamento, conforme item 13 deste edital e seus subitens.

6.2. O prazo de validade da proposta é de, no mínimo, 60 (sessenta) dias a contar da data de sua apresentação.

6.3. Prazo e condições de entrega:

6.3.1. Prazo e condições de entrega: A solução deverá ser entregue de imediato a 30 (trinta) dias corridos após o recebimento do Pedido de Compras, efetivando-se no Setor de Almoxarifado, na Rua José Casale, 400, Jardim São Paulo - São Carlos - SP, em dias úteis, das 08h às 11h e das 13h às 16h, de segunda-feira a sexta-feira, exceto feriados e pontos facultativos, por conta, risco e custo do Contratado, incluído todos os custos e despesas, tais como, e sem se limitar a: custos diretos e indiretos, tributos incidentes, despesas administrativas, materiais, serviços, encargos sociais, trabalhistas, seguros, frete, embalagens, carga/descarga, lucro, despesas, acessórios e encargos, inclusive tributários, incidente sobre a proposta, quando não incorporados ao preço oferecido e outros necessários ao cumprimento integral do objeto deste edital e seus anexos.

6.3.2. O licitante contratado, de acordo com a cláusula 2ª, inciso I, do protocolo ICMS 42, estará obrigado a emitir Nota Fiscal Eletrônica - NF-E, modelo 55, portanto, além da via original que acompanha a mercadoria, encaminhar também por meio eletrônico para o seguinte endereço de e-mail: almoxarifado@saaesaocarlos.com.br.

6.3.3. O licitante contratado ficará obrigado a trocar, a suas expensas, o produto que estiver em desacordo com as exigências do edital e/ou apresentar irregularidades, no prazo máximo de 10 (dez) dias, após comunicação do SAAE feita via ofício, fac-símile ou e-mail.

6.4. É de inteira responsabilidade do concorrente o preço e demais condições apresentadas, salvo se no momento da abertura da proposta for alegado erro, e aceito pelo Pregoeiro, será registrado em ata, devendo o lote ser desconsiderado da proposta.

6.5. No caso de discordância entre os preços unitários e totais, prevalecerá a soma dos unitários.

6.6. Serão desclassificadas as propostas que conflitem com as normas deste edital ou da legislação em vigor.

6.7. Igualmente serão desclassificadas as propostas que:

6.7.1. Sejam incompletas, isto é, não contenham informação(ões) suficiente(s) que permita(m) a perfeita especificação do material licitado;

6.7.2. Contenham qualquer limitação ou condição substancialmente contrastante com o presente Edital, ou seja, manifestamente inexequíveis, por decisão do Pregoeiro.

6.8. O Município é considerado consumidor final, sendo que o licitante deverá obedecer ao fixado no art. 155, §2º, VII, b, da Constituição Federal de 1988.

7. DO VALOR ESTIMADO:

7.1. O valor estimado para a presente contratação é de **R\$ 23.650,00 (vinte e três mil, seiscentos e cinquenta reais)**.

8. DOS CRITÉRIOS DE JULGAMENTO:

8.1. Para julgamento, será adotado o critério de "MENOR PREÇO GLOBAL", observados os prazos para fornecimento, as especificações técnicas, parâmetros mínimos, qualidade e demais condições definidas neste Edital e seu Anexo I.

8.2. O Pregoeiro anunciará o concorrente detentor da proposta ou lance de menor valor após o encerramento da etapa de lances da sessão pública ou, quando for o caso, após negociação e decisão pelo Pregoeiro acerca da aceitação do lance de menor valor.

8.3. Se a proposta ou o lance de menor valor não for aceitável, o Pregoeiro examinará a proposta ou o lance subsequente, na ordem de classificação, verificando a sua aceitabilidade e procedendo a sua habilitação. Se for necessário, repetirá esse procedimento, sucessivamente, até a apuração de uma proposta ou lance que atenda ao edital.

8.4. Ocorrendo a situação a que se referem os itens 8.2 e 8.3 deste Edital, o Pregoeiro poderá negociar com o concorrente para que seja obtido melhor preço.

8.5. Os concorrentes, ainda que não classificados em primeiro lugar, deverão consultar o sistema regularmente para verificar se passaram à condição de arrematante do lote, em função de desclassificação ou inabilitação do arrematante anterior, podendo o pregoeiro retomar a negociação pelo sistema, e convocá-los a apresentar os documentos de habilitação e demais medidas necessárias.

8.6. Da sessão, o sistema gerará ata circunstanciada, na qual estarão registrados todos os atos do procedimento e as ocorrências relevantes.

8.6.1. Quando necessário o Pregoeiro e a equipe de apoio poderão complementar as informações da ata gerada pelo sistema do Banco do Brasil, por meio de ata interna que será juntada aos autos referente ao certame.

9. DO JULGAMENTO FINAL:

9.1. O(s) licitante(s) que apresentar(em) menor preço, objeto do presente certame, bem como a documentação exigida em ordem, será(ão) considerado(s) vencedor(es).

10. DA HABILITAÇÃO:

10.1. O(s) licitante(s) arrematante(es) deverá(ão) apresentar a documentação abaixo relacionada da seguinte maneira: **digitalizada**, no prazo de até 04 (quatro) horas da confirmação de arrematação, via correio eletrônico para pregoeiro@saaesaocarlos.com.br; **e também os documentos físicos**, por meio dos originais ou de fotocópias autenticadas, no prazo máximo de 02 (dois) dias úteis, no Setor de Contratos e Licitações do SAAE, localizado à Avenida Getúlio Vargas, 1500 - Jardim São Paulo - CEP: 13570-390 - São Carlos - SP, aos cuidados do pregoeiro.

10.1.1. Juntamente com os documentos de habilitação deverá ser apresentada a proposta escrita com o valor atualizado (valor arrematado/negociado), conforme item 6.1.4 do edital.

10.1.2. Deverão também serem apresentadas tabelas das características solicitadas, através de documentos cuja origem seja exclusivamente do fabricante dos produtos, seus catálogos, manuais, ficha de especificações técnicas, informações obtidas em sites oficiais do fabricante ou por meio de declarações do fabricante.

10.1.3. Os documentos relativos à habilitação deverão ser entregues em envelope fechado e poderão ser apresentados em original, por qualquer processo de cópia autenticada por cartório competente ou publicação em órgão da Imprensa Oficial. **No(s) envelope(s) deverá haver a identificação do número do pregão eletrônico, o nome do pregoeiro responsável, bem como os dados da empresa.**

10.2. A participação no presente certame implica no reconhecimento da inexistência de fato impeditivo posterior ou anterior, à expedição dos documentos apresentados para habilitação, observado o disposto no Artigo 43, parágrafo 1º da Lei complementar 123/06.

10.2.1. A comprovação de regularidade fiscal e trabalhista das microempresas e empresas de pequeno porte somente será exigida para efeito de contratação e não como condição para participação no certame. No entanto, deverão elas apresentar todos os documentos referentes à regularidade fiscal e trabalhista, mesmo que apresentem alguma restrição.

10.2.2. Havendo alguma restrição na comprovação de regularidade fiscal e trabalhista de microempresas e empresas de pequeno porte, será assegurado o prazo de 05 (cinco) dias úteis, a contar da data da divulgação do resultado da habilitação, via chat, na página do pregão, para a regularização da documentação, pagamento ou parcelamento do débito e apresentação de eventuais certidões negativas ou positivas com efeito de negativa, após o que, a licitante será declarada vencedora, e dar-se-á início à fase recursal.

10.2.3. A não regularização da documentação, no prazo previsto acima, implicará na decadência do direito à contratação, sem prejuízo das sanções legais, procedendo-se a convocação dos demais licitantes para retomar os atos referentes ao procedimento licitatório.

10.3. Se o licitante desatender as exigências habilitatórias, o pregoeiro examinará a proposta subsequente, verificando a sua aceitabilidade e procederá conforme a ordem de classificação, e assim sucessivamente, até a apuração de uma proposta que atenda ao edital.

10.4. OS DOCUMENTOS DE HABILITAÇÃO SÃO OS SEGUINTEs:

10.4.1 – Habilitação Jurídica:

- a)** Registro comercial, no caso de empresa individual;
- b)** Ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado na Junta Comercial, em se tratando de sociedades comerciais;
- c)** Documentos de eleição dos atuais administradores, tratando-se de sociedades por ações, acompanhados da documentação mencionada na alínea "b", deste subitem;
- d)** Inscrição do ato constitutivo, no caso de sociedades civis, acompanhada de prova de diretoria em exercício;
- e)** Decreto de autorização e ato de registro ou autorização para funcionamento expedido pelo órgão competente, tratando-se de empresa ou sociedade estrangeira em funcionamento no país, quando a atividade assim o exigir.

10.4.2 – Regularidade Fiscal e Trabalhista:

- a)** Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas (CNPJ);
- b)** Prova de inscrição no cadastro de contribuintes estadual ou municipal, relativo ao

domicílio ou sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

c) Prova de Regularidade para com a Fazenda Federal e Prova de Regularidade Relativa à Seguridade Social mediante apresentação de: Certidão Negativa de Débitos Relativos a Tributos Federais e à Dívida Ativa da União, ou Certidão Positiva com Efeitos de Negativa, expedida pela Secretaria da Receita Federal e Procuradoria-Geral da Fazenda Nacional, com validade na data da apresentação, na forma da Lei.

d) Prova de Regularidade para com a Fazenda Estadual: Certidão Negativa de Débitos, ou Certidão Positiva com efeitos de Negativa, com validade na data da apresentação, na forma da lei.

e) Prova de Regularidade para com a Fazenda Municipal: Certidão Negativa de Débitos Mobiliários, ou Certidão Positiva com efeitos de Negativa, do domicílio ou sede do concorrente, ou outra equivalente na forma da Lei, com validade na data da apresentação.

f) Prova de regularidade relativa ao FGTS - (CRF) - Fundo de Garantia por Tempo de Serviço, com validade na data da apresentação.

g) Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante apresentação de Certidão Negativa de Débitos Trabalhistas, em nome do licitante, ou Certidão Positiva com efeitos de Negativa, com validade na data de apresentação, na forma da Lei.

10.4.3 – Capacidade Técnica:

a) Atestado(s) fornecido(s) por pessoa jurídica de direito público ou privado de desempenho anterior que comprove a capacidade para execução do objeto desta licitação, podendo tal comprovação ser efetuada por 01 (um) ou mais atestados, admitindo-se prova de execução similares em quantidades razoáveis, assim, consideradas 50% a 60% do fornecimento pretendido.

Obs.: Nos atestados deverão constar explicitamente as características exigidas, identificação da pessoa jurídica emitente, nome e cargo do signatário, endereço completo do emitente, ou identificação que permita fácil contato para averiguações, e objeto contratual.

10.4.3.1 – Outras declarações:

a) Declaração de que no ato da assinatura do Contrato e/ou emissão do pedido de compras, possuir, no mínimo, um profissional especializado na solução ofertada.

b) Declaração de que concorda e atende integralmente os termos deste edital e seus anexos, sem restrições de qualquer ordem; principalmente no que diz respeito ao prazo de entrega do software, da assistência técnica e de atendimento ao chamado.

c) Declaração do Representante legal é revenda autorizada e está apto a comercializar seus produtos objeto do presente certame, ou, opcionalmente, apresentar documento fornecido ao representante pelo fabricante do Software ou ainda o Certificado de Revenda Autorizada, para o mesmo fim.

Obs.: Estas declarações NÃO fazem parte dos Anexos deste edital.

10.4.4 – Qualificação Econômica Financeira:

a) Certidão Negativa de Falência, expedida pelo distribuidor da sede da pessoa jurídica

com data de expedição não superior a 90 (noventa) dias da data da abertura da licitação. Caso conste no documento a data de validade, esta prevalecerá.

b) Em caso de Recuperação Judicial, deverá ser apresentado o Plano de Recuperação já homologado pelo Juízo competente e em pleno vigor.

10.4.5 – Outras Comprovações:

a) Declaração que de acordo com o Art. 7º inciso XXXIII da Constituição Federal/1988, não emprega menores de 16 anos, salvo na condição de aprendiz, ou menores de 18 anos em trabalho noturno, perigoso ou insalubre, conforme o constante do Anexo III.

b) Declaração de pleno atendimento aos requisitos de habilitação e inexistência de qualquer fato impeditivo à participação, conforme o constante do Anexo IV.

c*) No caso de Microempresa ou Empresa de Pequeno Porte que optar pelos benefícios da Lei Complementar nº 123/06, apresentar declaração de enquadramento nessas situações conforme o constante do Anexo V, e deverá também ser apresentada uma das seguintes comprovações:

1) Quando optante pelo Simples Nacional: comprovante da opção pelo simples obtido no sítio da Secretaria da Receita Federal;

2) Quando não optante pelo Simples Nacional: prova através de documento expedido através da junta comercial ou balanço patrimonial e Demonstração do Resultado do Exercício – DRE, comprovando ter receita bruta dentro dos limites estabelecidos nos incisos I e II, do Artigo 3º, da Lei complementar 123/06;

* A participação nas condições previstas nesta alínea, implica no reconhecimento de não se encontrar em nenhuma das situações previstas no parágrafo 4º do Artigo 3º, da Lei Complementar 123/06.

10.5. Os licitantes cadastrados no SAAE poderão deixar de apresentar os documentos **originais** que já constem do respectivo cadastro (os que ainda estiverem dentro do prazo de validade), devendo os demais ser encaminhados observados os prazos e condições estabelecidos neste edital.

10.6. Os documentos apresentados deverão ser, obrigatoriamente, da mesma sede, ou seja, se da matriz, todos da matriz, se de alguma filial, todos da mesma filial, com exceção dos documentos que são válidos para matriz e todas as filiais.

10.6.1. Caso a licitante pretenda que um de seus estabelecimentos (filiais), que não o participante da licitação, execute o futuro contrato, deverá apresentar toda a documentação de ambos os estabelecimentos na forma e condições previstas neste edital.

10.7. Havendo recurso, o pregoeiro apreciará os mesmos e, caso não reconsidere sua posição, caberá à autoridade máxima competente a decisão em grau final.

10.8. Após a habilitação, poderá a concorrente ser desclassificada por motivo relacionado com a capacidade jurídica, regularidade fiscal, qualificação econômico-financeira, qualificação técnica e/ou inidoneidade, em razão de fatos supervenientes ou somente conhecidos após o julgamento.

10.9. Todos os documentos e certidões deverão ser apresentados dentro do respectivo prazo de validade.

11. DA IMPUGNAÇÃO AO EDITAL E RECURSOS:

11.1. Decairá do direito de impugnação dos termos do Edital de Pregão, perante o SAAE, aquele que não se manifestar até 02 (dois) dias úteis antes da data de abertura da sessão do pregão, apontando as falhas e irregularidade que o viciariam.

11.1.1. A impugnação poderá ser feita através do e-mail: pregoeiro@saaesaocarlos.com.br, devendo conter todos os dados da impugnante (nome, CNPJ, endereço e e-mail) para competente resposta.

11.1.2. A apresentação de impugnação, após o prazo estipulado no subitem anterior, não a caracterizará como recurso, recebendo tratamento como mera informação.

11.2. A sessão pública compreende, sucessivamente, a abertura das propostas, a etapa de lances e a declaração do vencedor.

11.2.1. A declaração do vencedor compreende a análise da proposta e o julgamento de habilitação, de acordo com as exigências previstas neste edital.

11.3. De todos os atos e decisões do Pregoeiro, relacionados ao pregão, cabe recurso;

11.3.1. Depois de declarado o vencedor, no sistema, qualquer concorrente poderá, durante a sessão pública, de forma imediata e motivada, em campo próprio do sistema, manifestar sua intenção de recorrer, com o registro da síntese de suas razões, sendo-lhes facultado apresentar as razões de recurso, no prazo de 03 (três) dias úteis, ficando os demais, desde logo, intimados para, querendo, apresentarem contrarrazões em igual prazo, que começará a contar do término do prazo do recorrente, sendo-lhes assegurada vista dos elementos indispensáveis à defesa dos seus interesses.

11.3.1.1. Encerrada a etapa de lances, os concorrentes deverão consultar regularmente o sistema para verificar se foi declarado o vencedor e se está aberta a opção para interposição de recurso. A partir da liberação, os licitantes terão 24 (vinte e quatro) horas para manifestarem sua intenção de recorrer, com o registro da síntese de suas razões, em campo próprio do sistema.

11.3.1.2. O recurso contra atos e decisões do pregoeiro terá efeito suspensivo e o seu acolhimento importará a invalidação apenas dos atos insuscetíveis de aproveitamento.

11.4. A falta de manifestação imediata e motivada do concorrente quanto à intenção de recorrer, importará na decadência desse direito, ficando o pregoeiro autorizado a adjudicar o objeto ao concorrente declarado vencedor.

11.4.1. Caso a adjudicação ao concorrente vencedor não seja proferida na própria sessão, o prazo de recurso passará a contar a partir da publicação do resultado do certame no Diário Oficial do Município (www.saocarlos.sp.gov.br).

11.5. Os recursos deverão ser endereçados ao SAAE e seu encaminhamento se dará por intermédio do pregoeiro.

11.6. Não serão conhecidos as impugnações e os recursos apresentados fora do prazo legal e/ou subscritos por representante não habilitado ou não identificado no processo para responder pelo concorrente.

11.7. No julgamento da habilitação e das propostas, o pregoeiro 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, inclusive através de verificação junto aos sítios oficiais certificados.

11.8. Cabe, ainda, recurso contra a decisão que:

- a) Anular ou revogar o pregão;
- b) Determinar a aplicação das penalidades de advertência, multa, suspensão temporária do direito de licitar e contratar com o SAAE.

11.8.1. Os recursos de que tratam as letras "a" e "b" do item 11.8 deverão ser interpostos no prazo de 05 (cinco) dias úteis a contar da intimação do ato, e terão efeito suspensivo;

11.8.1.1. A intimação dos atos referidos no item 15 será feita mediante publicação na imprensa oficial e terá efeito suspensivo.

11.8.1.2. Interposto o recurso de que tratam as letras "a" e "b" do item 11.8, será comunicado aos demais concorrentes, que poderão impugná-lo no prazo de 05 (cinco) dias úteis.

11.8.2. Os recursos interpostos fora do prazo não serão conhecidos.

11.8.3. O recurso será dirigido à autoridade superior, por intermédio da que praticou o ato recorrido, a qual poderá reconsiderar a sua decisão, no prazo de 05 (cinco) dias úteis, ou nesse mesmo prazo fazê-lo subir, devidamente informado, devendo, nesse caso, a decisão ser proferida no prazo de 05 (cinco) dias úteis, contado do recebimento do recurso.

12. DA HOMOLOGAÇÃO E CONTRATAÇÃO:

12.1. Decididos os recursos e constatada a regularidade dos atos procedimentais, a autoridade competente homologará os procedimentos licitatórios e adjudicará o objeto ao vencedor.

12.2. Adjudicada a licitação pela autoridade competente, o adjudicatário será convocado para assinar o contrato ou retirar o instrumento equivalente no prazo de 05 (cinco) dias úteis. Caso nos documentos de habilitação não estejam contemplados todos os dados do representante legal que assinará o Contrato, deverá o licitante vencedor encaminhar as informações e comprovações no prazo para entrega dos documentos no original ou cópia autenticada, previsto no item 10.1.

12.3. Como condição para a sua contratação, o concorrente vencedor deverá manter as condições de habilitação, prestar as informações solicitadas pela contratante dentro dos prazos estipulados, bem como não transferir a outrem as obrigações decorrentes desse contrato/instrumento equivalente.

12.4. A obrigação decorrente do fornecimento de bens será firmada entre a Administração e o Fornecedor, por meio de contrato ou instrumento equivalente, observando as condições estabelecidas neste Edital, e na legislação vigente.

12.5. Quando o concorrente vencedor convocado dentro do prazo de validade da sua proposta, não celebrar o contrato/instrumento equivalente ou não apresentar situação regular no ato da assinatura deste, sem motivo justo e aceito pelo Contratante, será facultada a convocação do outro concorrente, observada a ordem de classificação para celebrar o contrato/instrumento equivalente, e assim sucessivamente, sem prejuízo da aplicação das sanções cabíveis.

12.6. O objeto contratual poderá ser acrescido ou reduzido de acordo com o disposto no Art. 65, § 1º, da Lei nº 8.666/93 e alterações posteriores.

13. DO PAGAMENTO:

13.1. Liquidadas as despesas através do recebimento definitivo acompanhado dos documentos exigidos do Edital, será processado o respectivo pagamento.

13.2. O pagamento será efetuado mediante crédito em conta corrente devendo o concorrente informar o número do banco, da agência e conta bancária, ou através de banco credenciado, a critério do SAAE. Não serão aceitos boletos bancários.

13.3. Os pagamentos serão efetuados 30 (trinta) dias corridos contados do recebimento do objeto licitado, acompanhado da Nota Fiscal Fatura, e apresentação dos comprovantes de regularidade perante o INSS e FGTS, desde que devidamente atestado pelo SAAE, através de Termo de Recebimento Provisório/Definitivo (Resolução SAAE 03/2016).

14. DO RECURSO ORÇAMENTÁRIO:

14.1. As despesas decorrentes com a presente aquisição correrão por conta de Dotação Orçamentária nº 060100.1751250012.503 – 33903900, fonte 04.

15. DAS SANÇÕES ADMINISTRATIVAS:

15.1. O licitante que incorrer nas infrações previstas no Artigo 7º da Lei 10.520, de 17 de Julho de 2002, ficará sancionado nos termos abaixo dispostos:

- a)** Apresentar documento falso exigido para o certame: impedimento de contratar com a Administração Pública, por 5 (cinco) anos;
- b)** Ensejar o retardamento da execução do certame, valendo-se de meios ilícitos: impedimento de contratar com o SAAE, por 5 (cinco) anos;
- c)** Não manter a proposta ou não celebrar o contrato ou retirar o instrumento equivalente: impedimento de contratar, por 2 (dois) anos, com o SAAE;
- d)** Falhar na execução do contrato: impedimento de contratar, por 3 (três) anos, com o SAAE;
- e)** Fraudar na execução do objeto contratual: impedimento de contratar, por 5 (cinco) anos, com a Administração Pública;
- f)** Comportar-se de modo inidôneo ou cometer fraude fiscal: impedimento de contratar, por 5 (cinco) anos, com a Administração Pública.

Parágrafo Único: No processo administrativo serão garantidos ampla defesa e o contraditório.

15.2. O licitante sujeitar-se-á, ainda, as sanções de: advertência, multa, impedimento de contratar com declaração de inidoneidade, que poderão ser cumuladas com multa, sem prejuízo da rescisão contratual.

15.3. As multas poderão ser cumulativas, reiteradas e aplicadas em dobro, sempre que se repetir o motivo.

15.4. No descumprimento de quaisquer obrigações licitatórias/contratuais, bem como o descumprimento da regularização no exercício do direito previsto no subitem 10.2.2, poderá ser aplicada multa indenizatória de até 10% (dez por cento) do valor total do objeto licitado.

15.5. As multas serão, após regular processo administrativo, descontadas da(s) fatura(s), cobradas judicialmente ou extrajudicialmente, a critério do SAAE.

15.6. Da intenção de aplicação de quaisquer das penalidades previstas, será concedido prazo para defesa prévia de 05 (cinco) dias úteis a contar da notificação.

15.7. Da aplicação da sanção caberá recurso no prazo de 05 (cinco) dias úteis a contar da publicação no Diário Oficial do Município de São Carlos - SP.

15.8. As penalidades serão obrigatoriamente registradas no Cadastro de Fornecedores do SAAE. No caso de impedimento do direito de licitar e contratar ou declaração inidoneidade, o licitante terá seu cadastro cancelado por igual período.

15.9. A recusa do licitante vencedor em retirar e devolver devidamente assinado o contrato/instrumento equivalente no prazo estabelecido importará na decadência e aplicação de multa correspondente a 10% sobre o valor constante da proposta.

15.10. O Contrato ou documento equivalente poderá ser rescindido nas situações previstas nos artigos 77 e 78 da Lei nº 8.666/93 e alterações posteriores.

16. DAS DISPOSIÇÕES FINAIS:

16.1. A participação do presente certame implica no reconhecimento da inexistência de qualquer fator impeditivo à participação inclusive punição de impedimento ou inidoneidade para licitar e contratar com a Administração Pública.

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

16.3. É facultada ao Pregoeiro, ou à autoridade superior, em qualquer fase da licitação, a promoção de diligência destinada a esclarecer ou complementar a instrução do processo, vedada a inclusão posterior de documento ou informação que deveria constar no ato da sessão pública.

16.4. A autoridade competente para determinar a assinatura do Contrato e posteriores contratações, poderá revogar a licitação em face de razões de interesse público, derivadas de fato superveniente devidamente comprovado, pertinente e suficiente para justificar tal conduta, devendo anulá-la por ilegalidade, de ofício ou por provocação de qualquer pessoa, mediante ato escrito e fundamentado.

16.5. Os licitantes não terão direito à indenização em decorrência da anulação do procedimento licitatório.

16.6. A Administração reserva-se no direito de transferir o prazo para o recebimento e abertura das propostas, descabendo em tais casos, direito à indenização pelos licitantes.

16.7. A participação no presente certame implica em concordância tácita, por parte do licitante, com todos os termos e condições deste Edital e seus Anexos.

16.8. Todos os atos que demandem publicidade em imprensa oficial serão publicados no Diário Oficial do Município de São Carlos, ressalvada a hipótese do art. 21, §4º, da Lei 8.666/93.

16.9. Fica eleito o Foro da Comarca de São Carlos - SP, para dirimir litígios resultantes deste Edital e seus Anexos.

São Carlos, 08 de fevereiro de 2018.

João Carlos Ferreira
Pregoeiro
Portaria nº 059/2017

ANEXO I

TERMO DE REFERÊNCIA

1. OBJETO

1.1. Renovação de licenças existentes e aquisição de novas licenças, instalação, atualização, revisão da instalação operacional e suporte técnico total por 36 (trinta e seis) meses de Solução de Software corporativo para proteção completa contra vírus e códigos maliciosos, contemplando mecanismos de proteção (firewall), detecção de intrusos, controle de dispositivos e aplicações e controle de acesso e transferência de tecnologia do fabricante F-SECURE.

1.2 Divisão de Lotes, Especificações, Quantitativos e Valores Estimados:

LOTE 01				
Item	Descrição dos Materiais	Quant.	Un.	Valor Estimado Total do Item (R\$)
01	Aquisição de Solução de Software corporativo para proteção completa contra vírus e códigos maliciosos, e que contemple mecanismo de proteção (firewall), detecção de intrusos, controle de dispositivos e aplicações, e controle de acesso, além de serviços de instalação e transferência de tecnologia.	200	UN	R\$ 23.650,00
VALOR ESTIMADO TOTAL DO LOTE 01				R\$ 23.650,00

UN= unidade(s).

2. JUSTIFICATIVA

2.1. A justificativa para a renovação e atualização da solução implantada é baseada no alto risco de contaminação da rede por vírus, ransomware, spywares, malwares, adwares, phishing, rootkits, cavalos de tróia, worms, keyloggers, netbots, das variantes de todas essas ameaças e outros tipos de códigos maliciosos desconhecidos que estão sujeitos os computadores da Autarquia e seus clientes, colocando em risco o sigilo, a integridade e a disponibilidade das informações.

2.2. Dessa forma, com o crescimento das demandas dos serviços disponibilizados ao cidadão do município, o SAAE passou a ter que garantir que as unidades atendidas, tenham seus serviços nas melhores condições de uso possíveis.

2.3. Assim para que o sigilo, a integridade e a disponibilidade das informações sejam mantidas, faz-se necessária a renovação e atualização das licenças do referido software para manter a segurança da rede com recursos indispensáveis para tal.

3. REQUISITOS OBRIGATÓRIOS GERAIS

3.1. A proposta comercial deverá conter carta de apresentação em formulário oficial da licitante, em uma via, redigida em português, sem emendas, rasuras, ressalvas ou entrelinhas, assinada e carimbada na última folha e rubricada nas demais pelo seu representante legal. A proposta deve conter:

3.1.1. Todas as comprovações, declarações e especificações técnicas solicitadas neste

termo de referência;

3.1.2. Preço unitário e total de todos os componentes da solução, expressos em algarismos e o total também por extenso, em moeda nacional, a ser cobrado pelo objeto da presente licitação;

3.2. O licitante deverá fornecer em sua proposta todos os software referidos neste termo de referência, sob pena de desclassificação;

3.3. Não serão consideradas, por parte de um mesmo licitante propostas alternativas ou relativas à outra modalidade contratual além da mencionada neste edital;

3.4. Todos os produtos ofertados necessitam ser compatíveis entre si, com a solução implantada e operacional no CONTRATANTE.

3.5. Todos os custos para o funcionamento completo da solução é de responsabilidade da CONTRATADA e obrigatoriamente devem estar relacionados em proposta;

3.6. A proposta deve conter tabela das características solicitadas, através de documentos cuja origem seja exclusivamente do fabricante dos produtos, seus catálogos, manuais, ficha de especificações técnicas, informações obtidas em sites oficiais do fabricante ou por meio de declarações do fabricante.

3.7. As comprovações devem ser claras, com indicação de página na proposta. Serão aceitos documentos escritos em português ou inglês para comprovações técnicas. A não comprovação de alguma característica exigida levará à desclassificação da proposta;

3.8. Deverão ser listados todos os componentes da solução proposta com seus respectivos códigos do fabricante "part number", além de descrição e quantidades dos itens;

3.9. O prazo de validade da proposta deve ser de, no mínimo, 60 (sessenta) dias consecutivos da data da sessão de abertura desta licitação.

4. REQUISITOS DE QUALIDADE

4.1. A licitante vencedora deve possuir no mínimo um profissional especializado na solução ofertada. Deve comprovar competência em instalação e configuração das soluções ofertadas através de atestados de capacidade técnica exigindo-se similaridade pertinente com as tarefas e soluções relacionadas neste termo de referência;

4.2. A renovação das licenças, instalações e atualizações devem ser gerenciadas e monitoradas através de metodologia apropriada, através de representante nomeado como preposto, que fará a interface entre CONTRATADA e CONTRATANTE.

4.3. A CONTRATANTE, em qualquer tempo, reserva-se no direito legal de, em diligências, verificar a autenticidade e veracidade dos atestados apresentados pela licitante.

4.4. Certificações técnicas da solução apresentadas deverão ser obrigatoriamente técnicas e do mesmo fabricante dos produtos cotados;

5. DECLARAÇÕES

5.1. A licitante deve apresentar declarações fazendo constar que:

5.1.1. Concorda e atende integralmente os termos deste edital e seus anexos, sem restrições de qualquer ordem;

5.2. Nos preços cotados já estão incluídas todas e quaisquer despesas necessárias para a perfeita e completa execução do objeto desta licitação, tais como impostos, tributos, fretes e demais despesas inerentes.

5.3. O CONTRATANTE não aceitará cobranças posteriores de qualquer imposto, taxas, tributos ou assemelhado adicional, salvo se alterado ou criado após a data de abertura do certame e que venha expressamente a incidir sobre o objeto, na forma da Lei.

5.4. Na hipótese de redução de alíquota após a apresentação da proposta, a mesma será devidamente considerada por ocasião do pagamento.

5.5. A licitante deve apresentar documento, declarando que:

5.5.1. A prestação do serviço de garantia dos produtos ofertados é de total responsabilidade da CONTRATADA, conforme características especificadas neste termo de referência. A declaração deve informar prazos, acordo de nível de serviço, telefone de contato do suporte técnico, vigência e validade das licenças, localidade e produtos contemplados;

5.6. As novas versões, releases, atualizações e correções da solução ofertada serão disponibilizadas ao CONTRATANTE durante o período de garantia mínimo de 36 (trinta e seis) meses, sem nenhum ônus adicional;

6. ESPECIFICAÇÕES DO OBJETO

6.1. A solução antivírus já implantada e operacional no CONTRATANTE é do fabricante F-SECURE, conceito Client - Server Linux CentOS 6.9 instalado em Servidor Xeon 2,4GHz 8core, 4GB RAM, Hard Disk 200GB, LAN 1Gb/s com seguintes versões instaladas e operacionais:

- F-Secure Client 12.31.105
- F-Secure Client Server 12.11.103
- F-Secure Client (Windows XP) 11.60
- F-Secure Policy Manager 12.40.81.151

6.2. A solução antivírus obrigatoriamente será totalmente compatível com as versões instaladas e operacionais no CONTRATANTE.

6.3. A solução permitirá a administração e gerenciamento centralizado por meio de um único console, sendo que este possa ser estendido para os servidores de segmentos de redes distintas.

7. CARACTERÍSTICAS GERAIS DA SOLUÇÃO

7.1. Todos os componentes que fazem parte da solução, de segurança para servidores e estações de trabalho deverão ser fornecidas por um único fabricante. Não serão aceitas composições de produtos de fabricantes diferentes.

7.2. O conjunto de softwares que compõe a solução de antivírus para servidores e estações de trabalho deverão ser totalmente gerenciáveis através da mesma console de gerenciamento centralizado e de forma que todos os produtos sejam monitorados através desta.

7.3. Fornecer todo o material necessário para a instalação dos produtos solicitados.

7.4. Manuais necessários à instalação, manutenção e utilização da solução, nos seguintes meios: CD e/ou Website em Inglês ou Português do Brasil.

7.5. Apresentação de projeto detalhado do desenho da solução ofertada, abrangendo todo o conjunto de softwares, aplicação e gerenciamento unificado.

7.6. A solução deverá possuir ferramentas de varredura, detecção, análise e remoção de malwares, riskwares, spywares e demais formas de vírus e códigos maliciosos conhecidos, bem como Firewall, IDS/IPS, Controle de Aplicativos e Quarentena de Rede. Estas devem ser totalmente integradas, instaladas através de um único pacote sem a necessidade de instalação de módulos adicionais.

7.7. Solução de monitoramento remoto com utilização de interface gráfica (GUI), para administração, monitoração e gerenciamento da solução ofertada e que seja disponibilizada sua instalação em plataforma Windows e Linux, podendo o administrador escolher a plataforma desejada de acordo com sua necessidade.

7.8. Repositório remoto de distribuição de atualizações da lista de vírus e do mecanismo de varredura (Scan Engine) sem limite de instalações, podendo o administrador instalar quantos necessitar sem ônus com suporte para as plataformas Windows e Linux.

7.9. Prevenção de epidemia manual ou automática.

7.10. A propriedade de todos os componentes da solução passa a ser do (CLIENTE).

- 7.11.** O fabricante do antivírus deve possuir site indicando ameaças de malware presentes mundo em tempo real, através de indicação gráfica e mapa mundial.
- 7.12.** O fabricante deve possuir site próprio para coleta de amostras de arquivos infectados.
- 7.13.** O fabricante deve possuir site próprio para coleta de falsos positivos.
- 7.14.** O fabricante deverá participar do programa "Microsoft Active Protection Program" para obtenção de informações de modo a permitir a criação de regras de proteção antes mesmo dos patches serem publicados pelo fabricante.
- 7.15.** Possuir suporte ao padrão SIEM (Security Information and Event Management).

8. ESPECIFICAÇÕES TÉCNICAS PARA O SOFTWARE DE GERENCIAMENTO CENTRALIZADO PARA TODA A SOLUÇÃO DE SEGURANÇA.

- 8.1.** Possuir gerenciamento e configuração remota para a funcionalidade de controle de dispositivos.
- 8.2.** Possuir gerenciamento e configuração remota para a funcionalidade de antivírus, anti-spyware, detecção de rootkit e proteção de browser.
- 8.3.** Possuir gerenciamento e configuração remota para a funcionalidade de controle de aplicativos e firewall.
- 8.4.** Possuir gerenciamento e configuração remota para a funcionalidade de Zero Hour e/ou Zero Day.
- 8.5.** Possuir gerenciamento e configuração remota para a funcionalidade de Quarentena de rede.
- 8.6.** Gerenciar os produtos antivírus como uma árvore de diretórios parametrizável pelo administrador.
- 8.7.** Agendamento de verificação de comunicação entre o gerenciador e os produtos gerenciados.
- 8.8.** Suportar o gerenciamento acima de 5.000 máquinas a partir de um único servidor.
- 8.9.** Permitir a criação de usuários para acesso à console de gerenciamento, com opção de usuário administrador e usuário para leitura (read only).
- 8.10.** Permitir a criação de usuários com permissão de somente leitura para visualizar subpastas e/ou subdomínios, não acessando outras estruturas de diferente nível hierárquico.
- 8.11.** Permitir a criação de usuários com permissão administrativa para configurar subpastas e/ou subdomínios, não afetando outras estruturas de diferente nível hierárquico.
- 8.12.** Permitir logins simultâneos de usuários administradores ao sistema de gerenciamento da solução.
- 8.13.** Manter um registro de ações realizadas pelos administradores no sistema de gerenciamento da solução de segurança.
- 8.14.** Permitir diferentes níveis de administração do servidor, de maneira independente do login da rede.
- 8.15.** Comunicação segura entre os servidores de gerenciamento e clientes gerenciados através de assinatura digital, com chave pública e privada, permitindo ao administrador escolher entre os protocolos HTTP e HTTPS para a comunicação.
- 8.16.** Detecção de domínios e grupos de trabalho a partir da estrutura de diretórios pré-existentes.
- 8.17.** Importar a estrutura organizacional (OUs) do MS Active Directory para o serviço de gerenciamento da solução de segurança.
- 8.18.** Suporte a NAP (Network Access Protection).
- 8.19.** Atualização de listas, vacinas, mecanismos de rastreamento e desinfecção através da Internet via protocolo HTTP e distribuindo estas para todas as demais ferramentas que compõem a solução de antivírus automaticamente sem a intervenção do administrador.
- 8.20.** As atualizações devem ser incrementais, inclusive o download, este deve ser

gerenciado de forma que baixe somente a parte que lhe falta e do ponto onde foi interrompido.

8.21. Deve suportar conexões DialUp para download de atualizações e detectar quando esta estiver disponível e proceder com o download.

8.22. Deve ter capacidade de ser o repositório central de atualizações, independentemente da plataforma, Microsoft e Linux, repositório de políticas e relatórios sem a necessidade de instalação de software adicional além dos pacotes desenvolvidos pelo fabricante da solução de segurança.

8.23. Permitir a instalação do Antivírus nos clientes a partir de um único servidor de gerenciamento da solução remotamente.

8.24. Permitir a alteração das configurações dos Agentes Antivírus nos clientes de maneira remota.

8.25. Deve ser capaz de bloquear as configurações nas estações de trabalho sem a necessidade de senha, evitando que os usuários alterem as configurações do produto.

8.26. Opção de atualização automática de políticas de prevenção a partir da console de gerenciamento.

8.27. Políticas em caso de epidemia de vírus criando regras de bloqueio contra os ataques até que a vacina seja criada para estações/servidores com plataforma Microsoft e Linux.

8.28. Geração de relatórios que contenham informações sobre as infecções e atualizações da solução.

8.29. Exportar relatórios para os seguintes formatos: HTML, XML e CSV.

8.30. Enviar alertas em caso de epidemias através de e-mail e Popups.

8.31. Permitir a visualização de relatórios contendo as seguintes informações:

8.31.1 Última conexão com o servidor, última política aplicada .

8.31.2 Sumário dos produtos antivírus instalados (com indicação das versões dos módulos instalados).

8.31.3 Top 10 com os de quantidade de infecção.

8.31.4 Histórico de infecções.

8.31.5 Histórico das definições de vacinas.

8.31.6 O módulo IPS deve apresentar o último ataque sofrido, bem como dados sobre a origem do mesmo.

8.31.7 Indicação de hotfixes instalados.

8.31.8 Dados do host (Sistema Operacional e versão do mesmo, WINS Name, DNS Name, IP).

8.32. O armazenamento dos logs, alertas, status e qualquer informação pertinente a solução de segurança deve ser armazenada em um banco de dados. O banco de dados deve ser builtin, parte integrante da solução, além de permitir integração da solução com o banco de dados MySQL.

8.33. Possuir a capacidade de armazenar os eventos em banco de dados centralizado. Se a solução necessitar de um banco de dados proprietário este deverá ser fornecido, devidamente licenciado para a licitante.

8.34. Possibilidade de definir outro navegador de internet que não seja o padrão utilizado, para que o gerenciador do antivírus utilize as configurações desse novo navegador (tais como configurações de proxy).

8.35. Suporte para instalação em plataformas Linux e Microsoft atendendo no mínimo os sistemas operacionais abaixo relacionados:

Microsoft:

- Windows Server 2008 SP1 32-bit, editions: Standard, Enterprise, Web Server
- Windows Server 2008 SP1 64-bit, editions: Standard, Enterprise, Web Server, Small Business Server, Essential Business Server
- Windows Server 2008 R2 with or without SP1, editions: Standard, Enterprise, Web Server
- Windows Server 2012, editions: Essentials, Standard, Datacenter

- Windows Server 2012 R2, editions: Essentials, Standard, Datacenter
- Windows Server 2016, editions: Essentials, Standard, Datacenter
- Linux:
 - Red Hat Enterprise Linux 6 32/64-bit
 - Red Hat Enterprise Linux 5 32/64-bit
 - Red Hat Enterprise Linux 7 32/64-bit
 - CentOS 6 32/64-bit
 - CentOS 7 32/64-bit
 - SUSE Linux Enterprise Server 11 32/64-bit
 - SUSE Linux Enterprise Server 10 32/64-bit
 - SUSE Linux Enterprise Desktop 11 32/64-bit
 - openSUSE Linux 13.2 32/64-bit
 - Debian GNU Linux 7 Wheezy 32/64-bit
 - Debian GNU Linux 8 Jessie 32/64-bit
 - Ubuntu 12.04 (Precise Pangolin) 32/64-bit
 - Ubuntu 14.04 (Trusty Tahr) 32/64-bit
 - Ubuntu 16.04 (Xenial Xerus) 32/64-bit

8.36. O serviço de gerenciamento da solução de segurança deve suportar ser instalado tanto em plataforma Linux como em plataforma Microsoft. Permitindo ao administrador escolher a plataforma em que o serviço de gerenciamento será instalado. o console de gerenciamento também deve suportar ser instalado em plataforma Linux e Microsoft, permitindo ao administrador escolher a plataforma e inclusive utilizar um ambiente misto de administração, como o servidor de gerenciamento em um computador Linux e a console em um computador Microsoft e vice-versa.

8.37. Possuir um dashboard com informações do estado geral da solução de segurança e hosts gerenciados.

8.38. Possuir download direto (a partir da console de gerenciamento) de novas versões do antivírus ou link para página do fabricante para download de novas versões do antivírus durante a vigência da garantia do mesmo, dessa forma mitigando a possibilidade de entrar em falsa página para download de falsas atualizações do antivírus.

8.39. A solicitação de verificação de atualização de vacinas e políticas de segurança deve ser originada a partir da estação de trabalho para servidor de gerenciamento.

8.40. Utilizar protocolo seguro (HTTPS) para consulta/visualização de relatórios.

8.41. Capacidade de gerenciar e aplicar as atualizações de softwares e patches disponibilizados pela Microsoft para seus sistemas operacionais, bem como verificar a disponibilidade de atualizações e correções para softwares de terceiros de forma automática, através de configurações no console de gerenciamento central da solução de proteção para end-points.

8.42. Capacidade de aplicar as atualizações de software, sem a necessidade de intervenção do usuário final.

8.41.1. Aplicar as atualizações e correções de produtos Microsoft e de terceiros mesmo quando o usuário logado não possui privilégios para a tarefa de instalação.

8.41.2. Aplicar as atualizações e correções de produtos Microsoft e de terceiros mesmo quando o computador estiver bloqueado ou quando não houver usuário conectado (em logoff).

8.43. Capacidade de configurar grupos distintos para update de software, dessa forma, podendo marcar quais grupos sofrerão atualização de software e quais não sofrerão atualização de software.

8.44. Gerar alertas sobre atualizações críticas.

8.45. Possibilidade de criar lista de programas para exclusão da verificação da necessidade de atualização de software.

8.46. Possuir controle de conteúdo web, com no mínimo 28 categorias diferentes (nativo, sem necessidade de criar ou customizar nova categoria), entre eles:

- Payment services;
- Scam;

- Illegal downloads;
- Software downloads;
- Streaming media;
- Social Networking;
- Adult;
- Drugs;
- Dating;
- Banking;
- Auctions

O controle de conteúdo deve permitir a configuração por grupos, podendo o administrador determinar, por grupo, quais categorias serão permitidas ou não e se o controle estará ativado para aquele grupo ou não.

8.47. Possuir a funcionalidade de bloqueio de novas conexões, quando for detectado que foi aberta uma conexão bancária e/ou conexão que utilize protocolo seguro.

8.48. Possuir sistema de backup do banco de dados utilizado pelo gerenciador automatizado, com agendamento do backup a ser programado pelo administrador.

9. ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO DE SEGURANÇA PARA ESTAÇÕES DE TRABALHO

9.1. Suporte, no mínimo, aos seguintes sistemas operacionais: Windows Vista 32 e 64 Bits, Windows 7 32 e 64 Bits, Windows 8 32 e 64 Bits, Windows 10, Suse Linux, Debian GNU Linux, Ubuntu, RedHat e CentOS.

9.2. A interface dos clientes anti-vírus e anti-spyware para estações de trabalho deve ter a opção de ser instalada em português do Brasil.

9.3. A solução End-Point Security deve permitir ser instalada, no mínimo, através das seguintes opções:

- Remotamente via push;
- Via política de gerenciamento;
- Via pacote MSI através do MS GPO;
- Através de scripts.

9.4. Permitir instalação "silenciosa".

9.5. Permitir atualizações da versão da solução de segurança (programa end-point security) através de login script, Internet/Intranet, CD-ROM e arquivo off line.

9.6. Permitir instalação remota sem forçar a reinicialização da máquina.

9.7. Agrupar estações de trabalho por domínio ou grupo, ou permitir definir qual domínio ou grupo a estação irá pertencer.

9.8. Configuração diferenciada para cada estação, grupo de estações, domínio ou grupos de domínios.

9.9. Monitoramento e gerenciamento unificados através de uma console centralizada de todos os clientes da rede a partir de um servidor central, possibilitando a criação de configurações específicas para cada cliente ou grupo de clientes, atendendo os requisitos de sistemas operacionais constantes no item 9.1.

9.10. Funcionar tanto no ambiente corporativo (rede interna) como em VPN.

9.11. Atualizar listas de vírus, vacinas e mecanismos de rastreamento automaticamente através de um site local pré-definido ou pela Internet para todos os clientes com plataforma Microsoft e Linux.

9.12. Definir intervalos de tempo para os computadores solicitarem as atualizações podendo este tempo ser definido em minutos, horas e dias.

9.13. O módulo de atualização automática deve suportar serviço de Proxy autenticado.

9.14. Atualização em clientes móveis (LapTops de colaboradores externos e usuários remotos) a partir do site do fabricante do antivírus, ou de outra fonte definida pelo administrador, podendo o administrador definir as fontes de atualização por prioridade. Ex.: Primeiro o servidor de atualizações da rede interna depois o site do fabricante na

internet.

9.15. Capacidade de rastreamento em tempo real, manual ou agendada, tomando as seguintes ações: limpar, apagar, colocar em quarentena o arquivo infectado.

9.16. Permitir que o rastreamento agendado seja configurado pelo administrador da rede, com frequência diária, em horário definido, para todas as estações, para um grupo ou estações específicas.

9.17. Rastreamento manual com interface gráfica em português do Brasil.

9.18. No rastreamento manual, possuir capacidade de limitar número de arquivos a serem verificados simultaneamente.

9.19. Ferramenta integrada ao cliente antivírus que execute rastreamento de tráfego dos protocolos POP3 e SMTP em tempo real, com suporte para todos os clientes de e-mail que utilizem estes protocolos.

9.20. Detecção de cookies potencialmente indesejáveis no sistema.

9.21. Detecção heurística durante a varredura em tempo real, manual e agendada.

9.22. Possuir módulo ZERO DAY, para detecção de ameaças ainda desconhecidas, com opção de inserção de lista de exceções. Para maior segurança, a identificação do arquivo a ser excluído do módulo ZERO DAY deve ser efetuada através de hash.

9.23. Permitir a atualização de um determinado segmento de rede através de uma ou mais estações de trabalho eleitas para serem os repositórios deste seguimento de rede, sem a necessidade de instalação de um módulo adicional nas estações ou servidores para realizar esta tarefa. Esta função deve fazer parte do pacote de instalação padrão do módulo anti-vírus para estações de trabalho, sem a necessidade de instalação de módulo adicional.

9.24. Rastrear arquivos compactados no mínimo nos seguintes formatos: ZIP, ARJ, LZH, RAR, CAB, TAR, BZ2, GZ, JAR e TGZ.

9.25. Criação de uma lista de exclusão de pastas ou arquivos que não devem ser rastreados.

9.26. Possuir módulo Firewall integrado à ferramenta e gerenciado pela mesma console dos módulos anti-vírus e anti-spyware.

9.27. Bloquear em estações com plataforma Microsoft e Linux, portas TCP e UDP comuns e específicas.

9.28. Permitir a criação de serviços que utilizam portas específicas e protocolos TCP e UDP.

9.29. Possuir a funcionalidade de mudança de perfil automático do firewall, de acordo com o ambiente de rede em que o usuário se encontra (ex: Perfil de escritório, perfil de local público, perfil em ambiente residencial, etc.).

9.30. Trabalhar no modo de quarentena permitindo a verificação pelo software de gerenciamento se o cliente está trabalhando com versões desatualizadas das assinaturas de vírus, neste caso, a estação cliente é colocada em quarentena, limitando o acesso a rede desta estação.

9.31. Integração com Microsoft NAP.

9.32. Possuir a Tecnologia de análise DeepGuard ou CloudSecurity de detecção para vírus e ameaças desconhecidas que analisa o comportamento de códigos potencialmente maliciosos dentro de um ambiente virtual seguro de um computador, eliminando os falsos positivos e aumentando as taxas de detecção de malware desconhecidos.

9.33. Possuir módulo para controle de discagens (dialer control) permitindo criar uma lista de telefones permitidos e não permitidos para discagem.

9.34. Possuir módulo de controle de aplicativos, bloqueando aplicativos mesmo se estes tiverem seus nomes alterados pelo usuário e seu gerenciamento através da mesma console de gerenciamento dos módulos antivírus, anti-spyware e firewall.

9.35. Possibilidade de customizar a mensagem de bloqueio e liberação de aplicativos desconhecidos.

9.36. Possibilidade de customizar a mensagem de bloqueio e liberação de aplicativos conhecidos.

- 9.37.** Deve possuir módulo para varredura do tráfego HTTP durante a navegação via browser analisando o tráfego em busca de códigos maliciosos.
- 9.38.** A solução deve possuir a capacidade de bloqueio de URL's, incluindo bloqueio de URL's que utilizem o protocolo HTTPS para navegação.
- 9.39.** A solução deve conter um filtro de reputação WEB, alertando o usuário e bloqueando a página web quando esta for suspeita.
- 9.40.** O filtro de reputação deve identificar durante a pesquisa em sites de busca, no mínimo Google e Yahoo, sites suspeitos, assinalando cada um deles com um carimbo de confiável ou não confiável.
- 9.41.** Gerar notificações para o usuário em caso de detecção de vírus.
- 9.42.** Bloqueio de acesso às funções de configuração da solução de segurança nas estações de trabalho através do uso de senha e política de segurança para bloqueio das funções locais, de forma remota, através da console de gerenciamento. Esta função deve permitir bloquear as configurações locais, por domínio, grupos, subgrupos e hosts específicos.
- 9.43.** Gerar notificações para o administrador de rede quando ocorrer uma epidemia de vírus (outbreak alert) através de e-mail e NT Event Log.
- 9.44.** Bloqueio de acesso às funções de configuração do software nas estações remotas.
- 9.45.** Desinstalar remotamente a solução de antivírus na estação.
- 9.46.** Atualização automática e incremental das listas de vírus.
- 9.47.** Atualização e mudanças de configuração em tempo real através do protocolo http e https com verificação da assinatura digital do pacote de atualização.
- 9.48.** Procurar códigos maliciosos em arquivos potencialmente infectáveis, pelo tipo real de arquivo.
- 9.49.** Proteção e remoção contra spywares em tempo real em plataformas Windows XP / VISTA / WIN7 / WIN8 / WIN10.
- 9.50.** Proteção contra vírus para clientes POP3 durante o acesso ao Servidor de Correio.
- 9.51.** Armazenamento de log de ocorrência de vírus local e no servidor.
- 9.52.** Através do uso de política, impedir a desinstalação não autorizada ou remoção do módulo residente em memória do cliente de antivírus.
- 9.53.** Possuir módulo para bloqueio de dispositivos, permitindo limitar a somente leitura de dispositivos de armazenamento em massa e leitura e escrita.
- 9.54.** Permitir bloquear dispositivos no mínimo pelo Hardware ID, ID do dispositivo, ID compatível e Classe GUID.
- 9.55.** Permitir bloquear dispositivos como, no mínimo, Modems 3G, Dispositivos de armazenamento em massa, câmeras de vídeo embutidas e móveis, mouse com e sem fio, teclados, cd-rom, leitores de cartão, leitores de discos flexíveis (disquetes), discos rígidos (HDs).
- 9.56.** O bloqueio de dispositivos deve permitir bloquear um único dispositivo e liberar todos os demais, bem como liberar um único dispositivo e bloquear os demais. Ex.: Bloquear qualquer Pendrive exceto um em um único computador.
- 9.57.** As regras de bloqueio de dispositivos devem permitir ser aplicadas por grupo, host e todo o domínio.
- 9.58.** Possuir a possibilidade de emitir relatórios com ID de dispositivos anexos ao computador, para eventual bloqueio, sem necessidade de uso de outro software ou necessidade do administrador efetuar consulta ao Windows.
- 9.59.** Possibilidade de emitir relatório de dispositivos presentes no computador, no mínimo com as seguintes informações:
- 9.59.1.** ID do Dispositivo
 - 9.59.2.** Nome do Dispositivo
 - 9.59.3.** ID do Hardware
 - 9.59.4.** ID Compatível
 - 9.59.5.** Classe do Dispositivo
 - 9.59.6.** Estado do dispositivo
- 9.60.** Deve emitir alertas de tentativa de uso do dispositivo bloqueado por ordem do

administrador do sistema, contendo no alerta o ID do dispositivo bloqueado e a identificação da máquina que tentou utilizá-lo;

10. ESPECIFICAÇÃO TÉCNICA DA SOLUÇÃO DE SEGURANÇA PARA SERVIDORES DE REDE

10.1. Suporte para as plataformas:

Microsoft:

- Microsoft Windows Server 2003 32 e 64 bits com ultimo Service Pack.
- Microsoft Windows Server 2003 R2.
- Microsoft Windows 2008 Server 32 e 64 bits.
- Microsoft Windows 2008 Server R2.
- Microsoft Small Business Server 2003.
- Microsoft Small Business Server 2003 R2.
- Microsoft Small Business Server 2008.
- Microsoft Small Business Server 2011 Standard Edition.
- Microsoft Small Business Server 2011 Essentials.
- Microsoft® Windows Server 2012
- Microsoft® Windows Server 2012 Essentials
- Microsoft® Windows Server 2012 R2
- Microsoft® Windows Server 2012 R2 Essentials
- Microsoft® Windows Server 2012 R2 Foundation
- Microsoft® Windows Server 2016 Standard
- Microsoft® Windows Server 2016 Essentials
- Microsoft® Windows Server 2016 Datacenter
- Microsoft® Windows Server 2016 Core (SS/ESS only)

Linux:

- 32 Bits:
 - CentOS 6.7, 6.8
 - Debian 7.10, 7.11
 - Debian 8.5, 8.6
 - Oracle Linux 6.7, 6.8 RHCK
 - Red Hat Enterprise Linux 6.7, 6.8
 - SUSE Linux Enterprise Server 11 SP3, SP4
 - Ubuntu 14.04.(4-5), 16.04, 16.04.1
- 64 Bits:
 - CentOS 6.7, 6.8, 7.1-1503, 7.2-1511
 - Debian 7.10, 7.11
 - Debian 8.5, 8.6
 - Oracle Linux 6.7, 6.8 RHCK
 - Oracle Linux 7.2, 7.3 UEK
 - RHEL 6.7, 6.8, 7.2, 7.3
 - SUSE Linux Enterprise Server 11 SP3, SP4
 - SUSE Linux Enterprise Server 12, 12 SP1
 - Ubuntu 14.04.(4-5), 16.04, 16.04.1

10.2. Ser gerenciado pela mesma ferramenta de gerenciamento da solução de segurança para estações de trabalho.

10.3. A interface dos clientes da solução de segurança para servidores de ser acessível, também, via Browser, através do protocolo HTTPS, de qualquer ponto da rede, acessível somente por usuários com direito de administração.

10.4. Instalação da solução de segurança deve permitir se executada remotamente via push, via política de gerenciamento, via MSI através do MS GPO, no caso de plataforma Microsoft e por scripts e manualmente quando plataforma Linux.

- 10.5.** Permitir instalação "silenciosa".
- 10.6.** Permitir atualizações através de login script, Internet/Intranet, CD-ROM e arquivo off line.
- 10.7.** Permitir instalação remota sem forçar a reinicialização da máquina.
- 10.8.** Bloqueio de acesso às configurações locais do software.
- 10.9.** Agrupar servidores por domínio ou grupo, ou permitir definir qual domínio ou grupo o servidor irá pertencer.
- 10.10.** Configuração diferenciada para cada servidor, grupo de servidores, domínio ou grupos de domínios.
- 10.11.** Monitoramento e gerenciamento unificados através de uma console centralizada de todos os clientes da rede a partir de um servidor central, possibilitando a criação de configurações específicas para cada cliente ou grupo de clientes, atendendo os requisitos de sistemas operacionais constantes no item 10.1.
- 10.12.** Atualizar a lista de vírus, mecanismo de rastreamento, desinfecção automaticamente, a partir de um local específico na rede e site do fabricante na Internet.
- 10.13.** Atualização automática através de serviço de Proxy com e sem necessidade autenticação.
- 10.14.** Realizar rastreamento em tempo real e de forma manual e agendada em todos os servidores da rede.
- 10.15.** Rastreamento em tempo real a ser realizado durante entrada e saída (gravação e leitura) de arquivos no servidor.
- 10.16.** Capacidade de rastreamento em tempo real, manual e agendada, tomando as seguintes ações: limpar, apagar, colocar em quarentena o arquivo infectado.
- 10.17.** Permitir que o rastreamento agendado seja configurado pelo administrador da rede, com frequência diária, em horário definido, para todas as estações, para um grupo e estações específicas.
- 10.18.** Rastreamento manual com interface gráfica para clientes Microsoft e Linux.
- 10.19.** No rastreamento manual, possuir capacidade de limitar número de arquivos a serem verificados simultaneamente.
- 10.20.** Possuir módulo ZERO DAY, para detecção de ameaças ainda desconhecidas, com opção de inserção de lista de exceções. Para maior segurança, a identificação do arquivo a ser excluído do módulo ZERO DAY deve ser efetuada através de hash.
- 10.21.** Possuir a capacidade de detecção e remoção de vírus de macro em tempo real.
- 10.22.** Ferramenta de detecção e remoção de vírus, torjans, spyware e rootkits;
- 10.23.** Rastrear arquivos compactados no mínimo nos seguintes formatos: ZIP, ARJ, LZH, RAR, CAB, TAR, BZ2, GZ, JAR e TGZ.
- 10.24.** Capacidade de procurar códigos maliciosos em arquivos potencialmente infectáveis, pelo tipo real de arquivo.
- 10.25.** Exclusão de pastas e arquivos que não devem ser rastreados.
- 10.26.** Exclusão de extensões de arquivos que não devem ser rastreados.
- 10.27.** Gerar notificações ao administrador de rede e eventos de vírus (notificação e alertas de epidemias) através de e-mail e NT Event Log.
- 10.28.** Gerar relatório de incidente (logs) centralizado.
- 10.29.** Detectar e bloquear conteúdo malicioso (sobre o protocolo HTTP) para fornecer proteção adicional contra malware durante a navegação.
- 10.30.** Prevenir, proteger e alertar contra exploits do navegador web e sites desonestos para usuários locais e remotos (para Windows ou Linux).

11. ESPECIFICAÇÃO TÉCNICA DA SOLUÇÃO DE SEGURANÇA PARA AMBIENTES VIRTUALIZADOS

- 11.1.** Possuir agente para ambientes virtualizados.
- 11.2.** A solução para ambientes virtualizados deve ser compatível, no mínimo, com os sistemas abaixo:
 - VMware vSphere 5.1, 5.5, 6.0
 - Citrix XenServer 6.2, 6.5

- Microsoft Windows Server 2008 R2, 2012 and 2012 R2 with Hyper-V role
- Microsoft Hyper-V Server 2008 R2, 2012 and 2012 R2

11.3. Possuir suporte para estações de trabalho virtuais a partir do sistema operacional Windows XP.

11.4. Possuir suporte para servidores virtualizados a partir do sistema operacional Windows Server 2008 R2.

11.5. Todas as estações de trabalho e servidores virtualizados deverão ser gerenciados pela mesma console de gerenciamento das estações físicas e identificadas individualmente como as demais estações e servidores.

11.6. O content scanner, virtual appliance responsável pela verificação dos arquivos e varredura, deverá ser fornecido sem custos adicionais e sem limites de instalação, permitindo ao administrador instalar quantos virtuais appliances julgar necessário.

11.7. Deve permitir ao administrador instalar vários virtuais appliances para varredura de conteúdo criando um ambiente de alta disponibilidade e balanceamento de carga de acordo com sua necessidade.

11.8. O agente a ser instalado nas estações de trabalho e servidores virtualizados deve ser parte integrante do pacote de instalação destinado às estações de trabalho e servidores físicos, sem a necessidade de um pacote de instalação adicional.

11.9. A comunicação entre os content scanners (virtual appliances) e os agentes deve utilizar protocolo ICAP.

11.10. Verificação dos arquivos deve ser executada exclusivamente nos content scanners, sendo os agentes responsáveis somente pela interceptação e transporte dos dados analisados entre os hosts e os content scanners.

11.11. Nenhuma atividade de varredura (scan) de arquivos deve ser executada nos hosts, somente nos content scanners.

12. QUANTIDADES

12.1. Lote único

12.2. 190 (cento e noventa) Licenças para desktop Microsoft Windows.

12.3. 10 (dez) Licenças para servidores Microsoft Windows Server.

13. SUPORTE TÉCNICO, MANUTENÇÃO E GARANTIA

13.1. O tempo mínimo de duração do suporte técnico e atualizações será de 36 (trinta e seis) meses contados a partir da assinatura do contrato;

13.2. A contratação dará direito a todos os upgrades de versão, atualizações, firmwares e patches de correção de software obtidos através de download junto ao fabricante do software através de acesso nomeado ao site da fabricante;

13.3. O CONTRATADO fica responsável por monitorar o lançamento de novas versões pelo fabricante da solução, sugerindo e planejando junto ao CONTRATANTE a atualização quando esta contemplar os termos da contratação.

13.3.1. O CONTRATADO, durante o período de validade do contrato, fica responsável por alertar sobre ataques massivos de pragas virtuais, sempre alertando o CONTRATANTE sobre tais ameaças.

13.4. Durante todo o período contratual o serviço de suporte técnico da CONTRATADA estará disponível no regime 5x8 (oito horas por dia, cinco dias por semana, no horário comercial) para a solução adquirida.

13.5. Os chamados técnicos da CONTRATANTE serão registrados e gerenciados pelo CONTRATADO, através de contato telefônico ou e-mail, fornecendo no ato da abertura o número, a data e hora de abertura do chamado técnico. Estes dados serão considerados para o início da contagem dos prazos estabelecidos no item 7.6.;

13.6. O tempo de resposta de solicitação de chamado técnico, estabelecido no item 7.5. será de até 2 (duas) horas para todos os componentes da solução adquirida;

13.7. A CONTRATADA permitirá a abertura de chamados por até 02 (dois) profissionais

nomeados da CONTRATANTE;

14. SERVIÇOS DE INSTALAÇÃO E CONFIGURAÇÃO

14.1. Antes do início dos trabalhos, a CONTRATANTE agendará uma reunião com a equipe técnica da CONTRATADA. Serão apresentados todos os aspectos do atual cenário, incluindo as correções necessárias, configurações e políticas implantadas. Novas reuniões poderão ser convocadas por ambas as partes de modo a eliminar pendências.

14.2. Deverá ser apresentado pela CONTRATADA um plano básico de execução dos serviços, detalhando responsáveis e prazos, além de previsão de eventos e seus impactos na infraestrutura existente.

14.3. As instalações, atualizações e correções do ambiente operacional deverão ser efetuadas de forma a não paralisar totalmente o funcionamento dos sistemas, recursos ou equipamentos atualmente em operação e nem impedir ou interromper, por períodos prolongados (> 4 horas), a rotina de trabalho da CONTRATANTE.

14.4. Para tanto, quando da necessidade de interrupção, o serviços deverão ser executados preferencialmente fora do horário comercial (períodos noturnos e finais de semana), em horários previamente agendados com a CONTRATANTE.

14.5. No caso de necessidade de interrupção dos sistemas, recursos, equipamentos ou rotinas de trabalho de qualquer setor funcional em decorrência da instalação a ser efetuada, esta parada, será planejada antecipadamente junto ao CONTRATANTE;

14.6. Todos os componentes da solução, requeridos para atender as funcionalidades exigidas neste termo de referência, devem obrigatoriamente tornar a solução imediatamente operacional, mesmo que não tenham sido especificados e cotados na proposta apresentada. São consideradas partes integrantes dos serviços de instalação e deverão ser fornecidos pela CONTRATADA.

14.7. Quando da viabilidade, o suporte técnico, as instalações, atualizações e correções do ambiente operacional poderão ser executadas remotamente pelo CONTRATADO.

15. RESPONSABILIDADES DA CONTRATADA

15.1. Desenvolver e apresentar planejamento, indicando as atividades que serão realizadas;

15.2. Apresentar toda e qualquer documentação pertinente solicitada pelo CONTRATANTE.

16. DEFINIÇÃO E REQUISITOS DE IMPLANTAÇÃO

16.1. Revisão, atualização e operacionalização de toda solução operacional contratada;

16.2. Apresentar testes de funcionamento completo e homologação da solução;

16.3. Instalação de softwares de gerenciamento, quando disponíveis e/ou solicitados, em estações de gerenciamento;

16.4. Revisão pela CONTRATADA das políticas implantadas de acordo com as recomendações do fabricante da solução e normas internas do CONTRATANTE;

16.5. Revisão e/ou redefinição das políticas e estatísticas de backup implantadas bem como jobs e fluxos de informações da solução;

16.6. Apresentação de documentação com melhores práticas, testes e manutenção do ambiente operacional;

16.7. Apresentação e customização de relatórios e alertas.

17. DOCUMENTAÇÃO

17.1. Ao final dos trabalhos de atualização, a CONTRATADA entregará toda a documentação técnica pertinente ao CONTRATANTE no formato eletrônico, onde constará:

17.1.1. Definições, políticas e procedimentos estabelecidos;

17.1.2. Funcionamento, composição, características e arquitetura da solução;

17.1.3. Procedimentos de configuração para todas as funcionalidades suportadas pela

solução;

17.1.4. Procedimentos de resolução de problemas da solução;

17.1.5. Procedimentos de substituição, remoção ou adição do componente;

17.1.6. Procedimentos de atualização de versão ou do firmware da solução;

17.1.7. Documentação oficial do fabricante validando as licenças adquiridas e suas respectivas validades;

18. PRAZOS

18.1. O prazo para conclusão dos serviços e entrega da documentação será de até 45 (quarenta e cinco) dias corridos após a assinatura do contrato/emissão do pedido de compras.

19. SITUAÇÕES NÃO PREVISTAS NESTE TERMO DE REFERÊNCIA

19.1. Situações não previstas ou especificadas neste Termo de Referência, quando da necessidade, serão tratadas e solucionadas pontualmente pautando-se no edital e na Lei Federal nº 8.666, de 1993, exclusivamente dentro do interesse público do município.

19.2. Não serão aceitas adaptações, substituições de serviços ou especificações fora do escopo estabelecido neste Termo de Referência, salvo expressa justificativa e posterior autorização do CONTRATANTE.

19.3. Toda e qualquer mudança nos dispositivos legais municipais, estaduais ou federais, relativos e pertinentes às demandas especificadas e contratadas, devem ser atendidas, acatadas e implantadas pelo CONTRATADO dentro do prazo estabelecido por lei.

ANEXO II

MODELO DE PROPOSTA DE PREÇOS
Pregão Eletrônico nº ____/2018

Ao SAAE - SERVIÇO AUTÔNOMO DE ÁGUA E ESGOTO DE SÃO CARLOS - SP.

Prezados Senhores:

A EMPRESA _____, com endereço na Rua _____, nº _____, na cidade de _____, (UF), telefone para contato (DDD) _____, e-mail: _____, neste ato representada pelo seu (sócio/diretor/proprietário), _____, portador do RG nº _____ e CPF nº _____, inscrita no CNPJ/MF nº _____, Inscrição Estadual nº _____ e Inscrição Municipal nº _____, tendo examinado minuciosamente o Edital em epígrafe e seus Anexos e, com o conhecimento das condições estabelecidas, reconhecendo a inexistência de fato impeditivo, formula a seguinte PROPOSTA:

LOTE _____						
ITEM	DESCRIÇÃO	QT.	UN.	MARCA	PREÇO UNIT.	PREÇO TOTAL
VALOR TOTAL DO LOTE _____						
VALOR TOTAL DA PROPOSTA: R\$ _____						
Preço total por extenso:						
Prazo de entrega:						
Garantia dos materiais:						
Validade da Proposta:						
Condições de Pagamento:						
Nome do Banco, Ag. e nº C/Corrente:						

Obs.: Nos preços estão inclusos quaisquer ônus tais como, tributos, taxas administrativas, impostos, fretes, seguros e demais encargos, despesas com entrega dos valores dos materiais, da mão de obra utilizada, dos veículos, equipamentos, dos encargos sociais e fiscais, das ferramentas, aparelhos, instrumentos, da água e energia elétrica, da segurança e vigilância, dos ônus diretos e indiretos, da administração, do lucro e de quaisquer outras despesas incidentes sobre os serviços, e outras necessárias à perfeita execução do objeto.

Declaramos que, esse fornecimento será efetuado em conformidade com as condições constantes do Edital de Pregão na forma Eletrônica nº _____/2018 e seus anexos, o qual conhecemos e aceitamos em todos os seus termos.

Declaramos ainda que o representante legal de nossa empresa que assinará o Contrato ou instrumento equivalente é o(a) Sr.(a) _____ portador(a) do RG nº _____ e do CPF nº _____.

Local, _____ de _____ de 2018

Assinatura/Nome/Cargo

ANEXO III

**DECLARAÇÃO DE ADEQUAÇÃO AO ARTIGO 7º
INCISO XXXIII DA CONSTITUIÇÃO FEDERAL**

(Nome da empresa), CNPJ nº _____, sediada (endereço completo), por seu representante legal, abaixo subscrito, DECLARA EXPRESSAMENTE que não emprega menor de dezoito anos em trabalho noturno, perigoso ou insalubre; bem como não emprega menor de dezesseis anos ou o emprega na condição de aprendiz e, ainda não emprega, em hipótese alguma, menor de quatorze anos.

Local e data

Nome do representante legal
RG nº.....

ANEXO IV

DECLARAÇÃO DE INEXISTÊNCIA DE FATO IMPEDITIVO

Eu _____(nome completo), RG nº _____, representante legal da _____(denominação da empresa jurídica), CNPJ nº _____ DECLARO, sob as penas da lei, que a empresa cumpre plenamente as exigências e os requisitos de habilitação previstos no instrumento convocatório do Pregão nº _____/2018, realizado pelo Serviço Autônomo de Água e Esgoto de São Carlos, inexistindo qualquer fato impeditivo de sua participação neste certame, estando ciente da obrigatoriedade de declarar ocorrências posteriores.

Local e data

Nome do representante legal
RG nº.....

ANEXO V

DECLARAÇÃO DE MICROEMPRESA OU EMPRESA DE PEQUENO PORTE

Para fins de participação no Pregão Eletrônico _____ (indicar o nº do Edital), a(o) _____ (nome completo do proponente), CNPJ _____, sediada(o) _____ (endereço completo), DECLARA, sob as penas da lei, que cumpre os requisitos legais para a qualificação como _____ (Microempresa ou Empresa de Pequeno Porte, conforme o caso), na forma da Lei Complementar nº 123/2006, estando apta a usufruir do tratamento favorecido estabelecido nos arts. 42 a 49 daquela Lei Complementar.

DECLARA, ainda, que não existe qualquer impedimento entre os previstos nos incisos do § 4º do artigo 3º da Lei Complementar nº 123/2016.

Local e data

Nome do representante legal
RG nº.....

ANEXO VI

TERMO DE CIÊNCIA E NOTIFICAÇÃO

CONTRATANTE: SERVIÇO AUTÔNOMO DE ÁGUA E ESGOTO DE SÃO CARLOS - SAAE

CONTRATADA: _____

CONTRATO Nº: _____/2018

OBJETO: aquisição de Solução de Software corporativo para proteção completa contra vírus e códigos maliciosos, em conformidade com o Edital de Pregão Eletrônico nº _____/2018 e seus Anexos.

ADVOGADOS: (*) _____

Na qualidade de Contratante e Contratado, respectivamente, do Termo acima identificado, e, cientes do seu encaminhamento ao TRIBUNAL DE CONTAS DO ESTADO, para fins de instrução e julgamento, damo-nos por CIENTES e NOTIFICADOS para acompanhar todos os atos da tramitação processual, até julgamento final e sua publicação e, se for o caso e de nosso interesse, para, nos prazos e nas formas legais e regimentais, exercer o direito da defesa, interpor recursos e o mais que couber.

Outrossim, estamos CIENTES, doravante, de que todos os despachos e decisões que vierem a ser tomados, relativamente ao aludido processo, serão publicados no Diário Oficial do Estado, Caderno do Poder Legislativo, parte do Tribunal de Contas do Estado de São Paulo, de conformidade com o artigo 90 da Lei Complementar Estadual nº 709, de 14 de janeiro de 1993, precedidos de mensagem eletrônica aos interessados.

São Carlos, ____ de _____ de 2018.

CONTRATANTE:

Nome e cargo:

E-mail institucional

E-mail pessoal:

Assinatura:

CONTRATADA:

Nome e cargo:

E-mail institucional:

E-mail pessoal:

Assinatura:

() Facultativo. Indicar quando já constituído.*