EDITAL DE PREGÃO ELETRÔNICO SEADE n.º 017/2016
EXPEDIENTE SEADE n.º 085/2016
ENDEREÇO ELETRÔNICO:www.bec.sp.gov.br ou www.bec.fazenda.sp.gov.br
DATA DO INÍCIO DO PRAZO PARA ENVIO DA PROPOSTA ELETRÔNICA: 05/09/2016
DATA E HORA DA ABERTURA DA SESSÃO PÚBLICA: 16/09/2016 às 10:00 horas
OFERTA DE COMPRA: 291201290482016OC00060

A **FUNDAÇÃO SISTEMA ESTADUAL DE ANÁLISE DE DADOS – SEADE**, por sua Diretoria Executiva, no uso da competência delegada pelos artigos 3° e 7°, inciso I, do Decreto estadual n° 47.297, de 06 de novembro de 2002, c.c. artigo 8°, do Decreto Estadual n° 49.722, de 24 de junho de 2005, torna público que se acha aberta, nesta unidade, licitação na modalidade PREGÃO, a ser realizada por intermédio do sistema eletrônico de contratações denominado "Bolsa Eletrônica de Compras do Governo do Estado de São Paulo – Sistema BEC/SP", com utilização de recursos de tecnologia da informação, denominada **PREGÃO ELETRÔNICO**, do tipo **MENOR PREÇO** – **Expediente Seade nº 085/2016**, objetivando a contratação de empresa para **fornecimento de 360 (trezentos e sessenta) licenças de software antivírus, com suporte técnico do fabricante pelo período de 12 (doze) meses,** conforme Termo de Referência e nas condições deste Edital, **sob o regime de empreitada por preço unitário**, que será regida pela Lei Federal nº. 10.520, de 17 de julho de 2002, pelo Decreto n° 49.722, de 24 de junho de 2005, pelo regulamento anexo a Resolução n° CC-27, de 25/05/2006 e Resolução CC-52 de 26/11/2009, Decreto nº 55.938 de 21 de junho de 2010, aplicando-se, subsidiariamente, no que couberem, às disposições da Lei Federal nº 8.666, de 21 de junho de 1993 e suas alterações, da Lei Estadual nº 6.544, de 22 de novembro de 1989, do Decreto Estadual n° 47.297, de 06 de novembro de 2002, da Resolução CEGP-10, de 19 de novembro de 2002, Lei Estadual nº 13.122 de julho de 2008, Decreto Estadual nº 55.126, de 07/12/2009, alterado pelo Decreto Estadual nº 56.290, de 15/10/2010 e demais normas regulamentares aplicáveis à espécie.

As propostas deverão obedecer às especificações deste instrumento convocatório e seus anexos e serão encaminhadas por meio eletrônico após o registro dos interessados em participar do certame e o credenciamento de seus representantes, no Cadastro Unificado de Fornecedores do Estado de São Paulo - CAUFESP.

A sessão pública de processamento do Pregão Eletrônico será realizada no endereço eletrônico www.bec.sp.gov.br ou www.bec.fazenda.sp.gov.br , no dia e hora mencionados no preâmbulo deste Edital e será conduzida pelo pregoeiro com o auxílio da equipe de apoio, designados nos autos do processo em epígrafe e indicados no sistema pela autoridade competente.

I. DO OBJETO

A presente licitação tem por objeto a contratação de empresa para fornecimento de 360 (trezentos e sessenta) licenças de software antivírus, com Suporte Técnico do fabricante pelo período de 12(doze) meses**,** incluindo a implantação, a configuração e o treinamento do novo software, conforme especificações constantes do **Termo de Referência** que integra este edital, como Anexo I.

II. DA PARTICIPAÇÃO

1. Poderão participar do certame todos os interessados em contratar com a Administração Estadual que estiverem registrados no Cadastro Geral de Fornecedores do Estado de

São Paulo, em sua versão web CAUFESP, em atividade econômica compatível com o seu objeto, sejam detentores de senha para participar de procedimentos eletrônicos e tenham credenciado os seus representantes, na forma estabelecida no regulamento que disciplina a inscrição no referido cadastro.

1.1. O registro no CAUFESP, o credenciamento dos representantes que atuarão em nome da licitante no sistema de pregão eletrônico e a senha de acesso, deverão ser obtidos anteriormente à abertura da sessão pública e autorizam a participação em qualquer pregão eletrônico realizado por intermédio do Sistema BEC/SP.

1.2. As informações a respeito das condições exigidas e dos procedimentos a serem cumpridos, para o registro no CAUFESP, para o credenciamento de representantes e para a obtenção de senha de acesso, estão disponíveis no endereço eletrônico **www.bec.sp.gov.br** ou **www.bec.fazenda.sp.gov.br**

2. A participação no certame está condicionada, ainda, a que o interessado ao acessar, inicialmente, o ambiente eletrônico de contratações do Sistema BEC/SP, declare, mediante assinalação nos campos próprios, que inexiste qualquer fato impeditivo de sua participação no certame ou de sua contratação, que conhece e aceita os regulamentos do Sistema BEC/SP, relativos a Dispensa de Licitação, Convite e Pregão Eletrônico.

3. A licitante responde integralmente por todos os atos praticados no pregão eletrônico, por seus representantes devidamente credenciados, assim como pela utilização da senha de acesso ao sistema, ainda que indevidamente, inclusive por pessoa não credenciada como sua representante.

4. Cada representante credenciado poderá representar apenas uma licitante, em cada pregão eletrônico.

5. O envio da proposta vinculará a licitante ao cumprimento de todas as condições e obrigações inerentes ao certame.

6. Para o exercício do direito de preferência de que trata o subitem 6, bem como para a fruição do benefício da habilitação com irregularidade fiscal previsto na alínea "f", do subitem 9, ambos do item V deste edital, a condição de microempresa, empresa de pequeno porte ou cooperativa, que preencha as condições estabelecidas no artigo 34, da Lei federal n° 11.488, de 15/06/2007, deverá constar do registro da licitante junto ao CAUFESP.

III - DAS PROPOSTAS

1. As propostas deverão ser enviadas por meio eletrônico disponível no endereço www.bec.sp.gov.br ou www.bec.fazenda.sp.gov.br na opção PREGAO–ENTREGAR PROPOSTA, desde a divulgação da íntegra do edital no referido endereço eletrônico, até o dia e horário previstos no preâmbulo, devendo a licitante, para formulá-las, assinalar a declaração de que cumpre integralmente os requisitos de habilitação constantes do edital.

2. A proposta comercial a ser apresentada, em conformidade com o **Anexo II** deste Edital, deverá conter os **valores unitários e total.**

3. O prazo de validade da proposta será de 60 (sessenta) dias.

4. Não será admitida cotação inferior à quantidade prevista neste Edital.

5. A proposta de preço deverá ser orçada em valores vigentes à data de sua apresentação, que será considerada a data de referência de preços.

IV - DA HABILITAÇÃO

1. O julgamento da habilitação se processará na forma prevista no subitem 9, do item V, deste Edital, mediante o exame dos documentos a seguir relacionados, os quais dizem respeito a:

1.1. HABILITAÇÃO JURÍDICA

a) Registro empresarial na Junta Comercial, no caso de empresário individual (ou cédula de identidade em se tratando de pessoa física não empresária);

b) Ato constitutivo, estatuto ou contrato social atualizado e registrado na Junta Comercial, em se tratando de sociedade empresária ou cooperativa;

c) Documentos de eleição ou designação dos atuais administradores, tratando-se de sociedades empresárias ou cooperativas;

d) Ato constitutivo atualizado e registrado no Registro Civil de Pessoas Jurídicas tratando-se de sociedade não empresária, acompanhado de prova da diretoria em exercício;

e) Decreto de autorização em se tratando de sociedade empresária estrangeira em funcionamento no País, e ato de registro ou autorização para funcionamento expedido pelo órgão competente, quando a atividade assim o exigir;

f) Em se tratando de cooperativas, registro da sociedade cooperativa perante a entidade estadual da Organização das Cooperativas Brasileiras, nos termos do artigo 107 da Lei Federal nº 5.764, de 14 de julho de 1971, e em atendimento ao disposto no artigo 1º, §2º, do Decreto estadual nº 57.159, de 21 de julho de 2011.

1.2. REGULARIDADE FISCAL

a) Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas do Ministério da Fazenda (CNPJ) ou no Cadastro de Pessoas Físicas (CPF);

b) Prova de inscrição no Cadastro de Contribuintes Estadual e/ou Municipal, relativo à sede da licitante, pertinente ao seu ramo de atividade e compatível com o objeto do certame;

c) Certidão de regularidade de débito com as Fazendas Estadual e Municipal, da sede ou domicílio da licitante;

d) Certidão de regularidade de débito para o Fundo de Garantia por Tempo de Serviço (FGTS);

e) Certidão Conjunta Negativa de Débitos ou Positiva com efeitos de Negativa, relativos aos Tributos Federais e Dívida Ativa da União incluindo o Sistema de Seguridade Social (INSS) (Portaria Conjunta RFB/PGFN nº 1751 de 02/10/2014).

1.2.1 Se os serviços objeto desta licitação vierem a ser realizados por filial, os documentos relacionados neste subitem deverão ser dessa filial;

1.3. QUALIFICAÇÃO ECONÔMICO-FINANCEIRA

a) Certidão Negativa de Falência e Concordata, Recuperação Judicial e Extrajudicial expedida pelo distribuidor da sede da pessoa jurídica, ou de execução patrimonial, expedida pelo distribuidor do domicílio da pessoa física.

a.1) Se a licitante for cooperativa, a certidão mencionada na alínea "a", deste subitem 1.3, deverá ser substituída por certidão negativa de ações de insolvência civil.

1.4. REGULARIDADE TRABALHISTA

a) Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante apresentação de Certidão Negativa ou Positiva com efeitos de Negativa, de Débitos Trabalhistas – CNDT.

1.5. OUTRAS COMPROVAÇÕES

1.5.1. Declarações subscritas por representante legal da licitante, de acordo com os Anexos IV a VII, elaboradas em papel timbrado, atestando que:

a) se encontra em situação regular perante o Ministério do Trabalho, conforme modelo anexo ao Decreto Estadual n° 42.911, de 06/03/1998;

b) inexiste impedimento legal para licitar ou contratar com a Administração, inclusive em virtude das disposições da Lei Estadual nº 10.218 de 12 de fevereiro de 1999.

c) atende às normas relativas à saúde e segurança do trabalho (parágrafo único, art. 117, Constituição do Estado).

d) não tem dúvidas com relação à interpretação dos detalhes construtivos e das recomendações das especificações contidas no Projeto Básico do presente Edital.

2. DISPOSIÇÕES GERAIS

2.1. Na hipótese de não constar prazo de validade nas certidões apresentadas, a Administração aceitará como válidas as expedidas até 180 (cento e oitenta) dias imediatamente anteriores à data de apresentação das propostas.

V – DA SESSÃO PÚBLICA E DO JULGAMENTO

1. No dia e horário previstos neste edital, o Pregoeiro dará início à sessão pública do pregão eletrônico, com a abertura automática das propostas e a sua divulgação, pelo sistema, na forma de grade ordenatória, em ordem crescente de preços.

2. A análise das propostas pelo Pregoeiro, visará o atendimento das condições estabelecidas neste Edital e seus anexos.

2.1. Serão desclassificadas as propostas:

a) cujo objeto não atenda as especificações, prazos e condições fixados no Edital;

b) que apresentem preço baseado exclusivamente em proposta das demais licitantes;

c) que por ação da licitante ofertante, contenha elementos que permitam a sua identificação.

2.1.1. A desclassificação se dará por decisão motivada do Pregoeiro.

2.2. Serão desconsideradas ofertas ou vantagens baseadas nas propostas das demais licitantes.

2.3.O eventual desempate de propostas do mesmo valor, será promovido pelo sistema, com observância dos critérios legais estabelecidos para tanto.

3. Nova grade ordenatória será divulgada pelo sistema, contendo a relação das propostas classificadas e das desclassificadas.

4. Será iniciada a etapa de lances, com a participação de todas as licitantes detentoras de propostas classificadas.

4.1. A formulação de lances será efetuada, exclusivamente, por meio do sistema eletrônico.

4.1.1. Os lances deverão ser formulados em valores distintos e decrescentes, inferiores à proposta de menor preço, ou em valores distintos e decrescentes inferiores ao último valor apresentado pela própria licitante ofertante, observando, em ambos os casos, a redução mínima entre eles de **R$ 500,00 (quinhentos reais),** aplicável, inclusive, em relação ao primeiro formulado, prevalecendo o primeiro lance recebido, quando ocorrerem 2 (dois) ou mais lances do mesmo valor.

4.1.1.1. A aplicação do valor de redução mínima entre os lances incidirá sobre o **valor total.**

4.2. A etapa de lances terá a duração de 15 (quinze) minutos.

4.2.1. A duração da etapa de lances será prorrogada automaticamente pelo sistema, visando a continuidade da disputa, quando houver lance admissível ofertado nos 03 (três) minutos do período de que trata o subitem 4.2 ou nos sucessivos períodos de prorrogação automática.

4.2.1.1. Não havendo novos lances ofertados nas condições estabelecidas no subitem 4.2.1, a duração da prorrogação encerrar-se-á, automaticamente, quando atingido o terceiro minuto contado a partir do registro no sistema, do último lance que ensejar prorrogação.

4.3. No decorrer da etapa de lances, as licitantes serão informadas pelo sistema eletrônico:

a) dos lances admitidos e dos inválidos, horários de seus registros no sistema e respectivos valores;

b) do tempo restante para o encerramento da etapa de lances.

4.4. A etapa de lances será considerada encerrada, findos os períodos de duração indicados no subitem 4.2.

5. Encerrada a etapa de lances, o sistema divulgará a nova grade ordenatória, contendo a classificação final, em ordem crescente de valores.

5.1. Para essa classificação, será considerado o último preço ofertado, por licitante.

6. Com base na classificação a que alude o subitem 5 deste item, será assegurada às licitantes microempresas, empresas de pequeno porte e cooperativas que preencham as condições estabelecidas no artigo 34, da Lei Federal nº 11.488, de 15/06/2007, preferência à contratação, observadas as seguintes regras:

6.1. A microempresa, empresa de pequeno porte ou cooperativa que preencha as condições estabelecidas no artigo 34, da Lei Federal nº 11.488, de 15/06/2007, detentora da proposta de menor valor, dentre aquelas cujos valores sejam iguais ou superiores até 5% (cinco por cento) ao valor da proposta melhor classificada, será convocada pelo pregoeiro, para que apresente preço inferior ao da melhor classificada, no prazo de 5 (cinco) minutos, sob pena de preclusão do direito de preferência.

6.1.1. A convocação recairá sobre a licitante vencedora de sorteio, no caso de haver propostas empatadas nas condições do subitem 6.1;

6.2. Não havendo apresentação de novo preço, inferior ao preço da proposta melhor classificada, serão convocadas para o exercício do direito de preferência, respeitada a ordem de classificação, as demais microempresas, empresas de pequeno porte e cooperativas que preencham as condições estabelecidas no artigo 34, da Lei Federal nº 11.488, de 15/06/2007, cujos valores das propostas se enquadrem nas condições indicadas no subitem 6.1.

6.3. Caso a detentora da melhor oferta, de acordo com a classificação de que trata o subitem 5, seja microempresa, empresa de pequeno porte, ou cooperativa que preencha as condições estabelecidas no artigo 34, da Lei Federal nº 11.488, de 15/06/2007, não será assegurado o direito de preferência, passando-se, desde logo, à negociação do preço.

7. O Pregoeiro poderá negociar com o autor da oferta de menor valor, obtida com base nas disposições dos subitens 6.1 e 6.2, ou, na falta desta, com base na classificação de que trata o subitem 5, mediante troca de mensagens abertas no sistema, com vistas à redução do preço.

8. Após a negociação, se houver, o Pregoeiro examinará a aceitabilidade do menor

preço, decidindo, motivadamente, a respeito.

8.1. O critério de aceitabilidade dos preços ofertados será o de compatibilidade com os preços de mercado vigentes, apurados mediante pesquisa realizada pelo órgão licitante, conforme Decreto nº 34.350/91.

8.2. O Pregoeiro poderá a qualquer momento solicitar às licitantes a composição de preços unitários de serviços e/ou de materiais/equipamentos, bem como os demais esclarecimentos que julgar necessário.

9. Considerada aceitável a oferta de menor preço, passará o Pregoeiro ao julgamento da habilitação, observando as seguintes diretrizes:

a) A verificação dos dados e informações do autor da oferta aceita, constantes do CAUFESP e extraídos dos documentos indicados no item IV deste edital;

b) Caso os dados e informações constantes no CAUFESP, não atendam aos requisitos estabelecidos no item IV deste Edital, o Pregoeiro verificará a possibilidade de suprir ou sanear eventuais omissões ou falhas, mediante consultas efetuadas por outros meios eletrônicos hábeis de informações.

b.1) Essa verificação será certificada pelo Pregoeiro na ata da sessão pública, devendo ser anexados aos autos, os documentos passíveis de obtenção por meio eletrônico, salvo impossibilidade devidamente certificada e justificada.

c) A licitante poderá, ainda, suprir ou sanear eventuais omissões ou falhas, relativas ao cumprimento dos requisitos e condições de habilitação estabelecidos no Edital, mediante a apresentação de documentos, desde que os envie no curso da própria sessão pública do pregão e até a decisão sobre a habilitação, por meio correio eletrônico para o endereço sirabelo@seade.gov.br.

c.1) Sem prejuízo do disposto nas alíneas “a”, “b”, “c”, “d” e “e”, deste subitem 9, serão apresentados, obrigatoriamente, por fax ou por correio eletrônico, as declarações a que se referem os subitens 1.5 e 1.6, do item IV, deste edital.

d) A Administração não se responsabilizará pela eventual indisponibilidade dos meios eletrônicos hábeis de informações, no momento da verificação a que se refere a alínea “b”, ou dos meios para transmissão de cópias de documentos a que se refere a alínea “c”, ambas deste subitem 9, ressalvada a indisponibilidade de seus próprios meios. Na hipótese de ocorrerem essas indisponibilidades e/ou não sendo supridas ou saneadas as eventuais omissões ou falhas, na forma prevista nas alíneas “b” e “c”, a licitante será inabilitada, mediante decisão motivada.

e) Os originais ou cópias autenticadas por tabelião de notas, dos documentos enviados na forma constante da alínea “c”, deverão ser apresentados na Gerência Administrativa da Fundação Seade, sito à Avenida Professor Lineu Prestes, 913 – Cidade Universitária – CEP: 05508-000, São Paulo, nesta Capital, em até 02 (dois) dias após o encerramento da sessão pública, sob pena de invalidade do respectivo ato de habilitação e a aplicação das penalidades cabíveis.

f) Para habilitação de microempresas, empresas de pequeno porte ou cooperativas que preencham as condições estabelecidas no artigo 34, da Lei Federal nº 11.488, de 15/06/2007, não será exigida comprovação de regularidade fiscal, mas será obrigatória a apresentação dos documentos indicados no subitem 1.2, alíneas "a" a "e" do item IV deste Edital, ainda que os mesmos veiculem restrições impeditivas à referida comprovação;

g) Constatado o cumprimento dos requisitos e condições estabelecidos no Edital, a licitante será habilitada e declarada vencedora do certame.

h) Por meio de aviso lançado no sistema, o Pregoeiro informará aos demais licitantes que poderão consultar as informações cadastrais da licitante vencedora, utilizando opção disponibilizada no próprio sistema para tanto. Deverá, ainda, informar, o teor dos documentos recebidos por fac-símile ou outro meio eletrônico.

10. A licitante habilitada nas condições da alínea "f", do subitem 9, deste item V, deverá comprovar sua regularidade fiscal, sob pena de decadência do direito à contratação, sem prejuízo da aplicação das sanções cabíveis.

11. A comprovação de que trata o subitem 10 deste item V deverá ser efetuada mediante a apresentação das competentes certidões negativas de débitos, ou positivas com efeito de negativa, no prazo de 05 (cinco) dias úteis, contado a partir do momento em que a licitante for declarada vencedora do certame, prorrogável por igual período, a critério da Fundação Seade.

12. Ocorrendo a habilitação na forma indicada na alínea "f", do subitem 9, a sessão pública será suspensa pelo Pregoeiro, observados os prazos previstos no subitem 11, para que a licitante vencedora possa comprovar a regularidade fiscal de que tratam os subitens 10 e 11 deste item V.

13. Por ocasião da retomada da sessão, o Pregoeiro decidirá motivadamente sobre a comprovação ou não da regularidade fiscal, de que tratam os subitens 10 e 11 deste item V, ou sobre a prorrogação de prazo para a mesma comprovação, observado o disposto no mesmo subitem 11.

14. Se a oferta não for aceitável, se o licitante desatender às exigências para a habilitação, ou não sendo saneada a irregularidade fiscal, nos moldes dos subitens 10 a 13, deste item V, o Pregoeiro respeitada a ordem de classificação de que trata o subitem 5 do mesmo item V, examinará a oferta subsequente de menor preço, negociará com o seu autor, decidirá sobre a sua aceitabilidade e, em caso positivo, verificará as condições de habilitação e, assim, sucessivamente, até a apuração de uma oferta aceitável cujo autor atenda aos requisitos de habilitação, caso em que será declarado vencedor.

VI. DO RECURSO, DA ADJUDICAÇÃO E DA HOMOLOGAÇÃO

1. Divulgado o vencedor ou se for o caso, saneada a irregularidade fiscal, nos moldes dos subitens 10 a 13 do item V, o Pregoeiro informará às licitantes, por meio de mensagem lançada no sistema, que poderão interpor recurso, imediata e

motivadamente, por meio eletrônico, utilizando para tanto, exclusivamente, campo próprio disponibilizado no sistema.

2. Havendo manifestação motivada da intenção de interposição de recurso, na forma indicada no subitem "1" deste item, o Pregoeiro, por mensagem lançada no sistema, informará aos recorrentes que poderão apresentar memoriais contendo as razões de recurso, no prazo de 3 (três) dias após o encerramento da sessão pública e, às demais licitantes, que poderão apresentar contra razões, em igual número de dias, os quais começarão a correr do término do prazo para apresentação de memoriais, sendo-lhes assegurada vista imediata dos autos, no endereço da unidade promotora da licitação, ou seja, Avenida Professor Lineu Prestes, 913 – Cidade Universitária – CEP: 05508-000, São Paulo – Gerência Administrativa da Fundação Seade.

2.1. Os memoriais de recurso e as contrarrazões serão oferecidas, por meio eletrônico, no sítio www.bec.sp.gov.br/ ou www.bec.fazenda.sp.gov.br opção RECURSO, e a apresentação de documentos relativos às peças antes indicadas, se houver, será efetuada mediante protocolo, na Gerência Administrativa da Fundação Seade, sito a Avenida Professor Lineu Prestes, 913 – Cidade Universitária – CEP: 05508-000, São Paulo, nesta Capital, observados os prazos estabelecidos no subitem 2, deste item.

3. A falta de interposição na forma prevista no subitem "1" deste item, importará a decadência do direito de recurso e o pregoeiro adjudicará o objeto do certame ao vencedor, na própria sessão, propondo à autoridade competente a homologação do procedimento licitatório.

4. Decididos os recursos e constatada a regularidade dos atos praticados, a autoridade competente adjudicará o objeto da licitação à licitante vencedora e homologará o procedimento licitatório.

5. O recurso terá efeito suspensivo e o seu acolhimento importará a invalidação dos atos insuscetíveis de aproveitamento.

6. A adjudicação será feita considerando a totalidade do objeto.

VII - DA DESCONEXÃO COM O SISTEMA ELETRÔNICO

1. À licitante caberá acompanhar as operações no sistema eletrônico, durante a sessão pública, respondendo pelos ônus decorrentes de sua desconexão ou da inobservância de quaisquer mensagens emitidas pelo sistema.

2. A desconexão do sistema eletrônico com o Pregoeiro, durante a sessão pública, implicará:

a) fora da etapa de lances, a sua suspensão e o seu reinício, desde o ponto em que foi interrompida. Neste caso, se a desconexão persistir por tempo superior a 15 (quinze) minutos, a sessão pública deverá ser suspensa e reiniciado somente após comunicação expressa aos licitantes, de nova data e horário para a sua continuidade.

b) durante a etapa de lances, a continuidade da apresentação de lances pelas licitantes, até o término do período estabelecido no edital.

3. A desconexão do sistema eletrônico com qualquer licitante, não prejudicará a conclusão válida da sessão pública ou do certame.

VIII - DOS PRAZOS, CONDIÇÕES E DO LOCAL DE EXECUÇÃO DOS SERVIÇOS

1. A prestação de serviços objeto desta licitação deverá ser executada nas dependências da Fundação Seade à Avenida Professor Lineu Prestes, 913 – Cidade Universitária – São Paulo, devendo ser obedecido o prazo para a entrega e implantação da solução e demais condições constantes do Termo de Referência.

IX - DAS CONDIÇÕES DE RECEBIMENTO DO OBJETO

1. O recebimento desse objeto se dará por meio da emissão pela SUTIN (Superintendência de Informática) da Fundação Seade, do Termo de Recebimento Definitivo, em até três dias úteis, após a entrega definitiva do objeto e mediante a verificação de sua execução, em conformidade com as condições contratadas e a proposta comercial apresentada.

.

X – DA FORMA DE PAGAMENTO

1. O pagamento do valor será efetuado em parcela única, no prazo de 30 (trinta) dias (art. 2º do Decreto nº 32.117, de 10/08/1990 com a redação dada pelo Decreto nº 43.914, de 26/03/1999), contados da data da apresentação da nota fiscal/fatura (no caso de sábado domingo e feriado, será efetuado no primeiro dia útil subsequente), sem qualquer incidência de atualização monetária nesse período.

2. As notas fiscais/faturas que apresentarem incorreções serão devolvidas à Contratada para as devidas correções e seu vencimento ocorrerá 30 (trinta) dias após a data de sua apresentação válida.

3. Constitui condição para a realização dos pagamentos a inexistência de registros em nome da Contratada no "Cadastro Informativo dos Créditos não Quitados de Órgãos e Entidades Estaduais do Estado de São Paulo – CADIN ESTADUAL", o qual deverá ser consultado por ocasião da realização de cada pagamento.

4. O pagamento será feito mediante crédito aberto em conta corrente em nome da **CONTRATADA** no Banco do Brasil S/A, conforme disposto no Dec. nº. 55.357 de 18/01/2010.

5. Havendo atraso nos pagamentos devidos pela **CONTRATANTE,** sobre o valor devido incidirá correção monetária nos termos do artigo 74 da Lei estadual nº 6.544/1989, bem como juros moratórios, à razão de 0,5% (meio por cento) ao mês, calculados *"pro rata tempore"* em relação ao atraso

XI -DA CONTRATAÇÃO

1. A contratação decorrente desta licitação será formalizada mediante celebração de termo de contrato, cuja minuta integra este edital como **Anexo III.**

1.1. Se, por ocasião da formalização do contrato, as certidões de regularidade de débito da adjudicatária perante o Sistema de Seguridade Social (INSS), o Fundo de Garantia por Tempo de Serviço (FGTS) e a Fazenda Nacional (Certidão Conjunta Negativa de Débitos relativa a tributos federais e dívida ativa da União) estiverem com os prazos de validade vencidos, o órgão licitante verificará a situação por meio eletrônico hábil de informações, certificando nos autos do processo a regularidade e anexando os documentos passíveis de obtenção por tais meios, salvo impossibilidade devidamente justificada.

1.2. Se não for possível atualizá-las por meio eletrônico hábil de informações, a Adjudicatária será notificada para, no prazo de 05 (cinco) dias úteis, comprovar a sua situação de regularidade de que trata o subitem 1.1 deste item XI, mediante a apresentação das certidões respectivas com prazos de validade em vigência, sob pena de a contratação não se realizar.

1.3. Constitui condição para a celebração da contratação a inexistência de registros em nome da adjudicatária no "Cadastro Informativo dos Créditos não quitados de Órgãos e entidades Estaduais do Estado de São Paulo – CADIN ESTADUAL", o qual deverá ser consultado por ocasião da respectiva celebração.

1.4 Na hipótese de ser vencedora da licitação cooperativa de trabalho, constitui condição para a contratação a indicação, pela sociedade cooperativa, de gestor encarregado de representá-lo com exclusividade perante a contratante, nos termos previstos no artigo 1º, § 2º, item 2, do Decreto estadual nº 57.159/11.

1.4.1 Na situação prevista no subitem 1.4 deste item XI, caso celebrado o contrato com cooperativa de trabalho, o contrato administrativo será rescindido imediatamente na hipótese de caracterização superveniente de prestação de trabalho nas condições a que alude o alude § 1º do artigo 1º do Decreto estadual nº 57.159/2011, conforme estabelece o § 2º, item 3, do mesmo diploma legal.

2. A adjudicatária deverá, no prazo de 5 (cinco) dias corridos contados da data da convocação, comparecer à Gerência Administrativa sito à Av. Professor Lineu Prestes, 913, para assinar o termo de contrato.

3. Quando a Adjudicatária deixar de comprovar a regularidade fiscal, nos moldes das alíneas "10" e "11", ou na hipótese de invalidação do ato de habilitação com base no disposto na alínea "e", todas do subitem "9" do item V ou, ainda, quando convocada dentro do prazo de validade de sua proposta, não apresentar a situação regular de que trata o subitem 1.1 e 1.3 deste item XI, ou se recusar a assinar o contrato, serão convocadas as demais licitantes classificadas, para participar de nova sessão pública do pregão, com vistas à celebração da contratação.

3.1. Essa nova sessão será realizada em prazo não inferior a 03 (três) dias úteis, contados da divulgação do aviso.

3.2. A divulgação do aviso ocorrerá por publicação no Diário Oficial do Estado de São Paulo - DOE e divulgação nos endereços eletrônicos www.bec.sp.gov.br ou www.bec.fazenda.sp.gov.br e www.imesp.com.br, opção "e-negociospublicos".

3.3. Na sessão, respeitada a ordem de classificação, observar-se-ão as disposições dos subitens 7 a 10 do item V e subitens 1, 2, 3, 4 e 6 do item VI, todos deste Edital.

4. A validade das licenças será perpétua, porém as atualizações e versões das licenças terão validade de **12 (doze) meses.**

5. As atualizações e versões das licenças poderão ser renovadas por igual (ais) e sucessivo (s) período (s), a critério da Administração, até o limite de 48 (quarenta e oito) meses, nos termos e condições permitidos pela legislação vigente.

5.1. A renovação das atualizações e versões do sistema, somente será formalizada caso os preços mantenham-se vantajosos para a FUNDAÇÃO SEADE e consistentes com o mercado, conforme pesquisa a ser realizada à época.

5.2. Eventual prorrogação de prazo será formalizada por meio de Termo de Prorrogação Contratual, respeitadas as condições prescritas na Lei 8666/93.

5.3. A CONTRATADA poderá se opor à prorrogação de que trata o item V.2 desta cláusula, desde que o faça mediante documento escrito, recepcionado pela FUNDAÇÃO SEADE com antecedência de 90 (noventa) dias do término do prazo do contrato.

6. Não obstante o prazo estipulado no subitem 4 deste item XI, a vigência contratual nos exercícios subsequentes ao da assinatura do contrato estará sujeita à condição resolutiva, consubstanciada na existência de recursos aprovados nas respectivas Leis Orçamentárias de cada exercício, para atender as respectivas despesas.

7. Ocorrendo a resolução do contrato, com base na condição estipulada no subitem 6 deste item X, a CONTRATADA não terá direito a qualquer espécie de indenização.

8. Se sociedade cooperativa, esta deve apresentar registro perante a entidade estadual da Organização das Cooperativas Brasileiras, nos termos do artigo 107 da Lei federal nº 5.764, de 14 de julho de 1971

XII - DAS SANÇÕES PARA O CASO DE INADIMPLEMENTO

1. Ficará impedida de licitar e contratar com a Administração direta e indireta do Estado de São Paulo, pelo prazo de até 5 (cinco) anos, a pessoa física ou jurídica que praticar quaisquer atos previstos no artigo 7º da Lei Federal nº 10.520, de 17 de julho de 2002, c.c. o artigo 15 da Resolução CEGP-10 de 19 de novembro de 2002.

2. A sanção de que trata o subitem anterior poderá ser aplicada juntamente com as multas previstas nos artigos 86 e 87 da Lei Federal no. 8.666/93 e na Resolução SEP nº 06, de 27 de junho de 1990, garantido o exercício de prévia e ampla defesa, e deverá ser registrada no CAUFESP e no sítio www.sancoes.sp.gov.br

XIII - DA GARANTIA CONTRATUAL

1. Não será exigida garantia contratual.

XIV - DAS DISPOSIÇÕES FINAIS

1. As normas disciplinadoras desta licitação serão interpretadas em favor da ampliação da disputa, respeitada a igualdade de oportunidade entre as licitantes, desde que não comprometam o interesse público, a finalidade e a segurança da contratação.

2. Das sessões públicas de processamento do Pregão serão lavradas atas circunstanciadas, observado o disposto no artigo 14, inciso XII, da Resolução CC-27/2006, a ser assinada pelo Pregoeiro e pela equipe de apoio.

3. O sistema manterá sigilo quanto a identidade das licitantes, para o Pregoeiro até a etapa de negociação com o autor da melhor oferta e para os demais, até a etapa de habilitação.

4. O resultado deste Pregão e os demais atos pertinentes a esta licitação, sujeitos à publicação, serão divulgados no Diário Oficial do Estado e nos sítios eletrônicos www.imesp.com.br, opção "e-negociospublicos" e www.bec.sp.gov.br ou www.bec.fazenda.sp.gov.br, opção "pregaoeletronico".

5. Até 2 (dois) dias úteis anteriores à data fixada para abertura da sessão pública, qualquer pessoa poderá, por meio do sistema eletrônico, solicitar esclarecimentos, providências ou impugnar o ato convocatório do Pregão Eletrônico.

5.1. A impugnação, assim como os pedidos de esclarecimentos será formulada em campo próprio do sistema, encontrados na opção EDITAL.

5.2. As impugnações serão respondidas pelo subscritor do Edital e os esclarecimentos e informações prestados pelo pregoeiro, no prazo de até 1 (um) dia útil, anterior à data fixada para abertura da sessão pública.

5.3. Acolhida a impugnação contra o ato convocatório, será designada nova data para realização da sessão pública.

6. Os casos omissos do presente Pregão serão solucionados pelo Pregoeiro, e as questões relativas ao sistema, pelo Departamento de Controle de Contratações Eletrônicas – DCC.

7. Integram o presente Edital:

Anexo I	=>	Termo de Referência;
Anexo II	=>	Modelo de Proposta Comercial;
Anexo III	=>	Minuta de contrato;
Anexo IV	=>	Modelo de Declaração;
Anexo V	=>	Modelo de Declaração;
Anexo VI	=>	Modelo de Declaração;
Anexo VII	=>	Modelo de Declaração;
Anexo VIII	=>	Resolução SEP - 06/90, de 27 de junho de 1990;

8. Para dirimir quaisquer questões decorrentes da licitação, não resolvidas na esfera administrativa, será competente o foro da Comarca da Capital do Estado de São Paulo.

São Paulo, 31 de agosto de 2016

Simone Aparecida Pedro Rabelo
Pregoeira

ANEXO I
TERMO DE REFERÊNCIA

Objeto: Contratação de empresa para fornecimento de 360 (trezentos e sessenta) licenças de software antivírus, com Suporte Técnico do fabricante pelo período de 12(doze) meses, incluindo a implantação e a configuração do novo software.

Item	Quantidade	Unidade	Descrição
01	360	Licença	Software de Antivírus com Suporte Técnico, pelo fabricante, por 12 meses
02		Horas	Implantação e configuração da Solução

- Fornecimento de 360 (trezentos e sessenta) licenças de software antivírus pelo período de 12 (doze) meses com Suporte Técnico, do fabricante, pelo mesmo período;
- Implantação da solução no ambiente Seade;
- A entrega das licenças e implantação da solução deve ocorrer dentro do prazo de, no máximo, 30 (trinta) dias corridos, contados da assinatura do contrato.
- O recebimento desse objeto, dar-se-á por meio da emissão, pela Sutin – Superintendência de Informática da Fundação Seade, de Termo de Recebimento Definitivo, mediante verificação de sua execução em conformidade com as condições contratadas e a proposta comercial apresentada.

VIGÊNCIA E PRORROGAÇÃO DO CONTRATO

A validade das licenças será perpétua, mas as atualizações da solução de antivírus e suporte técnico, pelo fabricante, terão validade de 12 (doze) meses e as atualizações e versões do sistema poderão ser renovados anualmente de acordo com a Lei.

Das Exigências:

A solução ofertada deverá fornecer proteção para os servidores de dados, rede, e-mail e internet, protegendo também os microcomputadores conectados ao *Active Diretory* da Fundação Seade. A proteção deve funcionar no âmbito corporativo, possibilitando o gerenciamento centralizado a partir de uma console administrativa.

1. Servidor de Administração e Console Administrativa

1.1.Compatibilidade:

1.1.1.Microsoft Windows Server 2003 ou superior (Todas edições);

1.1.2. Microsoft Windows Server 2003 x64 ou superior (Todas edições);

1.1.3. Microsoft Windows Server 2008 (Todas edições);

1.1.4. Microsoft Windows Server 2008 Core (Todas edições);

1.1.5.Microsoft Windows Server 2008 x64 SP1 (Todas edições);

1.1.6.Microsoft Windows Server 2008 R2 (Todas edições);

1.1.7.Microsoft Windows Server 2008 R2 Core (Todas edições);

1.1.8.Microsoft Windows Server 2012 (Todas edições);

1.1.9.Microsoft Windows Server 2012 R2 (Todas edições);

1.1.10. Microsoft Windows XP Professional SP2 ou superior;

1.1.11. Microsoft Windows XP Professional x64 e superior;

1.1.12. Microsoft Windows Vista SP1;

1.1.13. Microsoft Windows Vista x64 SP1;

1.1.14. Microsoft Windows 7;

1.1.15. Microsoft Windows 7 x64;

1.1.16. Microsoft Windows 8;

1.1.17. Microsoft Windows 8 x64;

1.1.18. Microsoft Windows 10;

1.1.19. Microsoft Windows 10 x64.

1.2.Suportar as seguintes plataformas virtuais:

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

1.2.2. Microsoft Hyper-V: 2008, 2008 R2, 2012, 2012 R2;

1.2.3. KVM integrado com: RHEL 5.4 e 5.x acima, SLES 11 SPx, Ubuntu 10.10 LTS;

1.2.4. Citrix XenServer 6.1, 6.2.

1.3.Características:

1.3.1. A console deve ser acessada via WEB (HTTPS) ou MMC.

1.3.2. Console deve ser baseada no modelo cliente/servidor.

1.3.3. Compatibilidade com *Windows Failover Clustering* ou outra solução de alta disponibilidade.

1.3.4. Deve permitir a atribuição de perfis para os administradores da Solução de Antivírus.

1.3.5. Caso haja a necessidade, no futuro, de adicionar novas tecnologias tais como: criptografia, *patch management* e MDM a console deve suportar e ser totalmente integrada com suas funções e módulos.

1.3.6. **As licenças deverão ser perpétuas**, ou seja, expirado a validade da mesma o produto deverá permanecer funcional para a proteção contra códigos maliciosos;

1.3.7. Capacidade de remover remotamente e automaticamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores, sem a necessidade da senha de remoção do atual antivírus;

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

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

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

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

1.3.12. Capacidade de instalar remotamente a solução de segurança em smartphones e *tablets* de sistema iOS, Android e Windows.

1.3.13. Capacidade de instalar remotamente qualquer “app” em smartphones e *tablets* de sistema iOS;

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

1.3.15. Deverá ter a capacidade de criar regras para limitar o tráfego de comunicação cliente/servidor por subredes com os seguintes parâmetros: KB/s e horário.

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

1.3.17. Capacidade de gerenciar smartphones e *tablets* (Windows Phone, Android e iOS) protegidos pela solução antivírus;

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

1.3.19. Capacidade de atualizar os pacotes de instalação com as últimas vacinas;

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

1.3.21. A comunicação entre o cliente e o servidor de administração deve ser criptografada.

1.3.22. Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes a partir da console administrativa;

1.3.23. Deve permitir a realocação de máquinas novas na rede para um determinado grupo sem ter um agente ou *endpoint* instalado através dos seguintes parâmetros:

Nome do computador

Nome do domínio

Range de IP

Sistema Operacional

Máquina virtual

1.3.24. Capacidade de importar a estrutura do *Active Directory* para descobrimento dos microcomputadores;

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

1.3.26. Capacidade de monitorar diferentes subredes a fim de encontrar máquinas novas para serem adicionadas à proteção;

1.3.27. Capacidade de monitorar grupos de trabalhos já existentes e quaisquer grupos de trabalho que forem criados na rede, a fim de encontrar máquinas novas para serem adicionadas à proteção;

1.3.28. Capacidade de, assim que detectar máquinas novas no Active Directory, subredes ou grupos de trabalho, automaticamente importar a máquina para a estrutura de proteção da console e verificar se possui o antivírus instalado. Caso não possua, deverá instalar o mesmo automaticamente;

1.3.29. Capacidade de agrupamento de estações por características comuns entre as mesmas, por exemplo: agrupar todas as estações que não tenham o antivírus instalado, agrupar todas que não receberam atualização nos últimos 2 (dois) dias, etc.;

1.3.30. Capacidade de definir políticas de configurações diferentes por grupos de estações, permitindo que sejam criados subgrupos e com função de herança de políticas entre grupos e subgrupos;

1.3.31. Deve fornecer as seguintes informações dos computadores:

1.3.31.1. Se o antivírus está instalado;

1.3.31.2. Se o antivírus está iniciado;

1.3.31.3. Se o antivírus está atualizado;

1.3.31.4. Minutos/horas desde a última conexão da estação com o servidor administrativo;

1.3.31.5. Minutos/horas desde a última atualização de vacinas;

1.3.31.6. Data e horário da última verificação executada;

1.3.31.7. Versão do antivírus instalado;

1.3.31.8. Se é necessário reiniciar o computador para aplicar mudanças;

1.3.31.9. Data e horário que o computador foi ligado;

1.3.31.10. Quantidade de vírus encontrados (contador);

1.3.31.11. Nome do microcomputador;

1.3.31.12. Domínio ou grupo de trabalho;

1.3.31.13. Data e horário da última atualização de vacinas;

1.3.31.14. Versão do sistema operacional e qual Service Pack instalado;

1.3.31.15. Quantidade de processadores;

1.3.31.16. Quantidade de memória RAM;

1.3.31.17. Usuário(s) logado(s) naquele momento, com informações de contato (caso disponíveis no Active Directory);

1.3.31.18. Endereço IP;

1.3.31.19. Aplicativos instalados, inclusive de terceiros, com histórico de instalação, contendo data e hora que o software foi instalado ou removido.

1.3.31.20. Atualizações do Windows Update instaladas.

1.3.31.21. Informação completa de hardware contendo: processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de áudio, adaptadores de rede, monitores, drives de CD/DVD.

1.3.31.22. Vulnerabilidades dos aplicativos instalados no computador.

1.3.32. Deve permitir o bloqueio das configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterá-las;

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

1.3.33.1. Mudança de gateway;

1.3.33.2. Mudança de subrede DNS;

1.3.33.3. Mudança de domínio;

1.3.33.4. Mudança de servidor DHCP;

1.3.33.5. Mudança de servidor DNS;

1.3.33.6. Mudança de servidor WINS;

1.3.33.7. Aparecimento de nova subrede;

1.3.34. Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa ser atualizado usando a conexão com a Internet;

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

1.3.36. Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus;
1.3.37. Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos;
1.3.38. Capacidade de eleger qualquer computador cliente como repositório de vacinas e de pacotes de instalação, sem que seja necessária a instalação de um servidor administrativo completo, onde outras máquinas clientes irão atualizar-se e receber pacotes de instalação, a fim de otimizar tráfego da rede;
1.3.39. Capacidade de fazer deste repositório de vacinas um gateway para conexão com o servidor de administração, para que outras máquinas que não consigam conectar-se diretamente ao servidor possam usar este gateway para receber e enviar informações ao servidor administrativo.
1.3.40. Capacidade de exportar relatórios para os seguintes tipos de arquivos: PDF, HTML e XML.
1.3.41. Capacidade de gerar traps SNMP para monitoramento de eventos por softwares de gerenciamento, como por exemplo o Zabbix, utilizado pela Fundação Seade;
1.3.42. Capacidade de enviar e-mails para contas específicas em caso de algum evento;
1.3.43. Deve possuir compatibilidade com Microsoft NAP, quando instalado em um Sistema Operacional versão Windows 2008 Server;
1.3.44. Deve possuir compatibilidade com Cisco *Network Admission Control* (NAC);
1.3.45. Deve possuir documentação da estrutura do banco de dados para geração de relatórios a partir de ferramentas específicas de consulta, como por exemplo: *Crystal Report*.
1.3.46. Capacidade de ligar máquinas via *Wake on Lan* para realização de tarefas (varredura, atualização, instalação, etc.), inclusive de máquinas que estejam em subredes diferentes do servidor;
1.3.47. Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado intervalo de tempo);
1.3.48. Capacidade de realizar atualização incremental de vacinas nos computadores clientes;
1.3.49. Deve armazenar localmente e enviar ao servidor de gerência a(s) ocorrência(s) de vírus com, no mínimo, os seguintes dados:

- Nome do vírus;
- Nome do arquivo infectado;
- Data e hora da detecção;

- Nome da máquina ou endereço IP;
- Ação realizada.

1.3.50. Capacidade de reportar vulnerabilidades de softwares presentes nos computadores.

1.3.51. Capacidade de realizar inventário de aplicativos de todas as máquinas clientes;

1.3.52. Capacidade de diferenciar máquinas virtuais de máquinas físicas;

2. Estações Microsoft Windows

2.1.Compatibilidade:

2.1.1. Microsoft Windows XP Professional SP3 e superior;

2.1.2. Microsoft Windows Vista Business/Enterprise/Ultimate SP2;

2.1.3. Microsoft Windows Vista Business/Enterprise/Ultimate x64 SP2;

2.1.4. Microsoft Windows 7 Professional/Enterprise/Ultimate;

2.1.5. Microsoft Windows 7 Professional/Enterprise/Ultimate x64;

2.1.6.Microsoft Windows 7 Professional/Enterprise/Ultimate SP1 e superior;

2.1.7.Microsoft Windows 7 Professional/Enterprise/Ultimate x64 SP1 e superior;

2.1.8. Microsoft Windows 8 Professional/Enterprise;

2.1.9. Microsoft Windows 8 Professional/Enterprise x64;

2.1.10. Microsoft Windows 8.1 Enterprise x86 / 64;

2.1.11. Microsoft Windows 8.1 Pro x86 /64

2.1.12. Microsoft Windows 10 Enterprise x86 / 64

2.1.13. Microsoft Windows 10 Pro x86 / 64

2.2.Características:

2.2.1. Deve prover as seguintes proteções:

2.2.1.1. Antivírus de Arquivos residente (*anti-spyware, anti-trojan, anti-malware*, etc.) que verifique qualquer arquivo criado, acessado ou modificado.

2.2.1.2. Antivírus de Web (módulo para verificação de sites e downloads contra vírus).

2.2.1.3. Antivírus de *e-mail* (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos).

2.2.1.4. Antivírus de Mensagens Instantâneas (módulo para verificação de mensagens instantâneas, como ICQ, MSN, IRC, etc.).

2.2.1.5. O *Endpoint* deverá possuir opção para rastreamento por linha de comando, parametrizável, com opção de limpeza:

2.2.1.6. Firewall com IDS.

2.2.1.7. Autoproteção (contra ataques aos serviços/processos do antivírus).

2.2.1.8. Controle de dispositivos externos.

2.2.1.9. Controle de acesso a sites por categoria.

2.2.1.10. Controle de acesso a sites por horário.

2.2.1.11. Controle de acesso a sites por usuários.

2.2.1.12. Controle de execução de aplicativos.

2.2.1.13. Controle de vulnerabilidades do Windows e dos aplicativos instalados.

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

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

2.2.4. Capacidade de automaticamente desabilitar o Firewall do Windows (caso exista) durante a instalação, para evitar incompatibilidade com o Firewall da solução;

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

2.2.6.Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: “Win32.Trojan.banker”) para que qualquer objeto detectado com o veredicto escolhido seja ignorado;

2.2.7. Capacidade de adicionar aplicativos a uma lista de “aplicativos confiáveis”, onde as atividades de rede, atividades de disco e acesso ao registro do Windows não serão monitoradas;

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

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

2.2.10. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomá-la a partir da extensão do arquivo;

2.2.11. Capacidade de verificar somente arquivos novos e alterados;

2.2.12. Capacidade de verificar objetos usando heurística;

2.2.13. Capacidade de agendar uma pausa na verificação;

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

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

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

2.2.16.1. Perguntar o que fazer, ou;

2.2.16.2. Bloquear acesso ao objeto;

2.2.16.2.1. Apagar o objeto ou tentar desinfetá-lo (de acordo com a configuração pré-estabelecida pelo administrador);

2.2.16.2.2. Caso positivo de desinfecção:

2.2.16.2.2.1. Restaurar o objeto para uso;

2.2.16.2.3. Caso negativo de desinfecção:

2.2.16.2.3.1. Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);

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

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

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

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

2.2.21. Capacidade de verificar tráfego SSL nos browsers: Internet Explorer, Firefox e Chrome;

2.2.22. Capacidade de verificação de corpo e anexos de e-mails usando heurística;

2.2.23. O antivírus de e-mail, ao encontrar um objeto potencialmente perigoso, deve:

2.2.23.1. Perguntar o que fazer, ou;

2.2.23.2. Bloquear o e-mail;

2.2.23.2.1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);

2.2.23.2.2. Caso positivo de desinfecção:

2.2.23.2.2.1. Restaurar o e-mail para o usuário;

2.2.23.2.3. Caso negativo de desinfecção:

2.2.23.2.3.1. Mover para quarentena ou apagar o objeto (de acordo com a configuração pré-estabelecida pelo administrador);

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

2.2.25. Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados.

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

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

2.2.28. Deve ter suporte total ao protocolo IPv6;

2.2.29. Capacidade de alterar as portas monitoradas pelos módulos de Web e E-mail;

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

2.2.30.1. Perguntar o que fazer, ou;

2.2.30.2. Bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio, ou;

2.2.30.3. Permitir acesso ao objeto;

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

2.2.31.1. Verificação on-the-fly, onde os dados são verificados enquanto são recebidos em tempo real, ou;

2.2.31.2. Verificação de buffer, onde os dados são recebidos e armazenados para posterior verificação.

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

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

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

2.2.35. Deve possuir módulo que analise qualquer tentativa de edição, exclusão ou gravação do registro, de forma que seja possível escolher chaves específicas para serem monitoradas e/ou bloqueadas.

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

2.2.37. Capacidade de distinguir diferentes subredes e conceder opção de ativar ou não o firewall para uma subredes específica;

2.2.38. Deve possuir módulo IDS (*Intrusion Detection System*) para proteção contra *port scans* e exploração de vulnerabilidades de softwares. A base de dados de análise deve ser atualizada juntamente com as vacinas.

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

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

2.2.39.2. Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá

acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.

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

2.2.40.1. Discos de armazenamento locais;

2.2.40.2. Armazenamento removível;

2.2.40.3. Impressoras;

2.2.40.4. CD/DVD;

2.2.40.5. Modems;

2.2.40.6. Dispositivos multifuncionais;

2.2.40.7. Leitores de *smart card;*

2.2.40.9. Dispositivos de sincronização via ActiveSync (Windows CE, Windows Mobile, etc.);

2.2.40.10. Wi-Fi;

2.2.40.11. Adaptadores de rede externos;

2.2.40.12. Dispositivos MP3 ou smartphones;

2.2.40.13. Dispositivos Bluetooth

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

2.2.42. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por usuário.

2.2.43. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por agendamento.

2.2.44. Capacidade de configurar novos dispositivos por Class ID/Hardware ID.

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

2.2.46. Capacidade de limitar a execução de aplicativos por hash MD5, nome do arquivo, versão do arquivo, nome do aplicativo, versão do aplicativo, fabricante/desenvolvedor, categoria (ex: navegadores, gerenciadores de downloads, jogos, aplicação de acesso remoto, etc.).

2.2.47. Capacidade de bloquear execução de aplicativo que está em armazenamento externo.

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

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

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

3. Servidores Microsoft Windows

3.1. Compatibilidade:

3.1.1. Microsoft Windows Small Business Server 2011 Essentials/Standard x64;

3.1.2. Microsoft Windows Server 2003 Standard/Enterprise SP2 x86/x64;

3.1.3. Microsoft Windows Server 2003 R2 Standard/Enterprise SP2 x86/x64;

3.1.4. Microsoft Windows Server 2008 Standard/Enterprise/Datacenter SP1 x86/x64;

3.1.5. Microsoft Windows Server 2008 Core Standard/Enterprise/Datacenter SP1 x86/x64;

3.1.6. Microsoft Windows Server 2008 R2 Standard/Enterprise/Datacenter SP1;

3.1.7. Microsoft Windows Server 2008 R2 Core Standard/Enterprise/Datacenter SP1;

3.1.8. Microsoft Windows Server 2012 Foundation/Essentials/Standard x64;

3.1.9. Microsoft Windows Hyper-V Server 2008 R2 SP1;

3.1.10. Microsoft Terminal baseado em Windows Server 2003;

3.1.11. Microsoft Terminal baseado em Windows Server 2008;

3.1.12. Microsoft Terminal baseado em Windows Server 2008 R2;

3.1.13. Citrix Presentation Server 4.0 e 4.5;

3.1.14. Citrix XenApp 4.5, 5.0 e 6.0;

3.2.Características:

3.2.1. Deve prover as seguintes proteções:

3.2.1.1. Antivírus de Arquivos residente (*anti-spyware*, *anti-trojan*, *anti-malware*, etc.) que verifique qualquer arquivo criado, acessado ou modificado;

3.2.1.2. Autoproteção contra ataques aos serviços/processos do antivírus;

3.2.1.3. Firewall com IDS;

3.2.1.4. Controle de vulnerabilidades do Windows e dos aplicativos instalados

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

3.2.3. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora.

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

3.2.4.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);

3.2.4.2. Gerenciamento de tarefa (criar ou excluir tarefas de verificação);

3.2.4.3. Leitura de configurações;

3.2.4.4. Modificação de configurações;

3.2.4.5. Gerenciamento de Backup e Quarentena;

3.2.4.6. Visualização de relatórios;

3.2.4.7. Gerenciamento de relatórios;

3.2.4.8. Gerenciamento de chaves de licença;

3.2.4.9. Gerenciamento de permissões (adicionar/excluir permissões acima);

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

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

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

3.2.6.Capacidade de separadamente selecionar o número de processos que irão executar funções de varredura em tempo real, o número de processos que executarão a varredura sob demanda e o número máximo de processos que podem ser executados no total.

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

3.2.8.Capacidade de automaticamente pausar e não iniciar tarefas agendadas caso o servidor esteja em rodando com fonte ininterrupta de energia (*Uninterruptible Power supply – UPS*).

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

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

3.2.11. Capacidade de bloquear comunicação a servidores acessados por estações de trabalho infectadas e quando estações tentarem gravar arquivos infectados nos servidores.

3.2.12. Capacidade de criar uma lista de máquina que nunca serão bloqueadas mesmo quando infectadas.

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

3.2.14. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: "*Win32.Trojan.banker*") para que qualquer objeto detectado com o veredicto escolhido seja ignorado;

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

3.2.16. 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 tomá-la a partir da extensão do arquivo;

3.2.17. Capacidade de verificar somente arquivos novos e alterados;

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

3.2.19. Capacidade de verificar objetos usando heurística;

3.2.20. Capacidade de configurar diferentes ações para diferentes tipos de ameaças;

3.2.21. Capacidade de agendar uma pausa na verificação;

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

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

3.2.23.1. Perguntar o que fazer, ou;

3.2.23.2. Bloquear acesso ao objeto;

3.2.23.2.1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);

3.2.23.2.2. Caso positivo de desinfecção:

3.2.23.2.2.1. Restaurar o objeto para uso;

3.2.23.2.3. Caso negativo de desinfecção:

3.2.23.2.3.1. Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador).

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

3.2.25. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena.

3.2.26. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados.

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

4. Servidores Linux

4.1.Compatibilidade:

4.1.1. Plataforma 32-bits:

4.1.1.1. Canaima 3;

4.1.1.2. Asianux Server 3 SP4;

4.1.1.3. Asianux Server 4 SP1;

4.1.1.4. Red Hat Enterprise Linux 6.2 Server;

4.1.1.5. Red Hat Enterprise Linux 5.8 Server;

4.1.1.6. Fedora 16;

4.1.1.7. CentOS-6.2;

4.1.1.8. SUSE Linux Enterprise Server 11 SP2;

4.1.1.9. Novell Open Enterprise Server 11;

4.1.1.10. OpenSUSE Linux 12.1;

4.1.1.11. OpenSUSE Linux 12.2;

4.1.1.12. Mandriva Enterprise Server 5.2;

4.1.1.13. Ubuntu Server 10.04.2 LTS;

4.1.1.14. Ubuntu Server 12.04 LTS;

4.1.1.15. Debian GNU/Linux 6.0.5;

4.1.1.16. FreeB.SD 8.3;

4.1.1.17. FreeBSD 9.

4.1.2. Plataforma 64-bits:

4.1.2.1. Canaima 3

4.1.2.2. Asianux Server 3 SP4;

4.1.2.3. Asianux Server 4 SP1;

4.1.2.4. Red Hat Enterprise Linux 6.2 Server;

4.1.2.5. Red Hat Enterprise Linux 5.8 Server;

4.1.2.6. Fedora 16;

4.1.2.7. CentOS-6.2;

4.1.2.8. SUSE Linux Enterprise Server 11 SP2;

4.1.2.9. Novell Open Enterprise Server 11;

4.1.2.10. OpenSUSE Linux 12.1;

4.1.2.11. OpenSUSE Linux 12.2;

4.1.2.12. Mandriva Enterprise Server 5.2;

4.1.2.13. Ubuntu Server 10.04.2 LTS;

4.1.2.14. Ubuntu Server 12.04 LTS;

4.1.2.15. Debian GNU/Linux 6.0.5;

4.1.2.16. FreeBSD 8.3;

4.1.2.17. FreeBSD 9.

4.2.Características:

4.2.1. Deve prover as seguintes proteções:

4.2.1.1. Antivírus de Arquivos residente (*anti-spyware*, *anti-trojan*, *anti-malware*, etc.) que verifique qualquer arquivo criado, acessado ou modificado;

4.2.1.2. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora.

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

4.2.2.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);

4.2.2.2. Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;

4.2.2.3. Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;

4.2.2.4. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados.

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

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

4.2.5. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomá-la a partir da extensão do arquivo;

4.2.6. Capacidade de verificar objetos usando heurística;

4.2.7. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena.

4.2.8. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados.

4.2.9. Deve possuir módulo de administração remoto através de ferramenta nativa ou *webmin* (ferramenta nativa GNU-Linux)

5. Smartphones e tablets

5.1. Compatibilidade:

5.1.1. Apple iOS 7.0 – 9.2;

5.1.2. Windows Phone 8.1;

5.1.3. Android OS 2.3 – 5.1;

5.2. Características:

5.2.1. Deve prover as seguintes proteções:

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

5.2.1.1.1. Todos os objetos transmitidos usando conexões wireless (porta de infravermelho, *Bluetooth*) e mensagens *EMS*, durante sincronismo com PC e ao realizar download usando o navegador.

5.2.1.1.2. Arquivos abertos no smartphone

5.2.1.1.3. Programas instalados usando a interface do smartphone

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

5.2.2. Deverá isolar em área de quarentena os arquivos infectados;

5.2.3. Deverá atualizar as bases de vacinas de modo agendado;

5.2.4. Deverá bloquear spams de *SMS* através de *black lists*;

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

5.2.6.Capacidade de desativar por política: *Wi-Fi*, Câmera e *Bluetooth*.

5.2.7. Deverá ter função de limpeza de dados pessoais a distância, em caso de roubo, por exemplo.

5.2.8.Capacidade de requerer uma senha para desbloquear o dispositivo e personalizar a quantidade de caracteres para esta senha

5.2.9.

5.2.10. Deverá ter firewall pessoal;

5.2.11. Capacidade de tirar fotos quando a senha for inserida incorretamente (*Mugshot*).

5.2.12. Possibilidade de instalação remota utilizando o Microsoft System Center Mobile Device Manager 2008 SP1.

5.2.13. Capacidade de enviar comandos remotamente de: Localizar e Bloquear.

5.2.14. Capacidade de detectar j*ailbreak* em dispositivos iOS.

5.2.15. Capacidade de bloquear o acesso a site por categoria em dispositivos.

5.2.16. Capacidade de bloquear o acesso a sites *phishing* ou malicioso.

5.2.17. Capacidade de criar containers de aplicativos, separando dados corporativos de dados pessoais.

5.2.18. Capacidade de bloquear o dispositivo quando o cartão “SIM” for substituído.

5.2.19. Capacidade de configurar *white* e *blacklist* de aplicativos.

5.2.20. Capacidade de localizar o dispositivo quando necessário.

5.2.21. Permitir atualização das definições quando estiver em “roaming”.

5.2.22. Capacidade de selecionar endereço do servidor para buscar a definição de vírus.

5.2.23. Capacidade de enviar *URL* de instalação por e-mail.

5.2.24. Capacidade de executar as seguintes ações caso a desinfecção falhe: Deletar Ignorar Quarentenar. Perguntar ao usuário.

6. Gerenciamento de dispositivos móveis (MDM):

6.1.Compatibilidade:

6.1.1. Dispositivos conectados através do Microsoft Exchange ActiveSync

6.1.1.1. Apple iOS

6.1.1.2. Windows Phone

6.1.1.3. Android

6.1.2. Dispositivos com suporte ao Apple Push Notification (APNs) servisse.

6.1.2.1. Apple iOS 3.0 ou superior

6.2.Características:

6.2.1. Capacidade de aplicar políticas de ActiveSync através do servidor Microsoft Exchange

6.2.2. Capacidade de ajustar as configurações de:

6.2.2.1. Sincronização de e-mail;

6.2.2.2. Uso de aplicativos;

6.2.2.3. Senha do usuário;

6.2.2.4. Criptografia de dados;

6.2.2.5. Conexão de mídia removível;

6.2.3. Capacidade de instalar certificados digitais em dispositivos móveis.

6.2.4. Capacidade de, remotamente, resetar a senha de dispositivos iOS.

6.2.5. C apacidade de, remotamente, apagar todos os dados de dispositivos iOS.

6.2.6. Capacidade de, remotamente, bloquear um dispositivo iOS

7. Criptografia:

7.1. Compatibilidade:

7.1.1. Microsoft Windows XP Professional SP3 ou superior;

7.1.2. Microsoft Windows Vista Business/Enterprise/Ultimate SP2;

7.1.3. Microsoft Windows Vista Business/Enterprise/Ultimate x64 SP2;

7.1.4. Microsoft Windows 7 Professional/Enterprise/Ultimate;

7.1.5. Microsoft Windows 7 Professional/Enterprise/Ultimate x64;

7.1.6. Microsoft Windows 8 Professional/Enterprise;

7.1.7. Microsoft Windows 8 Professional/Enterprise x64;

7.1.8. Microsoft Windows 8.1 Professional / Enterprise;

7.1.9. Microsoft Windows 8.1 Professional / Enterprise x64;

7.1.10. Microsoft Windows 10 Pro x86 / x64;

7.1.11. Microsoft Windows 10 Enterprise x86 /x64.

7.2. Características:

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

7.2.2. Utilizar, no mínimo, algoritmo AES com chave de 256 bits.

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

7.2.4. Capacidade de utilizar *Single Sign-On* para a autenticação de pré-boot.

7.2.5. Permitir criar vários usuários de autenticação pré-boot.

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

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

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

7.2.7.2. Criptografar todos os arquivos individualmente.

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

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

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

7.2.9. Capacidade de criar regras de exclusões para que certos arquivos ou pastas nunca sejam criptografados.

7.2.10. Capacidade de selecionar aplicações que podem ou não ter acesso aos arquivos criptografados.

7.2.11. Verifica compatibilidade de hardware antes de aplicar a criptografia.

7.2.12. Possibilita estabelecer parâmetros para a senha de criptografia.

7.2.13. Bloqueia o reuso de senhas.

7.2.14. Bloqueia a senha após um número de tentativas pré estabelecidas.

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

7.2.16. Permite criar exclusões para não criptografar determinados "discos rígidos" através de uma busca por nome do computador ou nome do dispositivo.

7.2.17. Permite criptografar as seguintes pastas pré-definidas: "meus documentos", "Favoritos", "Desktop", "Arquivos temporários" e "Arquivos do outlook"

7.2.18. Permite utilizar variáveis de ambiente para criptografar pastas customizadas.

7.2.19. Capacidade de criptografar arquivos por grupos de extensão, tais como: Documentos do office, *Document*, arquivos de áudio, etc.

7.2.20. Permite criar um grupo de extensões de arquivos a serem criptografados

7.2.21. Capacidade de criar regra de criptografia para arquivos gerados por aplicações

7.2.22. Permite criptografia de dispositivos móveis mesmo quando o *endpoint* não possuir comunicação com a console de gerenciamento.

8. Gerenciamento de Sistemas:

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

8.2. Capacidade de detectar softwares de terceiros vulneráveis, criando assim um relatório de softwares vulneráveis.

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

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

8.5. Capacidade de gerenciar licenças de softwares de terceiros.

8.6. Capacidade de registrar mudanças de hardware nas máquinas gerenciadas.

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

8.8. Possibilita fazer distribuição de software de forma manual e agendada.

8.9. Suporta modo de instalação silenciosa.

8.10. Suporte a pacotes MSI, exe, bat, cmd e outros padrões de arquivos executáveis.

8.11. Possibilita fazer a distribuição através de agentes de atualização.

8.12. Utiliza tecnologia *multicast* para evitar tráfego na rede.

8.13. Possibilita criar um inventário centralizado de imagens.

8.14. Capacidade de atualizar o sistema operacional direto da imagem mantendo os dados do usuário.

8.15. Suporte a *Wake On Lan* para *deploy* de imagens

8.16. Capacidade de atuar como servidor de atualização do Windows podendo fazer *deploy* de patches

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

8.18. Capacidade de gerar relatórios de vulnerabilidades e *patches*.

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

8.20. Permite iniciar instalação de *patch* e correções de vulnerabilidades ao reiniciar ou desligar o computador.

8.21. Permite baixar atualizações para o computador sem efetuar a instalação.

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

8.23. Capacidade de instalar correções de vulnerabilidades de acordo com a severidade.

8.24. Permite selecionar produtos a serem atualizados pela console de gerenciamento.

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

9. Serviços de Instalação, configuração e treinamento do software.

9.1. Na assinatura do contrato, a empresa deverá entregar uma declaração de que todos os serviços serão executados por técnicos certificados pelo fabricante do software;

9.1.1 Na assinatura do contrato a empresa vencedora deverá apresentar a certificação dos técnicos mediante certificados emitidos pelo fabricante do software antivírus.

9.2. Documentação do Plano Técnico do Projeto e a Implementação do mesmo, deverá ser apresentado juntamente com a entrega das licenças.

9.3. Instalação e configuração total de todas as licenças do software adquirido no ambiente físico/virtual da CONTRATANTE;

9.4. Validação das soluções implantadas;

9.4.1. Criação das rotinas e teste de Backup / Restore;

9.4.2. Treinamento pelo fabricante ou por técnicos homologados pelo fabricante para ministrar treinamento para 04 (quatro) colaboradores;

9.4.3. Entrega dos ambientes em produção;

9.4.4. Políticas de segurança definidas;

9.4.5. Elaboração do documento técnico final do projeto;

9.5. Aceite por parte da CONTRATANTE, em até três dias úteis após a entrega definitiva.

10. SUPORTE TÉCNICO

A contratada ou fabricante deverá:

10.1. Prover suporte técnico de primeiro nível dos produtos, que poderão ser respondidas por telefone ou via e-mail. Esse suporte deverá estar disponível no horário comercial de segunda a sexta-feira.

10.2. Manter o ambiente em pleno funcionamento, solucionando eventuais problemas que venham a ocorrer.

São Paulo, 31 de agosto de 2016.

VIVALDO LUIZ CONTI
Superintendente de Tecnologia da Informação

ANEXO II

FOLHA DE PROPOSTA

EXPEDIENTE SEADE 085/2016
PREGÃO ELETRÔNICO Nº 017/2016

Examinadas as condições de participação do presente PREGÃO ELETRÔNICO, propomos fornecer os bens e prestar os serviços especificados no **TERMO DE REFERÊNCIA**.

Declaramos aceitar todas as cláusulas e condições que regem este PREGÃO ELETRÔNICO, ficando a presente proposta válida pelo prazo de 60 (sessenta) dias contados da sua apresentação.

LOTE						
ITEM	**QUANT.**	**UNID.**	**DESCRIÇÃO**	**PROCEDÊNCIA / MARCA / MODELO**	**R$ VALOR UNITÁRIO**	**R$ VALOR TOTAL**
01	360	Licença	Software de Antivírus com Suporte Técnico pelo fabricante, por 12 meses			
02		Horas	Implantação da Solução, Configuração da Solução e Treinamento			
VALOR TOTAL DO LOTE - R$ .....(.....).						

1) *O preço acima é final e nele estão incluídos todos os custos, tributos, encargos sociais e demais despesas relativas ao fornecimento objeto desta licitação, de forma a se constituírem na única contraprestação a ser paga pela Fundação Seade.*

_____
Assinatura do Representante legal

DADOS DA EMPRESA CONTRATADA: RAZÃO SOCIAL e CNPJ
DADOS DA PESSOA RESPONSÁVEL PELA ASSINATURA DO CONTRATO

(ESTE ANEXO DEVERÁ SER APRESENTADO APENAS PELA EMPRESA VENCEDORA)

ANEXO III

MINUTA DE CONTRATO

EXPEDIENTE SEADE Nº 085/2016

CONTRATO Nº

CONTRATO QUE ENTRE SI CELEBRAM A FUNDAÇÃO SISTEMA ESTADUAL DE ANÁLISE DE DADOS – SEADE E A EMPRESA_____, OBJETIVANDO O FORNECIMENTO DE 360 LICENÇAS DE SOFTWARE ANTIVÍRUS, COM SUPORTE TÉCNICO PELO FABRICANTE, PELO PERÍODO DE 12 MESES, INCLUINDO A CONFIGURAÇÃO, A IMPLANTAÇÃO E O TREINAMENTO DA SOLUÇÃO.

Pelo presente instrumento, de um lado a **FUNDAÇÃO SISTEMA ESTADUAL DE ANÁLISE DE DADOS – SEADE**, com sede nesta Capital, na Av. Professor Lineu Prestes,913 – São Paulo, inscrita no CNPJ., sob nº 51.169.555/0001-00, Inscrição Estadual nº 110.199.886.112, neste ato representada por seu Diretor Executivo, Dr. **DALMO DO VALLE NOGUEIRA FILHO,** doravante designada simplesmente como **FUNDAÇÃO SEADE** e, de outro lado, a _____, com sede na _____, inscrita no CNPJ, sob nº _____, neste ato representada por seu(sua) _____, Sr(a). _____**, portador do R.G. nº ____, CPF/MF nº_____,** doravante designada simplesmente como **CONTRATADA**, tem entre si justo e combinado, na melhor forma de direito, a prestação dos serviços descritos na cláusula primeira do presente contrato decorrente da licitação realizada na modalidade de Pregão Eletrônico nº 017/2016, sujeitando-se às normas da Lei Federal nº. 10.520/02, do Decreto n° 49.722/05, do regulamento anexo a Resolução n° CC-27, de 25/05/06, aplicando-se, subsidiariamente, no que couberem, às disposições da Lei Federal nº 8.666/93, alterada pelas Leis Federais nºs 8.883/94, 9.032/95, 9.648/98 e 9.854/99, da Lei Estadual nº 6.544/89, do Decreto Estadual n° 47.297/02, da Resolução CEGP-10, de 19/11/02, Lei Estadual nº 13.122 de 07 de julho de 2008 e demais normas regulamentares aplicáveis à espécie, mediante as seguintes cláusulas:

CLÁUSULA I – OBJETO

I.1. O presente instrumento tem por objeto a contratação de empresa para fornecimento de 360 (trezentos e sessenta) licenças de software antivírus pelo período de 12(doze) meses, com Suporte Técnico do fabricante pelo mesmo período**,** incluindo a implantação, a configuração e o treinamento do novo software, conforme especificações constantes do **Termo de Referência** que integra este edital, como Anexo I.

.

I.1.1. Integram também o presente contrato, os termos e condições do Edital do Pregão Eletrônico SEADE 017/2016 e seus Anexos e a Proposta apresentada, aos quais se vincula.

CLÁUSULA II - DAS CONDIÇÕES DE EXECUÇÃO DOS SERVIÇOS

II.1 Os serviços deverão ser executados nas dependências da Fundação SEADE, devendo ser obedecido o prazo para a entrega e implantação da Solução e demais condições estabelecidas no Termo de Referência Anexo I do Edital da Licitação indicada no preâmbulo, correndo por conta da CONTRATADA as despesas de seguros, transporte, tributos, encargos trabalhistas e previdenciários decorrentes da execução do objeto do contrato.

CLÁUSULA III – DO VALOR E DOS RECURSOS

III.1. O valor total deste Contrato é de R$ _____ (valor por extenso), perfazendo o valor total de R$ _____ (valor por extenso), correspondendo ao presente exercício.

III.2. A despesa com a execução do presente contrato onerará os recursos consignados no Programa de Trabalho:_____, Natureza de Despesa: _____, Fonte: _____.

IV. DOS PAGAMENTOS

IV.1. O pagamento do valor será efetuado em parcela única, no prazo de 30 (trinta) dias (art. 2º do Decreto nº 32.117, de 10/08/1990 com a redação dada pelo Decreto nº 43.914, de 26/03/1999), contados da data da apresentação da nota fiscal/fatura (no caso de sábado domingo e feriado, será efetuado no primeiro dia útil subsequente), sem qualquer incidência de atualização monetária nesse período.

IV.2. As notas fiscais/faturas que apresentarem incorreções serão devolvidas à Contratada para as devidas correções e seu vencimento ocorrerá 30 (trinta) dias após a data de sua apresentação válida.

IV.3. Constitui condição para a realização dos pagamentos a inexistência de registros em nome da Contratada no “Cadastro Informativo dos Créditos não Quitados de Órgãos e Entidades Estaduais do Estado de São Paulo – CADIN ESTADUAL”, o qual deverá ser consultado por ocasião da realização de cada pagamento.

IV.4. O pagamento será feito mediante crédito aberto em conta corrente em nome da **CONTRATADA** no Banco do Brasil S/A, conforme disposto no Dec. nº. 55.357 de 18/01/2010.

IV.5. Havendo atraso nos pagamentos devidos pela **CONTRATANTE,** sobre o valor devido incidirá correção monetária nos termos do artigo 74 da Lei estadual nº 6.544/1989, bem como juros moratórios, à razão de 0,5% (meio por cento) ao mês, calculados *"pro rata tempore"* em relação ao atraso

CLÁUSULA V – DO PRAZO DE VIGÊNCIA CONTRATUAL

V.1. A validade das licenças será perpétua, porém as atualizações e versões das licenças terão validade de **12 (doze) meses.**

V.2. As atualizações e versões das licenças poderão ser renovadas por igual (ais) e sucessivo (s) período (s), a critério da Administração, até o limite de 48 (quarenta e oito) meses, nos termos e condições permitidos pela legislação vigente

V.3. A renovação das atualizações e novas versões do sistema, somente será formalizada caso os preços mantenham-se vantajosos para a FUNDAÇÃO SEADE e consistentes com o mercado, conforme pesquisa a ser realizada à época.

V.4. Eventual prorrogação de prazo será formalizada por meio de Termo de Prorrogação Contratual, respeitadas as condições prescritas na Lei 8666/93.

V.5. A CONTRATADA poderá se opor à prorrogação de que trata o item V.2 desta cláusula, desde que o faça mediante documento escrito, recepcionado pela FUNDAÇÃO SEADE com antecedência de 90 (noventa) dias do término do prazo do contrato.

V.6. A vigência contratual nos exercícios subsequentes ao da assinatura do contrato estará sujeita à condição resolutiva, consubstanciada na existência de recursos aprovados nas respectivas Leis Orçamentárias de cada exercício, para atender as respectivas despesas.

CLÁUSULA VI – DAS OBRIGAÇÕES DA CONTRATADA

VI.1 À CONTRATADA, além das obrigações constantes no Edital, Termo de Referência e Proposta Comercial, encontra-se subordinada às condições estabelecidas em cláusulas próprias deste instrumento, e daquelas estabelecidas em lei, em especial as definidas nos diplomas federal e estadual sobre licitações, cabendo:

a) Fornecer/assegurar o objeto indicado nas condições, no preço e prazo estipulados, considerando-se inclusas no valor do contrato todas as despesas concernentes aos serviços prestados, tais como encargos sociais, previdenciárias de seguro acidentes de trabalho, transporte e outras impostas pela legislação trabalhista, fiscal e comercial;

CLÁUSULA VII – DAS OBRIGAÇÕES DA CONTRATANTE

VII.1. Para a execução dos serviços objeto do presente contrato, a FUNDAÇÃO SEADE obriga-se:

a) Controlar e fiscalizar os serviços executados pela Contratada.
b) Designar um gestor responsável pelo acompanhamento da execução dos serviços resultantes deste Contrato.
c) Efetuar o pagamento devido, de acordo com o estabelecido neste contrato.

CLÁUSULA VIII – DO ACRÉSCIMO OU SUPRESSÃO

VIII.1. Na forma estabelecida pelo parágrafo 1º do artigo 65 da Lei Federal nº 8.666/93 e suas alterações, a Contratada fica obrigada a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões decorrentes da necessidade do material, até o limite de 25% (vinte e cinco por cento) do valor inicial pactuado, atualizado, mediante comunicação por escrito da Fundação Seade.

CLÁUSULA IX - DA GARANTIA CONTRATUAL

IXI.1. Não será exigida a prestação de garantia para a contratação.

CLÁUSULA X – DAS SANÇÕES PARA O CASO DE INADIMPLEMENTO

X. 1. Ficará impedida de licitar e contratar com a Administração direta e indireta do Estado de São Paulo, pelo prazo de até 5 (cinco) anos, a pessoa física ou jurídica, que praticar quaisquer atos previstos no artigo 7º da Lei Federal nº 10.520, de 17 de julho de 2002, c.c. o artigo 15 da Resolução CEGP-10 de 19 de novembro de 2002.

X.2. A sanção de que trata o subitem anterior poderá ser aplicada juntamente com as multas previstas na Resolução SEP nº 6, de 27/06/1990, garantido o exercício de prévia e ampla defesa, e deverá ser registrada no **CAUFESP** e no sítio **www.sancoes.sp.gov.br**

CLÁUSULA XI- DA RESCISÃO E RECONHECIMENTO DOS DIREITOS DA FUNDAÇÃO SEADE

XI.1. O contrato poderá ser rescindido, na forma, com as consequências e pelos motivos previstos nos artigos 75 a 82 da Lei Estadual nº 6.544/89 e artigos 77 a 80 e 86 a 88, da Lei Federal nº 8.666/93.

XI.1.1 - A CONTRATADA reconhece, desde já, os direitos da Fundação SEADE nos casos de rescisão administrativa, prevista no artigo 79 da Lei Federal n.º 8.666/93, e no artigo 77 da Lei Estadual nº 6.544/89.

CLÁUSULA XII – TRANSFERÊNCIA DO CONTRATO

XII.1. A CONTRATADA não poderá transferir o presente contrato, no todo ou em parte, nem poderá subcontratar os serviços ora contratados.

CLÁUSULA XIII - DOS CASOS OMISSOS

XIII.1. As eventuais omissões deste contrato aplicam-se os preceitos de Direito Público, dentre os quais as disposições da Lei federal nº 10.520, de 17 de julho de 2002; Decreto nº 49.722, de 24 de junho de 2005; regulamento anexo à Resolução nº CC-27, de 25/05/2006; Decreto estadual nº 47.297, de 06 de novembro de 2002; Resolução CEGP-10, de 19 de novembro de 2002; Lei Federal nº 8.666, de 21 de junho de 1993; Lei estadual nº 6.544, de 22 de novembro de 1989; Decreto estadual nº 52.205, de 27 de setembro de 2007; demais normas regulamentares da espécie e, supletivamente, os princípios da teoria geral dos contratos e disposições de direito privado, na forma prevista no "caput" do art. 54 da Lei 8.666/93.

CLÁUSULA XIV - DAS DISPOSIÇÕES GERAIS

XIV.1. Farão parte deste instrumento de contrato, mesmo que não expressamente declarado, as Condições Específicas do **Pregão Eletrônico nº 017/2016**, Termo de Referência e a proposta técnica comercial da CONTRATADA.

XIV.2. A CONTRATADA fica obrigada a manter-se durante toda a execução do presente Contrato, em compatibilidade com as obrigações assumidas, referente às condições de habilitação e qualificação exigidas na licitação, consoante determina o artigo 55, inciso XIII, da Lei Federal nº. 8.666, de 21 de junho de 1993.

Parágrafo único: Qualquer documentação pertinente ao objeto, bem como as demais referidas no caput, deverá ser encaminhada pela CONTRATADA à CONTRATANTE, sempre que solicitado e dentro do prazo por esta fixado.

CLÁUSULA XV – FORO

XV.1. As partes contratantes elegem, desde logo o Foro da Capital do Estado de São Paulo, para dirimir questão atinente ao presente contrato, com renúncia de qualquer outro, por mais privilegiado que seja.

E assim, por estarem as partes justas e contratadas, foi lavrado o presente instrumento, em 04 (quatro) vias de igual teor e forma, que, depois de lido e achado conforme, é assinado pelas partes para que produza todos os efeitos de direito, na presença das testemunhas abaixo identificadas.

São Paulo,

FUNDAÇÃO SISTEMA ESTADUAL DE ANÁLISE DE DADOS – SEADE

_____
DALMO DO VALLE NOGUEIRA FILHO
Diretor Executivo

EMPRESA CONTRATADA

_____
REPRESENTANTE LEGAL
Cargo

Testemunhas:

_____	_____
Nome:	Nome:
RG.:	RG.:

ANEXO IV

(PAPEL TIMBRADO DA LICITANTE)

DECLARAÇÃO

(nos termos do Decreto Federal nº 4.358/02, de 05 de Dezembro de 2002)

PREGÃO ELETRÔNICO SEADE Nº 017/2016

Eu (**nome completo)**, representante legal da empresa **(razão social da proponente)**, participante do processo licitatório, na modalidade de **PREGÃO ELETRÔNICO Nº 017/2016** da Fundação Sistema Estadual de Análise de Dados – SEADE, **declaro**, sob as penas da lei, que, nos termos do disposto no inciso V, do artigo 27, da Lei Federal 8.666/93, incluído pela Lei nº 9.854, de 1999, que não emprego menor de dezoito anos em trabalho noturno, perigoso ou insalubre e não emprego menor de dezesseis anos**.**

Ressalva: emprega menor, a partir de quatorze anos, na condição de aprendiz ( ).
Obs.: em caso afirmativo, assinalar com "x" a ressalva acima

Local e data

_____
Nome do representante legal
(com carimbo da empresa)

ANEXO V

(PAPEL TIMBRADO DA LICITANTE)

DECLARAÇÃO

(nos termos da Lei Estadual nº 10.218/99)

PREGÃO ELETRÔNICO SEADE Nº 017/2016

Eu (**nome completo)**, representante legal da empresa **(razão social da proponente)**, participante do processo licitatório, na modalidade de **PREGÃO ELETRÔNICO Nº 017/2016** da Fundação Sistema Estadual de Análise de Dados – SEADE, **declaro**, sob as penas da lei, que inexiste impedimento legal para licitar ou contratar com a Administração, inclusive em virtude das disposições da Lei Estadual nº 10.218, de 12.02.99.

Local e data

_____-
Nome do representante legal
(com carimbo da empresa)

ANEXO VI

(PAPEL TIMBRADO DA LICITANTE)

DECLARAÇÃO

(nos termos do artigo 117, parágrafo único da Constituição do Estado de São Paulo)

PREGÃO ELETRÔNICO SEADE Nº 017/2016

Eu (**nome completo)**, representante legal da empresa **(razão social da proponente)**, participante do processo licitatório, na modalidade de **PREGÃO ELETRÔNICO Nº 017/2016** da Fundação Sistema Estadual de Análise de Dados – SEADE, **declaro**, sob as penas da lei, que observo as normas relativas à saúde e segurança no trabalho, nos termos do parágrafo único, do artigo 117, da Constituição do Estado de São Paulo.

Local e data

_____
Nome do representante legal
(com carimbo da empresa)

ANEXO VII

(PAPEL TIMBRADO DA LICITANTE)

DECLARAÇÃO

PREGÃO ELETRÔNICO SEADE Nº 017/2016

Eu (**nome completo)**, representante legal da empresa **(razão social da proponente)**, participante do processo licitatório, na modalidade de **PREGÃO ELETRÔNICO Nº 017/2016** da Fundação Sistema Estadual de Análise de Dados – SEADE, **declaro**, sob as penas da lei, não ter dúvidas com relação à interpretação dos detalhes construtivos e das recomendações das especificações contidas no Termo de Referência do presente Edital.

Local e data

_____
Nome do representante legal
(com carimbo da empresa)

ANEXO VIII

RESOLUÇÃO SEP-6, de 27 de junho de 1990

Dispõe sobre a aplicação de multas previstas nos artigos 79, 80 e 81, inciso II da Lei 6.544, de 21/11/89

O Secretário de Estado de Economia e Planejamento resolve:

Artigo 1º - A aplicação das multas a que aludem os arts. 79, 80 e 81, inciso II, da Lei 6.544/89, obedecerá, no âmbito desta Secretaria de Economia e Planejamento, as seguintes normas.

SEÇÃO I

Da multa por atraso

Artigo 2º - O atraso injustificado na execução do contrato sujeitará o contratado à multa de mora, calculada por dia de atraso e, cumulativamente, sobre o Vlor da obrigação não cumprida, incluída a atualização contratual, se for o caso, na seguinte proporção:

a) atraso de até 30 dias, multa de 0,4%;

b) atraso superior a 30 dias, multa de 0,8%.

Parágrafo único – A reincidência na falta contemplada neste artigo ensejará a aplicação da multa em dobro.

Artigo 3º - Se objeto do contrato não for aceito, o contratado deverá substituí-lo ou providenciar a sua regularização dentro do prazo assinalado pela Administração, sob pena de sujeitar-se às multas do artigo anterior.

SEÇÃO II

Da multa por inexecução

artigo 4º - A inexecução total ou parcial do ajuste sujeita o contratado às seguintes penalidades, a serem aplicadas isolada ou cumulativamente:

I – multa de 10 a 30% calculada sobre o total ou parte da obrigação não cumprida;

II - multa correspondente à diferença de preço resultante da nova licitação efetuada para a realização ou complementação de obrigação não cumprida.

Artigo 5º - Previamente à imposição da multa contemplada no artigo anterior, será notificado o interessado facultando-lhe defesa prévia no prazo de 5 dias úteis do recebimento da notificação, nos termos do artigo 81 da Lei 6.544/89.

SEÇÃO III

Dos recursos

Artigo 6º - Da imposição das multas cabe recurso, no prazo de 5 dias úteis da intimação do ato, nos termos do artigo 83, inciso I, letra “c” da Lei 6.544/89.

SEÇÃO IV

Do pagamento das multas

Artigo 7º - Da aplicação da multa o adjudicatário ou contratado será notificado pessoalmente, por escrito, para que recolha ao Tesouro do Estado, no prazo de 7 dias úteis, o valor correspondente.

Parágrafo único – A multa será descontada dos pagamentos ou da garantia do respectivo contrato, ou cobrada judicialmente, sendo, em qualquer caso, o seu valor atualizado de acordo com o índice oficial de correção monetária a ser aplicado a partir da data na qual se verificou o seu inadimplemento.

SEÇÃO V

Disposições gerais

Artigo 8º - As disposições desta resolução aplicam-se a todos os contratos celebrados por esta Secretaria, inclusive os precedidos de dispensa de licitação ou declaração de sua inexigibilidade, nos termos da legislação vigente.

Artigo 9º - As multas estabelecidas nesta resolução não impedem que a Administração rescinda unilateralmente o contrato e aplique outras sanções previstas em lei.

Artigo 10 – A presente resolução entrará em vigor na data de sua publicação, ficando revogadas a Resolução SEP-1, de 17-8-79, retificada pela Resolução SEP-7, conforme publicação no DO de 22-8-79.