GOVERNO DO ESTADO DE SÃO PAULO
Secretaria de Planejamento e Gestão
SEADE
Fundação Sistema Estadual de Análise de Dados

EDITAL DE PREGÃO ELETRÔNICO SEADE n° 011/2015

EXPEDIENTE SEADE n° 093/2015

OFERTA DE COMPRA nº 291201290482015OC00064

ENDEREÇO ELETRÔNICO: www.bec.sp.gov.br ou www.bec.fazenda.sp.gov.br

DATA DO INÍCIO DO PRAZO PARA ENVIO DA PROPOSTA ELETRÔNICA: 27/08/2015

DATA E HORA DA ABERTURA DA SESSÃO PÚBLICA: 09/09/2015 às 10:00 horas

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 093/2015**, cujo objeto trata da **contratação de empresa para fornecimento de licenças do software antivírus utilizados na instituição para a versão *Cross Grade* – EPS X CEB, *McAfee Complete EndPoint Protection – Business* (CEB)** , de acordo com as especificações constantes do Termo de Referência, ANEXO I, **sob o regime de empreitada por preço unitário. O critério de julgamento será o de menor valor.** A contratação 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, aplicando-se, subsidiariamente, no que couberem, as 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 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 licenças do software antivírus utilizados na instituição para a versão *Cross Grade* – EPS X CEB, *McAfee Complete EndPoint Protection – Business* (CEB),** 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 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 cooperativas, 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 para abertura da sessão pública, 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 **unitário e total.**

3. O valor total remunerará todas as despesas com a prestação dos serviços e devem compreender todos os custos com mão de obra, encargos sociais e trabalhistas, seguros, transporte e demais despesas diretas e indiretas que onerem a prestação dos serviços.

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

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

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 ou ao domicílio 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 do 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, 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. QUALIFICAÇÃO TÉCNICA

a) Apresentar original ou cópia (s) autenticada (s) de atestado (s) em nome da licitante, emitido (s) por pessoa jurídica de direito público ou privado devendo conter a identificação do emitente, bem como o nome e o cargo do signatário, comprovando quantitativos de 50% a 60%, no mínimo, de prestação de serviços compatíveis com o objeto desta licitação em características, quantidades e prazos. Deverá constar do documento ainda, o endereço completo, inclusive eletrônico, se houver, do órgão/pessoa emitente, para eventuais esclarecimentos que se julgarem necessários.

a.1) Tais atestados deverão conter, necessariamente, a especificação dos serviços e o prazo de execução.

b) Declaração de Competência - Comprovação do licitante de que está apto a comercializar as soluções Mcafee. Esta comprovação será feita através de declaração oficial da Mcafee Brasil ou contrato de parceria.

c) Apresentar prospectos técnicos dos produtos, a fim de identificar o atendimento dos requisitos técnicos solicitados. Opcionalmente, a proponente poderá indicar na proposta o endereço eletrônico completo e direto de documentos técnicos em formato eletrônico que comprovem que os produtos propostos atendem as especificações técnicas deste Edital;

1.6. OUTRAS COMPROVAÇÕES

1.6.1. Declarações subscritas por representante legal da licitante, elaborada em papel timbrado, conforme modelos dispostos nos **ANEXOS IV, V, VI e VII** deste, atestando que:

a) Encontra-se em situação regular perante o Ministério do Trabalho, conforme disposto no Decreto estadual nº 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 n° 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 Termo de Referência do presente Edital.

2. DISPOSIÇÕES GERAIS

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 ao atendimento das condições estabelecidas neste Edital e seus anexos.

2.1. Serão desclassificadas as propostas:

a) cujo objeto não atenda às 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 contenham 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-se, em ambos os casos, a redução mínima entre eles de **R$ 800,00 (oitocentos reais),** aplicável, inclusive, em relação ao primeiro formulado, prevalecendo o primeiro lance recebido, quando ocorrerem 02 (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** da proposta.

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

4.2.1. A duração da etapa de lances será prorrogada automaticamente pelo sistema, visando à 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 admitido de cada 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 a 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 praticados no mercado, coerentes com a execução do objeto ora licitado.

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) 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 de fac-símile para o número (11) 3324-7223 ou por correio eletrônico indicado na sessão pública do Pregão.

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 a 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 Divisão Administrativa e de Suprimentos da FUNDAÇÃO SEADE, sito na Avenida Cásper Libero, 464 – 10º andar – sala 101 – Santa Ifigênia, 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 às 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 5 (cinco) dias úteis, contado a partir do momento em que a licitante for declarada vencedora do certame, prorrogável por igual período, a critério da Administração.

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 a 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 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 03 (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 Cásper Libero, 464 – 10º andar – sala 101 – Santa Ifigênia, nesta Capital.

2.1. Os memoriais de recurso e as contra razões 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 Divisão Administrativa e de Suprimentos da FUNDAÇÃO SEADE, sito à Avenida Cásper Líbero, 464 – 10º andar – sala 101 – Santa Ifigênia, 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 reiniciada somente após comunicação expressa às 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. DAS CONDIÇÕES DE EXECUÇÃO DOS SERVIÇOS

1. O objeto desta licitação deverá ser executado em conformidade com o estabelecido no Termo de Referência - **ANEXO I** deste Edital, correndo por conta da **CONTRATADA** as despesas de seguros, transporte, tributos, encargos trabalhistas e previdenciários decorrentes da execução do objeto do contrato.

IX – DAS CONDIÇÕES DE PAGAMENTO

1. O pagamento do valor será efetuado 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), mediante 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 do pagamento 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.

6. O valor da prestação devida pela FUNDAÇÃO SEADE será reajustado anualmente, mediante a aplicação da seguinte fórmula paramétrica:

$$R = Po.[(\frac{IPC}{IPCo}) - 1]$$

Onde:

R = parcela de reajuste

Po = preço inicial do contrato no mês de referência dos preços, ou preço do contrato no mês de aplicação do último reajuste.

IPC/IPCo = variação do IPC FIPE – Índice de Preço ao Consumidor, ocorrida entre o mês de referência de preços, ou no mês do último reajuste aplicado e o mês de aplicação do reajuste.

7. A periodicidade anual, de que trata o subitem 6 deste item IX, será contada a partir da data de apresentação da proposta.

X. 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 02 (dois) dias úteis, comprovar a sua situação de regularidade de que trata o subitem 1.1 deste item X, 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 X, 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 § 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 até 05 (cinco) dias corridos contados da data da convocação, comparecer à Divisão Administrativa e de Suprimentos sito na Av. Cásper Líbero, 464 10º andar sala 101 para assinar o termo de contrato.

3. Quando a Adjudicatária deixar de comprovar a regularidade fiscal, nos moldes dos subitens "10" e "11", ou na hipótese de invalidação do ato de habilitação com base no disposto na alínea "e", do subitem "9", todos 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, ambos 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 **05 (cinco)** 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. O contrato será celebrado com duração de **12 (doze) meses**, contados da data de sua assinatura.

5. O prazo mencionado no subitem anterior poderá ser prorrogado por iguais e sucessivos períodos, a critério das partes, até o limite de **48 (quarenta e oito) meses**, nos termos e condições permitidos pela legislação vigente.

5.1. A Contratada poderá se opor à prorrogação de que trata o subitem anterior, desde que o faça mediante documento escrito, formalmente recebido pela Fundação SEADE em até **90 (noventa) dias** antes do vencimento do contrato ou de cada uma das prorrogações do prazo de vigência.

5.2. As prorrogações de prazo de vigência serão formalizadas mediante celebração dos respectivos termos de aditamento ao contrato, respeitadas as condições prescritas na Lei Federal nº 8.666/1993.

5.3. A não prorrogação do prazo de vigência contratual por conveniência da Administração não gerará à contratada direito a qualquer espécie de indenização.

6. Não obstante o prazo estipulado nos subitens 4 e 5 deste item X, 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. A entrega do produto deverá ocorrer no prazo máximo de 15 (quinze) dias, a contar da assinatura do contrato e o prazo para implantação dos serviços não deverá ultrapassar 30 (trinta) dias a contar da entrega do produto;

XI. 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 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** e ainda comunicado o Tribunal de Contas do Estado de São Paulo – TCE-SP.

XII. DA GARANTIA CONTRATUAL

1. Não será exigida a prestação de garantia para a contratação resultante desta licitação.

XIII. 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, do regulamento anexo a Resolução CC-27/2006, a serem assinadas pelo Pregoeiro e pela equipe de apoio.

3. O sistema manterá sigilo quanto à 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 "enegociospublicos" e **www.bec.sp.gov.br** ou **www.bec.fazenda.sp.gov.br**, opção "pregao eletronico".

5. Até 02 (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, encontrado na opção EDITAL.

5.2 As impugnações serão respondidas pelo subscritor do Edital e os esclarecimentos e informações prestados pelo pregoeiro, no prazo de 01 (um) 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, 25 de agosto 2015.

_____
Lucia Regina dos Santos
Pregoeira

ANEXO I

TERMO DE REFERÊNCIA

1. DO OBJETO:

Aquisição de 350 licenças do software antivírus utilizado na Instituição para a versão *Cross Grade - EPS X CEB, McAfee Complete EndPoint Protection - Business (CEB),* contemplando serviços de instalação, Suporte Técnico e Manutenção, por um período de 12 (doze) meses**,** além de transferência de conhecimento (*Hands On*) para até 03 (três) analistas.

- VIGÊNCIA E PRORROGAÇÃO DO CONTRATO

O Contrato a ser firmado com a empresa vencedora da licitação, terá vigência de um ano a partir da data da assinatura, podendo ser prorrogado nos termos do inciso IV, do art. 57, da Lei nº 8.666/93 e suas alterações.

2. JUSTIFICATIVA E NECESSIDADE

As corporações que fazem uso ou oferecem serviços por meio da Internet devem ter extrema preocupação com esse canal de comunicação, pois além do benefício incontestável de permitir conectividade em âmbito global, também representa, em contrapartida, risco potencial de segurança à informação trocada entre os usuários.

Para que seja possível manter adequado nível de segurança nesse ambiente e assim preservar os ativos corporativos (*hardware, software* e dados), garantindo a integridade, confidencialidade e segurança das informações institucionais, torna-se imprescindível a adoção de soluções que minimizem os riscos e evitem prejuízos, não só em relação às questões que envolvem tecnologia, mas também de ordem financeira e da imagem institucional.

Nesse sentido, o emprego de soluções integradas de antivírus para servidores e estações de trabalho (computadores da rede interna), tem sido prática comum nas corporações, possibilitando monitorar e controlar o tráfego de dados, infestações e *e-mails* desnecessários que circulam entre a rede interna e a Internet, resultando em uma redução efetiva no risco, conforme já mencionado.

A contratação da solução completa e integrada de segurança é imprescindível para garantir as melhores práticas de Segurança da Informação em conformidade com as normas de referência dessa área, no âmbito da instituição. É indiscutível a necessidade de se manter a solução existente atualmente para estações de trabalho e servidores, denominada em âmbito interno de "antivírus corporativo" e composta por agentes integrados de antivírus nas estações de trabalho e gerenciadas por um servidor com a instalação do produto chamado EPO.

A facilidade de comunicação com a rede mundial de computadores aliada às dificuldades em manter uma política de segurança da informação que seja compreensível e fácil ao usuário final, resulta em um índice de infecção de *softwares* maliciosos, por vezes alto, em várias Instituições.

A solução atual de antivírus provê proteção constantemente atualizada contra grande parte dessas infecções, principalmente no que tange às estações de trabalho e equipamentos servidores de rede. Entretanto, o nível de proteção no uso de dispositivos móveis em nossa rede interna *tablets* utilizados pela PED e pela SUTIN para o desenvolvimento de sistemas.

O grande diferencial de uma solução integrada é proporcionar gerenciamento centralizado de todos os produtos da solução e proporcionar uma visão geral da segurança das redes internas da Instituição. Embora existam ferramentas no mercado para serem usadas individualmente e prover de modo não centralizado a maior parte das funcionalidades solicitadas nessa especificação, o uso de ferramentas de diferentes fabricantes para compor todo o conjunto de requisitos de segurança é reconhecidamente uma dificuldade quase intransponível, pois inviabiliza a gestão adequada de segurança pelos seguintes motivos:

- Necessidade de uma equipe de suporte técnico multidisciplinar para gerenciar todas as ferramentas. Muitas vezes é difícil descobrir a origem de um evento devido à falta de um técnico que saiba operar todas as ferramentas. Logo, se cada um detém conhecimento em uma ferramenta, é difícil integrar as informações. Com a solução completa e gerência centralizada de todos os dispositivos, a capacitação do pessoal se torna mais fácil, principalmente com a solicitação de suporte técnico da contratada para repasse de conhecimentos;

- Necessidade de instalação de diversos *softwares* de terceiros e vários agentes ou aplicativos nas estações de trabalho e servidores. A instalação de vários *softwares*, agentes ou aplicativos para prover um conjunto de funcionalidades que podem ser integradas em um único agente, além da falta de integração, pode ocasionar incompatibilidade entre os aplicativos. A instalação de diversos agentes coletores de informação também pode comprometer o desempenho da máquina e dificultar o suporte, pois pode ser difícil encontrar quem está gerando a incompatibilidade.

Outra deficiência detectada atualmente está relacionada a não conformidade de dispositivos que entram na rede com as normas de segurança, ABNT, ISO/IEEC. Diversas vezes são encontrados computadores sem atualizações de segurança do próprio sistema operacional, e até do antivírus e do sistema operacional instalados, que são responsáveis por disseminação de *vírus*, *malwares*, *worms e etc.*, comprometendo segurança e desempenho da rede interna. Para contornar essa deficiência, estão sendo incluídos no mesmo agente instalado nas estações de trabalho e servidores, módulos de controle de acesso à rede e de controle de dispositivos móveis, como por exemplo *pen-drive*.

Vale o registro de que a solução de segurança para navegação na *Web* atualmente utilizada por esta Fundação é o Firewall da empresa *Fortinet*, e é sabido que apenas um sistema de

firewall não é efetivo em todos os perímetros da segurança da Informação, Tal fato, por si só, reforça a necessidade pela aquisição de uma solução antivírus, para reforçar a segurança nesta área.

A compra de *software* ou equipamentos de um mesmo fabricante não é uma prática nova nas empresas e instituições, inclusive havendo previsão na Lei de Licitações pelas vantagens da padronização. Além dos pontos já amplamente citados anteriormente, podemos ainda citar os seguintes pontos que embasam tal afirmação:

- Compatibilidade, interoperabilidade e melhor gerência dos equipamentos;
- Unificar o contrato de assistência técnica e garantia, evitando que os fabricantes não assumam integralmente o problema;
- Menor necessidade de treinamento da equipe técnica;
- Aumento do nível de segurança pela possibilidade de correlação de eventos e maior acoplamento entre os produtos.

Informamos que o produto atualmente em uso por esta Fundação é fruto de uma licitação, ocorrida no ano de 2012. A opção pela eventual troca do produto suscita riscos e custos, conforme detalhado a seguir:

> O período de transição entre produtos distintos traz riscos à Instituição. Na eventual substituição do produto, é necessário fazer a remoção do *software* de antivírus existente em cada dispositivo (Servidor, estação de trabalho ou notebook). Embora os fabricantes anunciem que esse processo é totalmente automático, a prática mostra que em muitas ocasiões é necessária uma intervenção manual. Considerando que possuímos mais do que 350 dispositivos, o esforço de substituição é grande, assim como o tempo para concluir esse processo. Ainda no caso dos servidores de rede, embora tenhamos aproximadamente 90 (noventa), o risco de a troca causar uma parada de serviços é muito maior, assim como ocasionar perda de desempenho até que se concluam os ajustes finos e necessários.

A instalação de um produto de segurança novo causa impacto em outros sistemas e/ou produtos existentes. A instalação de uma nova solução de segurança traz reflexos na operação de outros produtos, tais como sistemas de *backup*, sistemas internos, armazenamento de arquivos e outros. O reflexo vai desde a perda de desempenho, por alguma configuração que deva ser refeita, até o mau funcionamento do sistema impactado. Embora tudo seja uma questão de ajuste, é necessário tempo e esforço a fim de que haja uma convergência para a normalidade de operação de todos os sistemas.

Quanto à necessidade de transferência de tecnologia para a equipe técnica da SUTIN, existe uma curva de aprendizado considerável em uma solução desse tipo e porte, visto que eventuais erros ou falhas na operação de tal sistema podem gerar resultados inesperados e talvez até graves à Instituição, tais como contaminação generalizada de computadores por

vírus ou outros tipos de *malwares* (*sofwares* maliciosos). Como consequências de uma contaminação em larga escala ou pontual podemos citar a perda ou vazamento de dados e a indisponibilidade de serviços (correio eletrônico, acesso à Internet, *site* oficial da Instituição, sistemas internos, entre outros), o que representa custos intangíveis, mas de grande monta.

No tocante à existência de licenças perpétuas do produto de antivírus para computador de mesa, vale ressaltar que o contrato vigente promoveu a aquisição de licenças perpétuas, sendo que a aquisição em tela, em relação a esse produto, refere-se apenas atualização tecnológica, por outro lado, tem-se, na nova versão, características e funcionalidades adicionais, como por exemplo, ao acessar um site "malicioso" um plugin no navegador emitirá um pop-up, informando o usuário que aquele site é suspeito; possibilidade de travar pen drives, podendo ser liberado acesso quando necessário.

Por fim, o eventual ganho econômico em uma aquisição de outro produto, caso ocorresse, seria pequeno se comparado com os riscos e custos associados à troca de uma plataforma de antivírus eficiente e eficaz como a existente. Ademais, sob a ótica dos princípios da razoabilidade, economicidade e eficiência, entendemos que o objeto solicitado na presente licitação seja o melhor a esta Fundação.

Além do exposto técnico acima e a grande importância de informações armazenadas nesta Instituição, e a necessidade de mantê-la inalterada, se faz necessário que a instituição tenha uma solução eficaz e confiável de antivírus instalada em todos os equipamentos, sendo estas estações de trabalho e/ou servidores, evitando a perda e/ou acesso indevido a informações sigilosas, bem como proteger documentos e e-mails que são enviadas às outras Secretarias.

O fabricante *McAfee* modificou a sua grade de produtos, incluindo uma gama de proteções mais eficazes e percebemos que se tornaram ainda mais adequadas a realidade da Fundação, que a suíte atual ***EPS.*** Solicitamos a aquisição do modelo ***Cross Grade - EPS X CEB, McAfee Complete End Point Protection - Business (CEB).***

A equipe técnica da Superintendência de TI efetuou um estudo das soluções e produtos disponíveis no mercado, e levando em consideração a estrutura física e lógica da rede, chegou-se à conclusão que a melhor opção e menos onerosa solução corporativa de software de segurança continua sendo a do fabricante *McAfee*.

Verificamos que existem no mercado vários fornecedores da solução McaFee, o que possibilita a participação de diversas empresas no processo licitatório e deve garantir um nível adequado de competição para a venda do software ao Seade.

Consultando sites de comparativos entre soluções de antivírus temos a figura abaixo, que confirma nossa constatação:

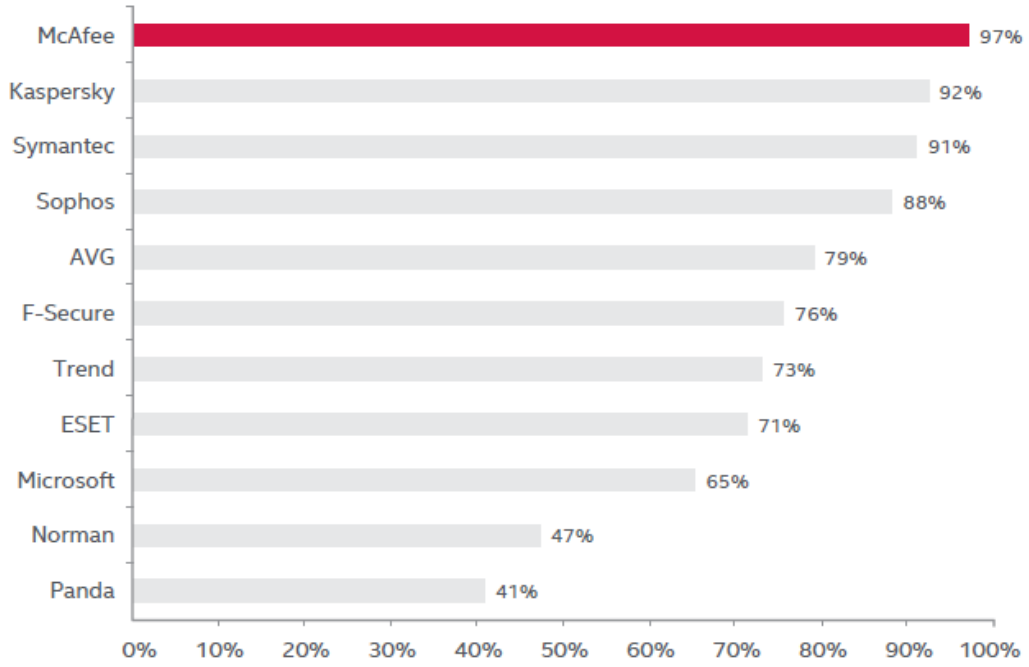

Figura 1. Taxas de bloqueio combinadas (incluindo vetores alternativos)
Fonte: Relatório da NSS Labs — *Corporate AV / EPP Comparative Analysis* (Análise comparativa de AV / EPP corporativos), 2013

A tabela a seguir apresenta os tipos de *anti-malwares* necessários aos equipamentos da Fundação Seade, bem como as quantidades:

Equipamentos	Finalidade	Quant.
Servidores Windows (CEB)	Proteger servidores conectados diretamente a rede mundial de computadores que abrigam sites com sistemas internos e seus respectivos bancos de dados, web-servers além de proteger os mesmos de forma automática, impedindo que pragas eletrônicas vindas de fora, por meio de: pen-drives, CD/DVD, internet, e-mail, etc.	30
Servidores Linux (McAfee Virusscan-for-linux)	Proteger informações de bancos de dados *mySql*, *postgree*, Web-servers de produção, e-mail, desenvolvimento e homologação, além de proteger os mesmos de forma automática, impedindo que pragas eletrônicas vindas de fora, por meio de: pen-drives, CD/DVD, internet, e-mail, etc	60
Estações/notebooks (CEB)	Proteger as estações de trabalho de forma automática, impedindo que pragas eletrônicas vindas de fora, por meio de: pen-drives, CD/DVD, internet, e-mail, etc.	260

3. CARACTERÍSTICAS SOLICITADAS

3.1. Console de Gerenciamento:

3.1.1. Administração centralizada por console único de gerenciamento;

3.1.2. As configurações do Antivírus, AntiSpyware, Firewall, Proteção Contra Intrusos, controle de Dispositivos e Controle de Aplicações deverão ser realizadas para maquinas físicas e virtuais através da mesma console;

3.1.3. Toda a solução deverá funcionar com agente único na estação de trabalho, servidores físicos e virtuais a fim de diminuir o impacto ao usuário final;

3.1.4. Console de gerenciamento via tecnologia Web (HTTP e HTTPS);

3.1.5. Implementar console de gerenciamento e monitoramento centralizado através de single-sign-on (SSO) das soluções abaixo:

3.1.5.1. Solução segurança de estação de trabalho e servidores ("endpoint") físicos e virtuais;

3.1.5.2. IPS para Servidores e Estações;

3.1.5.3. Controle de conteúdo/Antivírus WEB;

3.1.5.4. Prevenção de Antispam e AntiVirus para Gateway e Servidores de E-mail;

3.1.5.5. Prevenção contra perda de dados;

3.1.5.6. Solução de Criptografia de Pastas, Disco Rígido e Dispositivos Removíveis;

3.1.5.7. Solução de Conformidade e Validação de Configuração;

3.1.6. Mecanismo de comunicação (via push) em tempo real entre servidor e clientes, para entrega de configurações e assinaturas;

3.1.7. Mecanismo de comunicação randômico (via pull) em tempo determinado pelo administrador entre o cliente e servidor, para consulta de novas configurações e assinaturas evitando sobrecarga de rede e servidor;

3.1.8. Permitir a divisão lógica dos computadores, dentro da estrutura de gerenciamento, em sites, domínios e grupos, com administração individualizada por domínio;

3.1.9. O servidor de gerenciamento deverá possuir compatibilidade para instalação nos sistemas operacionais Microsoft Windows Server 2008, 2008 R2 e Windows Server 2012;

3.1.10. O servidor de gerenciamento deverá possuir compatibilidade para instalação em sistemas operacionais de 64-bits suportando ambiente virtual VMWARE 5.5 e Microsoft;

3.1.11. Possuir integração com LDAP, para importação da estrutura organizacional e autenticação dos Administradores;

3.1.12. Possibilidade de aplicar regras diferenciadas baseando na localidade lógica da rede;

3.1.13. Permitir que a localidade lógica da rede seja definida pelo conjunto dos seguintes itens:

3.1.13.1. IP e range de IP;

3.1.13.2. Endereço de Servidores de DNS, DHCP e WINS;

3.1.13.3. Conexão com o servidor de gerência;

3.1.13.4. Conexões de rede como VPN, Ethernet, Wireless e Modem;

3.1.14. Possibilidade de aplicar regras diferenciadas por grupos de usuários e maquinas;

3.1.15. O servidor de gerenciamento deverá permitir o uso de banco de dados relacional Microsoft SQL Server nas versões 2005, 2008 ou 2012; As licenças de banco de dados necessárias para o bom e correto funcionamento do servidor de gerenciamento, deverão ser fornecidas juntamente com a solução.

3.1.16. Possuir a funcionalidade e recursos para a criação e agendamento periódicos de backups da base de dados ou fornecer uma ferramenta para tal finalidade;

3.1.17. Permitir a opção instalação de Servidores de Gerenciamento adicionais fornecendo assim a possibilidade de trabalhar em modo de Load Balance e Failover;

3.1.18. Possuir na solução replicação nativa do Banco de Dados entre os Servidores de Gerenciamento com opção de customização do conteúdo à ser replicado (Assinaturas, Pacotes de Instalação, Políticas e Logs);

3.1.19. Possibilidade de instalação dos clientes em servidores, estações de trabalho e maquinas virtualizadas de forma remota via console de gerenciamento com opção de remoção de soluções previamente instaladas;

3.1.20. Permitir a instalação remota do software por Group Policy (GPO), Web e via console de gerenciamento;

3.1.21. Descobrir automaticamente as estações da rede que não possuem o cliente instalado;

3.1.22. Fornecer ferramenta de pesquisa de estações e servidores da rede que não possuem o cliente instalado com opção de instalação remota;

3.1.23. Fornecer atualizações do produto e das definições de vírus e proteção contra intrusos;

3.1.24. A console de gerenciamento deve permitir travar as configurações por senha nos clientes servidores e estações físicas e virtuais, definindo permissões para que somente o administrador possa alterar as configurações, desinstalar ou parar o serviço do cliente;

3.1.25. A console de gerenciamento deve permitir ao administrador travar separadamente os itens e cada subitem de acesso as configurações do cliente;

3.1.26. Capacidade de criação de contas de usuário com diferentes níveis de acesso de administração e operação;

3.1.27. Instalação e atualização do software sem a intervenção do usuário;

3.1.28. Possibilidade de configurar o bloqueio da desinstalação, desabilitar o serviço do cliente, importar e exportar configurações e abrir a console do cliente, por senha;

3.1.29. Suportar redirecionamentos dos logs para um servidor de Syslog;

3.1.30. Utilizar os protocolos **HTTP** e **HTTPS** para comunicação entre console de gerenciamento e o cliente gerenciado;

3.1.31. Possuir certificação *FIPS 140-2*;

3.1.32. Possuir certificação *Common Criteria* (CC) EAL2+;

3.1.33. O **fabricante** deverá possuir certificação *ICSA Labs* no mínimo nas plataformas Windows XP, Windows e Windows 7;

3.2. Atualização de Vacinas

3.2.1. Atualização incremental, remota e em tempo real, da vacina dos Antivírus, mecanismo de verificação (*engine*) e dos clientes da rede;

3.2.2. Permitir criar planos de distribuição das atualizações via comunicação segura entre cliente e Servidores de Gerenciamento, site do fabricante, via servidor de atualização interno e podendo eleger qualquer cliente gerenciado para distribuição das atualizações;

3.2.3. Permitir eleger qualquer cliente gerenciado como um servidor de distribuição das atualizações com opção de controle de banda, quantidades de definições e espaço em disco utilizado, podendo eleger mais de um cliente para esta função;

3.2.4. Atualização remota e incremental da versão do software cliente instalado;

3.2.5. Nas atualizações das configurações e das definições de vírus não poderá utilizar login scripts, agendamentos ou tarefas manuais ou outros módulos adicionais que **NÃO** sejam parte integrante da solução e sem requerer reinicialização do computador ou serviço para aplicá-la;

3.3. Quarentena

3.3.1. Possuir funcionalidades que permitam o isolamento (área de quarentena) de arquivos contaminados por códigos maliciosos que não sejam conhecidos ou que não possam ser reparados em um servidor central da rede;

3.3.2. Forma automática de envio dos arquivos da área de isolamento central para o fabricante, via protocolo seguro, onde este será responsável por gerar a vacina, automaticamente, sem qualquer tipo de intervenção do administrador. Recebimento utilizando o mesmo método e aplicação da vacina recém criada nas estações infectadas;

3.3.3. Possibilidade de adicionar manualmente arquivos na quarentena do cliente com opção de restrições na console de gerenciamento;

3.4. Cliente Gerenciado

3.4.1. Suportar máquinas com arquitetura 32-bits e 64-bits;

3.4.2. O cliente para instalação em estações de trabalho e servidores deverá possuir compatibilidade com os sistemas operacionais Microsoft Windows XP, 2003, 2008, 2008 R2, 7 e 8, Linux Red Hat Enterprise 5.x e 6.x, CentOS 6.4, 6.5 e versão 7;

3.5. Funcionalidade de Firewall e Detecção e Proteção de Intrusão (IDS\IPS) com as seguintes funcionalidades:

3.5.1. Suporte aos protocolos TCP, UDP e ICMP;

3.5.2. Reconhecimento dos tráficos DNS, DHCP e WINS com opção de bloqueio;

3.5.3. Possuir proteção contra exploração de buffer overflow;

3.5.4. Possuir proteção contra ataques de Denial of Service (DoS), Port-Scan e MAC Spoofing;

3.5.5. Possibilidades de criação de assinaturas personalizadas para detecção de novos ataques;

3.5.6. Possibilidade de agendar a ativação da regra de Firewall; 3.5.7. Possibilidade de criar regras diferenciadas por aplicações;

3.5.8. Gerenciamento integrado à console de gerência da solução;

3.5.9. Possibilidade de reconhecer automaticamente as aplicações utilizadas via rede baseado no *fingerprint* do arquivo;

3.5.10. Proteger o computador através da criação de uma impressão digital para cada executável existente no sistema, para que somente as aplicações que possuam essa impressão digital executem no computador (*Whitelist*);

3.5.11. Proteger o computador através da criação de uma impressão digital para cada executável existente no sistema, com o intuito de bloquear as ações de tais executáveis (*Blacklist*);

3.5.12. Permitir criação de zona confiável, permitindo que determinados IPs, protocolos ou aplicações se comuniquem na rede;

3.5.13. Bloqueio de ataques baseado na exploração da vulnerabilidade;

3.5.14. Capacidade de executar varreduras em tempo real (real-time) contra ataques dirigidos às vulnerabilidades do navegador (*browser*);

3.6. Funcionalidade de *Antivírus* e *AntiSpyware*:

3.6.1. Proteção em tempo real contra vírus, *trojans, worms, spyware, adwares* e outros tipos de códigos maliciosos;

3.6.2. Proteção *antispyware* deverá ser nativa do próprio antivírus, ou seja, não dependente de plugin ou módulo adicional;

3.6.3. As configurações do antispyware deverão ser realizadas através da mesma console de todos os itens da solução;

3.6.4. Permitir a configuração de ações diferenciadas para cada subcategoria de riscos de segurança (*Adware*, Discadores, Ferramentas de hacker, Programas de brincadeiras, Acesso Remoto, *Spyware*, *Trackware* e outros);

3.6.5. Permitir a configuração de duas ações, primária e secundária, executadas automaticamente para cada ameaça, com as opções de: somente alertar, limpar automaticamente, apagar automaticamente e colocar em quarentena;

3.6.6. Permitir a criação de listas de exclusões com informação da severidade, impacto e grau de remoção da ameaça nos níveis baixos, médio ou alto, onde os riscos excluídos não serão verificados pelo produto;

3.6.7. Permitir verificação das ameaças da maneira manual, agendada e em tempo real, detectando ameaças no nível do *kernel* do Sistema Operacional, fornecendo a possibilidade de detecção de *rootkits*;

3.6.8. Capacidade de realizar monitoramento em tempo real (real-time) por heurística correlacionando com a reputação de arquivos;

3.6.9. Capacidade de verificar a reputação de arquivos, correlacionando no mínimo as seguintes características:

3.6.9.1. Origem confiável;

3.6.9.2. Origem não confiável;

3.6.9.3. Tempo de existência do arquivo na internet;

3.6.9.4. Comportamento do arquivo;

3.6.9.5. Quantidade mínima de usuários que baixaram o arquivo da internet;

3.6.10. Implementar intervalos de tempo para início de verificações agendadas de forma a reduzir impacto em ambientes virtuais;

3.6.11. Possuir funcionalidades que permitam o isolamento (área de quarentena) de arquivos contaminados por códigos maliciosos que não sejam conhecidos ou que não possa ser reparado no cliente;

3.6.12. Possuir funcionalidades que permitam a inclusão manual em isolamento (área de quarentena) de arquivos a serem enviados e vistoriados pelo centro de pesquisa do fabricante;

3.6.13. Permitir configurar ações a serem tomadas na ocorrência de ameaças, incluindo Reparar, Deletar, Mover para a Área de Isolamento e Ignorar;

3.6.14. Verificação de vírus nas mensagens de correio eletrônico, pelo antivírus da estação de trabalho, suportando clientes Outlook, Notes e POP3/SMTP;

3.6.15. Possuir funcionalidades que permitam a detecção e reparo de arquivos contaminados por códigos maliciosos mesmo que sejam compactados, tendo como abrangência até o 10º (décimo) nível de compactação;

3.6.16. Capacidade de detecção em tempo real de vírus novos, desconhecidos pela vacina com opção de ajuste da sensibilidade de detecção;

3.6.17. Capacidade de remoção automática total dos danos causados por *spywares, adwares e worms*, como limpeza do registro e pontos de carregamento, com opção de terminar o processo e terminar o serviço da ameaça no momento de detecção;

3.6.18. A remoção automática dos danos causados deverá ser nativa do próprio antivírus, ou seja, não dependente de *plugin*, execução de arquivo ou módulo adicional;

3.6.19. Capacidade de identificação da origem da infecção, para vírus que utilizam compartilhamento de arquivos como forma de propagação informando nome ou IP da origem com opção de bloqueio da comunicação via rede;

3.6.20. Possibilidade de bloquear verificação de vírus em recursos mapeados da rede, por senha;

3.6.21. Criar uma cópia backup do arquivo suspeito antes de limpá-lo;

3.6.22. Gerenciamento integrado à console de gerência da solução;

3.6.23. Possibilitar a criação de um disco (CD ou DVD) inicializável para verificação e remoção de ameaças sem a necessidade de carregar o Sistema Operacional do cliente;

3.7. Funcionalidade de detecção proativa de reconhecimento de novas ameaças com as funcionalidades:

- 3.7.1. Funcionalidade de detecção de ameaças desconhecidas que estão em memória por comportamento dos processos e arquivos das aplicações;

- 3.7.2. Não utilizar a assinatura de vírus para esta funcionalidade e fornecer atualizações periódicas da técnica de detecção;
- 3.7.3. Capacidade de detecção Keyloggers, Trojans, Spyware e Worms por comportamento dos processos em memória, com opção da sensibilidade distintas da detecção;
- 3.7.4. Reconhecimento de comportamento malicioso de modificação da configuração de DNS e arquivo de Hosts;
- 3.7.5. Possuir a funcionalidade de exclusão de detecção diferenciada do recurso de Antivírus;
- 3.7.6. Possibilidade de habilitar o recurso de correlacionamento da funcionalidade de detecção proativa com a base de reputação do fabricante;

3.8. Funcionalidade de Controle de Dispositivos e Aplicações:

- 3.8.1. Gerenciar o uso de dispositivos USB e CD/DVD, através de controles de leitura/escrita/execução do conteúdo desses dispositivos e também sobre o tipo de dispositivo permitido (ex: permitir mouse USB e bloquear disco USB);

3.9. Proteções para ambientes virtualizados

- 3.9.1. Capacidade de identificar automaticamente maquinas virtuais e físicas, possibilitando a criação de regras especificas por tipo de ambiente (virtual ou físico);
- 3.9.2. Suportar as mesmas funcionalidades existentes para o ambiente físico no ambiente virtual, contemplando os virtualizadores VMware e Microsoft sem a necessidade de instalar outro agente, software, modulo e/ou plugins;
- 3.9.3. Cache compartilhado de reputação e resultado de varredura de arquivos, possibilitando exclusão automática de varredura de arquivos categorizados como não maliciosos e já escaneados anteriormente;
- 3.9.4. Capacidade de identificar "templates" de máquinas virtuais, marcando seus arquivos já verificados eliminando a necessidade de verificar esses arquivos todas as vezes que o template for clonado;
- 3.9.5. Capacidade de implementar varreduras otimizadas em máquinas físicas e virtuais, onde o arquivo verificado pela varredura uma vez, não será verificado novamente, até que ocorra alguma alteração no mesmo;
- 3.10. Relatórios e Monitoramentos
    - 3.10.1. Possuir pelo menos 10 tipos de relatórios diferentes, permitindo a exportação para o formato HTML;

- 3.10.2. Recursos do relatório e monitoramento deverão ser nativos da própria console central de gerenciamento;
- 3.10.3. Possibilidade de exibir a lista de servidores e estações que possuam o antivírus instalado, contendo informações como nome da máquina, usuário logado, versão do antivírus, versão do engine, data da vacina, data da última verificação e status;
- 3.10.4. Capacidade de Geração de relatórios, estatísticos e gráficos contendo no mínimo os seguintes tipos pré-definidos:
  - 3.10.4.1. As 10 máquinas com maior ocorrência de códigos maliciosos;
  - 3.10.4.2. Os 10 usuários com maior ocorrência de códigos maliciosos;
  - 3.10.4.3. Localização dos códigos maliciosos;
  - 3.10.4.4. Sumários das ações realizadas;
  - 3.10.4.5. Número de infecções detectadas diário, semanal e mensal; 3.10.4.6. Códigos maliciosos detectados.

- 3.11. Modulo de Integração com Console avançada de distribuição e relatórios já existente com a seguintes características:
  - 3.11.1. Console de gerenciamento via tecnologia Web (HTTP ou HTTPS) independente da console central da solução;
  - 3.11.2. Detectar e desinstalar soluções de antivírus dos seguintes fabricantes:
    - 3.11.2.1. CA
    - 3.11.2.2. ESET
    - 3.11.2.3. F-Secure
    - 3.11.2.4. Kaspersky
    - 3.11.2.5. Sophos
    - 3.11.2.6. Symantec
    - 3.11.2.7. Trend Micro
  - 3.11.3. Permitir a remoção de outros softwares não desejados;
  - 3.11.4. Criar tarefas de migração baseadas no resultado do inventário de antivírus;
  - 3.11.5. Disparar comandos de verificações de ameaças nos clientes a partir da console do inventário;
  - 3.11.6. Permitir a instalação do agente de antivírus com agendamento e implementar controle de banda para minimizar impacto na rede;
  - 3.11.7. Possibilidade de recuperar instalação em clientes em caso de falha;

- 3.11.8. Exibir na console do inventário informações do ambiente de antivírus como falhas de varredura e autoproteção;
- 3.11.9. Oferecer relatórios avançados através da criação de cubos OLAP e tabelas Pivot;
- 3.11.10. Os seguintes cubos devem ser disponibilizados para criação de relatórios:
  - 3.11.10.1. Alertas;
  - 3.11.10.2. Clientes;
  - 3.11.10.3. Políticas;
  - 3.11.10.4. Rastreamento;
- 3.11.11. Possibilidade de criação de indicadores de performance para medir eficácia da solução de segurança
- 3.11.12. Exportar os relatórios criados nos formados xls, pdf e html;

4. MANUTENÇÃO E SUPORTE TÉCNICO

- 4.1. A contratada oferecerá garantia do suporte técnico e atualização do objeto contratado, que forem lançados no mercado durante 12 (doze) meses, a partir da assinatura do contrato, na forma prevista neste Termo de Referência que integra o edital.
- 4.2. O serviço de suporte técnico deverá fornecer suporte corporativo telefônico, em português, sem custo adicional, ilimitado, com regime 8X5 durante o período de contrato, das 09:00 as 18:00;
- 4.3. O início do atendimento não poderá ultrapassar o prazo de 4 (quatro) horas, contado a partir da abertura do chamado;
- 4.4. O tempo de solução será de até 24 (vinte e quatro) horas. Para problemas desconhecidos, que depender de resposta do fabricante, este tempo poderá ser maior, com autorização prévia da SUTIN, e após o comprovante de registro de suporte no fabricante, pela contratada. Neste segundo caso o registro deverá ser aberto na primeira hora após o vencimento do tempo de solução.
- 4.5. A CONTRATANTE poderá abrir chamados e consultar o andamento dos mesmos pelo site e/ou Serviço de Atendimento ao Cliente (SAC) do fabricante;
- 4.6. O serviço de suporte técnico deverá fornecer acesso gratuito às atualizações de conteúdo do produto, incluindo as vacinas contra vírus de computador e o filtro antispam da Suite;

- 4.7. O serviço de suporte técnico deverá fornecer acesso gratuito a correções do software (patches) e melhorias do produto (updates);
- 4.8. O serviço de suporte técnico deverá fornecer atualização gratuita do software em caso de mudança de versão (upgrade), durante o período de vigência do contrato;
- 4.9. A Superintendência de TI poderá disponibilizar, caso ache necessário, canal de atendimento por acesso remoto, através de conexão via Internet (Web), mediante autorização prévia da Superintendência de TI da Fundação Seade;
- 4.10. Será disponibilizado um banco de horas para atendimento local com a limitação pré-estabelecida de 4 (quatro) horas mês não cumulativas, para casos em que não sejam resolvidos o problema por telefone, e-mail ou através do suporte remoto, será enviado um técnico ao local da instalação em até 48 horas contados a partir do término de atendimento.
- 4.11. O suporte técnico será prestado nos dias úteis, em horário comercial, das 09:00 as 18:00 com atendimento por técnicos especializados para dirimir dúvidas de configuração e utilização do software, sem limitação para o número de chamadas;

5. Serviços de instalação, configuração, documentação e Treinamento Hands On

5.1 Instalação, Configuração e Documentação

Os serviços de instalação e configuração dos produtos, deverão ser acordados previamente e acompanhamento de analista da Fundação. Antes da execução dos serviços, deverá ser elaborado um plano de trabalho, com cronograma e previsão para início e conclusão das tarefas; Esse plano deverá ser previamente aprovado pela equipe técnica da Superintendência de TI, antes de ser implementado; Toda instalação deverá ser feita on site

McAfee Complete EndPoint Protection - Business (CEB)

Instalação das ferramentas especificadas, CEB, em no mínimo 12 (doze) equipamentos (Endpoints), um por andar, onde todas as soluções serão administradas a partir de um único servidor de administração – chamado EPO.

Instalação, e configuração do EPO no servidor disponibilizado pela área de Informática;

Serão 12 (doze) computadores que receberão a instalação da ferramenta de antivírus atualizada, uma máquina em cada andar, 02 (dois) servidores, um Microsoft e outro Linux CentOS, e a configuração do servidor gerenciador dos clientes das estações de trabalho e

servidores (EPO), e com a transferência de conhecimento para os três analistas de rede da Instituição farão as demais atualizações;

Depois de concluída a instalação será necessário fazer o *deploy* do novo agente para os 12 (doze) computadores.

Instalação e configuração do ***McAfee Virusscan-for-linux*** **em pelo menos um servidor com versão CentOS do Sistema Operacional Linux;**

Ao final da instalação / configuração, a licitante deverá entregar a documentação completa e detalhada dos serviços executados;

5.2. Treinamento

Deverá ser fornecido treinamento dos produtos ofertados, na modalidade **hands on**, para todas as ferramentas implementadas para até 03 pessoas, a serem designadas pela Superintendência de TI, onde deve contemplar:

Estratégias de implantação de regras de segurança e gerenciamento e monitoramento no Servidor EPO, tratando basicamente dos módulos de manutenção e de epidemia de vírus.

- Desenvolver estratégia para a distribuição do Agente do ePO nos desktops e servidores da empresa;
- Desenvolvimento de política de segurança para desktop;
- Desenvolvimento de estratégia de atualizações de agentes, a fim de minimizar o impacto na rede e no desempenho dos desktops;
- Interpretação e programação dos relatórios do ePO;
- Procedimentos de contenção de epidemias (outbreaks)

6. CONSIDERAÇÕES DE PARTICIPAÇÂO

Considerando a contratação de empresa para o fornecimento de Solução Corporativa de Software de Segurança e como forma de garantir a qualidade do fornecimento e dos serviços a serem prestados a licitante deverá apresentar na fase de habilitação, os seguintes documentos:

6.1 - Declaração de Competência - Comprovação do licitante de que está apto a comercializar as soluções Mcafee. Esta comprovação será feita através de declaração oficial da Mcafee Brasil ou contrato de parceria.

6.2 - Comprovar que prestou ou presta serviços similares ao objeto deste Termo de Referência em empresas privadas ou órgãos da administração pública direta ou indireta. A comprovação deverá ser através da apresentação de pelo menos 01 (um) documento.

7. CONDIÇÕES GERAIS

7.1. PRAZOS

A entrega do produto deverá ocorrer no prazo máximo de 15 (quinze) dias, a contar da assinatura do contrato.

O prazo para implantação dos serviços não deverá ultrapassar 30 (trinta) dias a contar da entrega do produto;

7.1.1. GARANTIA

- A contratada obriga-se a fornecer o objeto deste contrato com garantia técnica de suporte técnico e atualização (*updates e releases*) de, no mínimo, 12 (doze) meses, observado o prazo maior oferecido pelo fabricante no mercado, a contar do recebimento definitivo.

7.2. Obrigações da Contratante

A **Fundação SEADE** compromete-se em ceder os profissionais e os recursos necessários para a implantação das soluções adquirida e dar o apoio necessário ao gerenciamento e a aprovação formal dos resultados.

7.3. Local de entrega

Todas as licenças devem ser entregues na Fundação Seade, localizada na AV. Cásper Líbero, 464, Centro - São Paulo/SP - CEP 01033- 000, aos cuidados da SUTIN.

- Superintendência de Tecnologia da Informação, ou diferente do indicado e dentro do perímetro urbano, conforme aviso da SUTIN.

As licenças serão tecnicamente aceitas pela SUTIN que emitirá Termo Recebimento Definitivo ou Recibo.

7.4. Apresentação de Prospectos

Devem ser enviados prospectos técnicos dos produtos, a fim de identificar o atendimento dos requisitos técnicos solicitados, na fase de habilitação. Opcionalmente, a proponente poderá indicar na proposta o endereço eletrônico completo e direto de documentos técnicos em

formato eletrônico que comprovem que os produtos propostos atendem as especificações técnicas deste Edital;

8. CONSIDERAÇÕES E CONCLUSÃO

Com a aquisição e instalação de software de antivírus os seguintes benefícios serão agregados aos usuários desta Instituição:

Mitigar a problemas causados por vírus, trojans, spywares e malwares às estações de trabalho, mantendo ama maior integridade de arquivos em geral, documentos, planilhas, imagens, projetos, etc. Manter a integridade do sistema operacional utilizado nas estações, evitando falhas, abertura de portas e lentidão por processos desnecessários.

Mitigar que por meio de brechas do sistema operacional servidores possam ser invadidos; mitigar integridade de todo e qualquer dado (arquivos/sistemas internos), impedir que informações (arquivos) passados a outras secretarias possam estar infectados propagando pragas na rede Internet.

São Paulo, 25 de agosto de 2015.

Vivaldo Luiz Conti
Superintendente de Tecnologia da Informação

ANEXO II

MODELO DE PROPOSTA COMERCIAL

PREGÃO ELETRÔNICO Nº 011/2015

EXPEDIENTE SEADE Nº 093/2015

Item	Descrição	Quant	Valor Unit	Valor Total
01	Licenças do software antivírus versão Cross Grade – EPS X CEB – McAfee Complete EndPoint Protection – Business	**350**	R$_____	R$_____
02	Serviços de instalação, configuração, treinamento, suporte técnico e manutenção.	**1**	R$_____	R$_____
			TOTAL	**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.***

2) *Declaramos estar de acordo com todos os termos do Edital e seus Anexos que dele fazem parte integrante, bem como não existir nenhum fato impeditivo para celebrar Contrato com a Administração.*

3) *Prazo de vigência do Contrato: 12 (doze) meses, a contar de sua assinatura, prorrogável nos termos da Lei Federal nº 8.666/93.*

_____
Assinatura do Representante legal

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

ANEXO III

MINUTA DE CONTRATO

EXPEDIENTE SEADE ***Nº 093/2015***
CONTRATO Nº___ /2015

CONTRATO EM QUE ENTRE SI CELEBRAM A **FUNDAÇÃO SISTEMA ESTADUAL DE ANÁLISE DE DADOS - SEADE** E A EMPRESA **_____,** OBJETIVANDO A CONTRATAÇÃO DE EMPRESA PARA **FORNECIMENTO DE 350 LICENÇAS DO SOFTWARE ANTIVÍRUS UTILIZADO NA INSTITUIÇÃO PARA A VERSÃO *CROSS GRADE - EPS X CEB, MCAFEE COMPLETE ENDPOINT PROTECTION - BUSINESS (CEB),* CONTEMPLANDO SERVIÇOS DE INSTALAÇÃO, SUPORTE TÉCNICO, MANUTENÇÃO E TRANSFERÊNCIA DE CONHECIMENTO.**

Pelo presente instrumento, de um lado a **FUNDAÇÃO SISTEMA ESTADUAL DE ANÁLISE DE DADOS - SEADE**, CNPJ nº 51.169.555/0001-00, Inscrição Estadual nº 110.199.866.112, com sede na Av. Cásper Líbero, 464, nesta Capital, doravante denominada FUNDAÇÃO SEADE, neste ato representada por sua Diretora Executiva, **Dra*. MARIA HELENA GUIMARÃES DE CASTRO***, de outro lado, a **_____,** doravante denominada CONTRATADA, com sede na _____, CNPJ nº _____, neste ato representada por seu _____, Sr. _____, têm entre si justo e contratado, na melhor forma de direito, o presente contrato de prestação de serviços, decorrente do **Pregão Eletrônico nº 011/2015**, sujeitando-se às normas da Lei Federal 8.666/93, da Lei Estadual 6.544/89, da Lei Federal nº 10.520/02, Decreto Estadual nº 49.722/05, Decreto Estadual 47.297/02, Resolução CEGP-10, de 19/11/02 e demais normas regulamentares aplicáveis à espécie, mediante cláusulas e condições seguintes:

CLÁUSULA I - DO OBJETO

I.1 Contratação de empresa especializada para fornecimento de 350 licenças do software antivírus utilizado na Instituição para a versão *Cross Grade - EPS X CEB, McAfee Complete EndPoint Protection - Business (CEB),* contemplando serviços de instalação, Suporte Técnico e Manutenção, por um período de 12 (doze) meses, além de transferência de conhecimento (*Hands On*) para até 03 (três) analistas.

I.1.1. A execução do objeto contratual deverá atingir o fim a que se destina, com a eficácia e qualidade requeridas.

I.1.2. Integram também o presente contrato, os termos e condições do Edital do **Pregão Eletrônico SEADE 011/2015**, seus anexos e a proposta apresentada, aos quais se vincula.

I.1.3. A contratada deverá manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação.

CLÁUSULA II – DESCRIÇÃO DOS SERVIÇOS

II.1 CARACTERÍSTICAS SOLICITADAS

II.1.1- Console de Gerenciamento:

1. Administração centralizada por console único de gerenciamento;
2. As configurações do Antivírus, AntiSpyware, Firewall, Proteção Contra Intrusos, controle de Dispositivos e Controle de Aplicações deverão ser realizadas para maquinas físicas e virtuais através da mesma console;
3. Toda a solução deverá funcionar com agente único na estação de trabalho, servidores físicos e virtuais a fim de diminuir o impacto ao usuário final;
4. Console de gerenciamento via tecnologia Web (HTTP e HTTPS);
5. Implementar console de gerenciamento e monitoramento centralizado através de single-sign-on (SSO) das soluções abaixo:
   - 5.1. Solução segurança de estação de trabalho e servidores ("endpoint") físicos e virtuais;
   - 5.2. IPS para Servidores e Estações;
   - 5.3. Controle de conteúdo/Antivírus WEB;
   - 5.4. Prevenção de Antispam e AntiVirus para Gateway e Servidores de E-mail;
   - 5.5. Prevenção contra perda de dados;
   - 5.6. Solução de Criptografia de Pastas, Disco Rígido e Dispositivos Removíveis;
   - 5.7. Solução de Conformidade e Validação de Configuração;
6. Mecanismo de comunicação (via push) em tempo real entre servidor e clientes, para entrega de configurações e assinaturas;
7. Mecanismo de comunicação randômico (via pull) em tempo determinado pelo administrador entre o cliente e servidor, para consulta de novas configurações e assinaturas evitando sobrecarga de rede e servidor;
8. Permitir a divisão lógica dos computadores, dentro da estrutura de gerenciamento, em sites, domínios e grupos, com administração individualizada por domínio;
9. O servidor de gerenciamento deverá possuir compatibilidade para instalação nos sistemas operacionais Microsoft Windows Server 2008, 2008 R2 e Windows Server 2012;
10. O servidor de gerenciamento deverá possuir compatibilidade para instalação em sistemas operacionais de 64-bits suportando ambiente virtual VMWARE 5.5 e Microsoft;
11. Possuir integração com LDAP, para importação da estrutura organizacional e autenticação dos Administradores;
12. Possibilidade de aplicar regras diferenciadas baseando na localidade lógica da rede;

13. Permitir que a localidade lógica da rede seja definida pelo conjunto dos seguintes itens:

    13.1. IP e range de IP;

    13.2. Endereço de Servidores de DNS, DHCP e WINS;

    13.3. Conexão com o servidor de gerência;

    13.4. Conexões de rede como VPN, Ethernet, Wireless e Modem;

14. Possibilidade de aplicar regras diferenciadas por grupos de usuários e maquinas;
15. O servidor de gerenciamento deverá permitir o uso de banco de dados relacional Microsoft SQL Server nas versões 2005, 2008 ou 2012; As licenças de banco de dados necessárias para o bom e correto funcionamento do servidor de gerenciamento, deverão ser fornecidas juntamente com a solução.
16. Possuir a funcionalidade e recursos para a criação e agendamento periódicos de backups da base de dados ou fornecer uma ferramenta para tal finalidade;
17. Permitir a opção instalação de Servidores de Gerenciamento adicionais fornecendo assim a possibilidade de trabalhar em modo de Load Balance e Failover;
18. Possuir na solução replicação nativa do Banco de Dados entre os Servidores de Gerenciamento com opção de customização do conteúdo à ser replicado (Assinaturas, Pacotes de Instalação, Políticas e Logs);
19. Possibilidade de instalação dos clientes em servidores, estações de trabalho e maquinas virtualizadas de forma remota via console de gerenciamento com opção de remoção de soluções previamente instaladas;
20. Permitir a instalação remota do software por Group Policy (GPO), Web e via console de gerenciamento;
21. Descobrir automaticamente as estações da rede que não possuem o cliente instalado;
22. Fornecer ferramenta de pesquisa de estações e servidores da rede que não possuem o cliente instalado com opção de instalação remota;
23. Fornecer atualizações do produto e das definições de vírus e proteção contra intrusos;
24. A console de gerenciamento deve permitir travar as configurações por senha nos clientes servidores e estações físicas e virtuais, definindo permissões para que somente o administrador possa alterar as configurações, desinstalar ou parar o serviço do cliente;
25. A console de gerenciamento deve permitir ao administrador travar separadamente os itens e cada subitem de acesso as configurações do cliente;
26. Capacidade de criação de contas de usuário com diferentes níveis de acesso de administração e operação;
27. Instalação e atualização do software sem a intervenção do usuário;
28. Possibilidade de configurar o bloqueio da desinstalação, desabilitar o serviço do cliente, importar e exportar configurações e abrir a console do cliente, por senha;
29. Suportar redirecionamentos dos logs para um servidor de Syslog;

30. Utilizar os protocolos HTTP e HTTPS para comunicação entre console de gerenciamento e o cliente gerenciado;
31. Possuir certificação *FIPS 140-2*;
32. Possuir certificação *Common Criteria* (CC) EAL2+;
33. O fabricante deverá possuir certificação *ICSA Labs* no mínimo nas plataformas Windows XP, Windows e Windows 7;

II.1.2. Atualização de Vacinas

1. Atualização incremental, remota e em tempo real, da vacina dos Antivírus, mecanismo de verificação (*engine*) e dos clientes da rede;
2. Permitir criar planos de distribuição das atualizações via comunicação segura entre cliente e Servidores de Gerenciamento, site do fabricante, via servidor de atualização interno e podendo eleger qualquer cliente gerenciado para distribuição das atualizações;
3. Permitir eleger qualquer cliente gerenciado como um servidor de distribuição das atualizações com opção de controle de banda, quantidades de definições e espaço em disco utilizado, podendo eleger mais de um cliente para esta função;
4. Atualização remota e incremental da versão do software cliente instalado;
5. Nas atualizações das configurações e das definições de vírus não poderá utilizar login scripts, agendamentos ou tarefas manuais ou outros módulos adicionais que NÃO sejam parte integrante da solução e sem requerer reinicialização do computador ou serviço para aplicá-la;

II.1.3. Quarentena

1. Possuir funcionalidades que permitam o isolamento (área de quarentena) de arquivos contaminados por códigos maliciosos que não sejam conhecidos ou que não possam ser reparados em um servidor central da rede;
2. Forma automática de envio dos arquivos da área de isolamento central para o fabricante, via protocolo seguro, onde este será responsável por gerar a vacina, automaticamente, sem qualquer tipo de intervenção do administrador. Recebimento utilizando o mesmo método e aplicação da vacina recém criada nas estações infectadas;
3. Possibilidade de adicionar manualmente arquivos na quarentena do cliente com opção de restrições na console de gerenciamento;

II.1.4. Cliente Gerenciado

1. Suportar máquinas com arquitetura 32-bits e 64-bits;
2. O cliente para instalação em estações de trabalho e servidores deverá possuir compatibilidade com os sistemas operacionais Microsoft Windows XP, 2003, 2008, 2008 R2, 7 e 8, Linux Red Hat Enterprise 5.x e 6.x, CentOS 6.4, 6.5 e versão 7;

II.1.5. Funcionalidade de Firewall e Detecção e Proteção de Intrusão (IDS\IPS) com as seguintes funcionalidades:

1. Suporte aos protocolos TCP, UDP e ICMP;

2. Reconhecimento dos tráficos DNS, DHCP e WINS com opção de bloqueio;
3. Possuir proteção contra exploração de buffer overflow;
4. Possuir proteção contra ataques de Denial of Service (DoS), Port-Scan e MAC Spoofing;
5. Possibilidades de criação de assinaturas personalizadas para detecção de novos ataques;
6. Possibilidade de agendar a ativação da regra de Firewall;
7. Possibilidade de criar regras diferenciadas por aplicações;
8. Gerenciamento integrado à console de gerência da solução;
9. Possibilidade de reconhecer automaticamente as aplicações utilizadas via rede baseado no *fingerprint* do arquivo;
10. Proteger o computador através da criação de uma impressão digital para cada executável existente no sistema, para que somente as aplicações que possuam essa impressão digital executem no computador (*Whitelist*);
11. Proteger o computador através da criação de uma impressão digital para cada executável existente no sistema, com o intuito de bloquear as ações de tais executáveis (*Blacklist*);
12. Permitir criação de zona confiável, permitindo que determinados IPs, protocolos ou aplicações se comuniquem na rede;
13. Bloqueio de ataques baseado na exploração da vulnerabilidade;
14. Capacidade de executar varreduras em tempo real (real-time) contra ataques dirigidos às vulnerabilidades do navegador (*browser*);

II.1.6. Funcionalidade de *Antivírus* e *AntiSpyware*:

1. Proteção em tempo real contra vírus, *trojans, worms, spyware, adwares* e outros tipos de códigos maliciosos;
2. Proteção *antispyware* deverá ser nativa do próprio antivírus, ou seja, não dependente de plugin ou módulo adicional;
3. As configurações do antispyware deverão ser realizadas através da mesma console de todos os itens da solução;
4. Permitir a configuração de ações diferenciadas para cada subcategoria de riscos de segurança (*Adware*, Discadores, Ferramentas de hacker, Programas de brincadeiras, Acesso Remoto, *Spyware*, *Trackware* e outros);
5. Permitir a configuração de duas ações, primária e secundária, executadas automaticamente para cada ameaça, com as opções de: somente alertar, limpar automaticamente, apagar automaticamente e colocar em quarentena;
6. Permitir a criação de listas de exclusões com informação da severidade, impacto e grau de remoção da ameaça nos níveis baixos, médio ou alto, onde os riscos excluídos não serão verificados pelo produto;
7. Permitir verificação das ameaças da maneira manual, agendada e em tempo real, detectando ameaças no nível do *kernel* do Sistema Operacional, fornecendo a possibilidade de detecção de *rootkits*;

8. Capacidade de realizar monitoramento em tempo real (real-time) por heurística correlacionando com a reputação de arquivos;
9. Capacidade de verificar a reputação de arquivos, correlacionando no mínimo as seguintes características:
   9.1. Origem confiável;
   9.2. Origem não confiável;
   9.3. Tempo de existência do arquivo na internet;
   9.4. Comportamento do arquivo;
   9.5. Quantidade mínima de usuários que baixaram o arquivo da internet;
10. Implementar intervalos de tempo para início de verificações agendadas de forma a reduzir impacto em ambientes virtuais;
11. Possuir funcionalidades que permitam o isolamento (área de quarentena) de arquivos contaminados por códigos maliciosos que não sejam conhecidos ou que não possa ser reparado no cliente;
12. Possuir funcionalidades que permitam a inclusão manual em isolamento (área de quarentena) de arquivos a serem enviados e vistoriados pelo centro de pesquisa do fabricante;
13. Permitir configurar ações a serem tomadas na ocorrência de ameaças, incluindo Reparar, Deletar, Mover para a Área de Isolamento e Ignorar;
14. Verificação de vírus nas mensagens de correio eletrônico, pelo antivírus da estação de trabalho, suportando clientes Outlook, Notes e POP3/SMTP;
15. Possuir funcionalidades que permitam a detecção e reparo de arquivos contaminados por códigos maliciosos mesmo que sejam compactados, tendo como abrangência até o 10º (décimo) nível de compactação;
16. Capacidade de detecção em tempo real de vírus novos, desconhecidos pela vacina com opção de ajuste da sensibilidade de detecção;
17. Capacidade de remoção automática total dos danos causados por *spywares, adwares e worms*, como limpeza do registro e pontos de carregamento, com opção de terminar o processo e terminar o serviço da ameaça no momento de detecção;
18. A remoção automática dos danos causados deverá ser nativa do próprio antivírus, ou seja, não dependente de *plugin*, execução de arquivo ou módulo adicional;
19. Capacidade de identificação da origem da infecção, para vírus que utilizam compartilhamento de arquivos como forma de propagação informando nome ou IP da origem com opção de bloqueio da comunicação via rede;
20. Possibilidade de bloquear verificação de vírus em recursos mapeados da rede, por senha;
21. Criar uma cópia backup do arquivo suspeito antes de limpá-lo;
22. Gerenciamento integrado à console de gerência da solução;
23. Possibilitar a criação de um disco (CD ou DVD) inicializável para verificação e remoção de ameaças sem a necessidade de carregar o Sistema Operacional do cliente;

II.1.7. Funcionalidade de detecção proativa de reconhecimento de novas ameaças com as funcionalidades:

1. Funcionalidade de detecção de ameaças desconhecidas que estão em memória por comportamento dos processos e arquivos das aplicações;
2. Não utilizar a assinatura de vírus para esta funcionalidade e fornecer atualizações periódicas da técnica de detecção;
3. Capacidade de detecção Keyloggers, Trojans, Spyware e Worms por comportamento dos processos em memória, com opção da sensibilidade distintas da detecção;
4. Reconhecimento de comportamento malicioso de modificação da configuração de DNS e arquivo de Hosts;
5. Possuir a funcionalidade de exclusão de detecção diferenciada do recurso de Antivírus;
6. Possibilidade de habilitar o recurso de correlacionamento da funcionalidade de detecção proativa com a base de reputação do fabricante;

II.1.8. Funcionalidade de Controle de Dispositivos e Aplicações

1. Gerenciar o uso de dispositivos USB e CD/DVD, através de controles de leitura/escrita/execução do conteúdo desses dispositivos e também sobre o tipo de dispositivo permitido (ex: permitir mouse USB e bloquear disco USB);

II.1.9. Proteções para ambientes virtualizados

1. Capacidade de identificar automaticamente maquinas virtuais e físicas, possibilitando a criação de regras especificas por tipo de ambiente (virtual ou físico);
2. Suportar as mesmas funcionalidades existentes para o ambiente físico no ambiente virtual, contemplando os virtualizadores VMware e Microsoft sem a necessidade de instalar outro agente, software, modulo e/ou plugins;
3. Cache compartilhado de reputação e resultado de varredura de arquivos, possibilitando exclusão automática de varredura de arquivos categorizados como não maliciosos e já escaneados anteriormente;
4. Capacidade de identificar "templates" de máquinas virtuais, marcando seus arquivos já verificados eliminando a necessidade de verificar esses arquivos todas as vezes que o template for clonado;
5. Capacidade de implementar varreduras otimizadas em máquinas físicas e virtuais, onde o arquivo verificado pela varredura uma vez, não será verificado novamente, até que ocorra alguma alteração no mesmo;

II.1.10. Relatórios e Monitoramentos

1. Possuir pelo menos 10 tipos de relatórios diferentes, permitindo a exportação para o formato HTML;
2. Recursos do relatório e monitoramento deverão ser nativos da própria console central de gerenciamento;
3. Possibilidade de exibir a lista de servidores e estações que possuam o antivírus instalado, contendo informações como nome da máquina, usuário logado, versão do antivírus, versão do engine, data da vacina, data da última verificação e status;

4. Capacidade de Geração de relatórios, estatísticos e gráficos contendo no mínimo os seguintes tipos pré-definidos:
   - 4.1. As 10 máquinas com maior ocorrência de códigos maliciosos;
   - 4.2. Os 10 usuários com maior ocorrência de códigos maliciosos;
   - 4.3. Localização dos códigos maliciosos;
   - 4.4. Sumários das ações realizadas;
   - 4.5. Número de infecções detectadas diário, semanal e mensal;
   - 4.6. Códigos maliciosos detectados.

II.1.11. Modulo de Integração com Console avançada de distribuição e relatórios já existente com a seguintes características:

1. Console de gerenciamento via tecnologia Web (HTTP ou HTTPS) independente da console central da solução;
2. Detectar e desinstalar soluções de antivírus dos seguintes fabricantes:
   - 2.1. CA
   - 2.2. ESET
   - 2.3. F-Secure
   - 2.4. Kaspersky
   - 2.5. Sophos
   - 2.6. Symantec
   - 2.7. Trend Micro
3. Permitir a remoção de outros softwares não desejados;
4. Criar tarefas de migração baseadas no resultado do inventário de antivírus;
5. Disparar comandos de verificações de ameaças nos clientes a partir da console do inventário;
6. Permitir a instalação do agente de antivírus com agendamento e implementar controle de banda para minimizar impacto na rede;
7. Possibilidade de recuperar instalação em clientes em caso de falha;
8. Exibir no console do inventário informações do ambiente de antivírus como falhas de varredura e autoproteção;
9. Oferecer relatórios avançados através da criação de cubos OLAP e tabelas Pivot;
10. Os seguintes cubos devem ser disponibilizados para criação de relatórios:
    - 10.1. Alertas;
    - 10.2. Clientes;
    - 10.3. Políticas;
    - 10.4. Rastreamento;
11. Possibilidade de criação de indicadores de performance para medir eficácia da solução de segurança

12. Exportar os relatórios criados nos formados xls, pdf e html;

II.2. MANUTENÇÃO E SUPORTE TÉCNICO

II.2.1. A contratada oferecerá garantia do suporte técnico e atualização do objeto contratado, que forem lançados no mercado durante 12 (doze) meses, a partir da assinatura do contrato, na forma prevista no Termo de Referência que integra o edital.

II.2.2. O serviço de suporte técnico deverá fornecer suporte corporativo telefônico, em português, sem custo adicional, ilimitado, com regime 8X5 durante o período de contrato, das 09:00 as 18:00;

II.2.3. O início do atendimento não poderá ultrapassar o prazo de 4 (quatro) horas, contado a partir da abertura do chamado;

II.2.4. O tempo de solução será de até 24 (vinte e quatro) horas. Para problemas desconhecidos, que depender de resposta do fabricante, este tempo poderá ser maior, com autorização prévia da SUTIN, e após o comprovante de registro de suporte no fabricante, pela contratada. Neste segundo caso o registro deverá ser aberto na primeira hora após o vencimento do tempo de solução.

II.2.5. A CONTRATANTE poderá abrir chamados e consultar o andamento dos mesmos pelo site e/ou Serviço de Atendimento ao Cliente (SAC) do fabricante; II.2.6. O serviço de suporte técnico deverá fornecer acesso gratuito às atualizações de conteúdo do produto, incluindo as vacinas contra vírus de computador e o filtro antispam da Suite;

II.2.7. O serviço de suporte técnico deverá fornecer acesso gratuito a correções do software (patches) e melhorias do produto (updates);

II.2.8. O serviço de suporte técnico deverá fornecer atualização gratuita do software em caso de mudança de versão (upgrade), durante o período de vigência do contrato;

II.2.9. A Superintendência de TI poderá disponibilizar, caso ache necessário, canal de atendimento por acesso remoto, através de conexão via Internet (Web), mediante autorização prévia da Superintendência de TI da Fundação Seade;

II.2.10. Será disponibilizado um banco de horas para atendimento local com a limitação pré-estabelecida de 4 (quatro) horas mês não cumulativas, para casos em que não sejam resolvidos o problema por telefone, e-mail ou através do suporte remoto, será enviado um técnico ao local da instalação em até 48 horas contados a partir do término de atendimento.

II.2.11. O suporte técnico será prestado nos dias úteis, em horário comercial, das 09:00 as 18:00 com atendimento por técnicos especializados para dirimir dúvidas de configuração e utilização do software, sem limitação para o número de chamadas;

II.3. SERVIÇOS DE INSTALAÇÃO, CONFIGURAÇÃO, DOCUMENTAÇÃO E TREINAMENTO HANDS ON

II.3.1 Instalação, Configuração e Documentação

Os serviços de instalação e configuração dos produtos, deverão ser acordados previamente e acompanhamento de analista da Fundação. Antes da execução dos serviços, deverá ser elaborado um plano de trabalho, com cronograma e previsão para início e conclusão das tarefas; Esse plano deverá ser previamente aprovado pela equipe técnica da Superintendência de TI, antes de ser implementado; Toda instalação deverá ser feita on site.

McAfee Complete EndPoint Protection - Business (CEB)

- Instalação das ferramentas especificadas, CEB, em no mínimo 12 (doze) equipamentos (Endpoints), um por andar, onde todas as soluções serão administradas a partir de um único servidor de administração – chamado EPO.
- Instalação, e configuração do EPO no servidor disponibilizado pela área de Informática;
- Serão 12 (doze) computadores que receberão a instalação da ferramenta de antivírus atualizada, uma máquina em cada andar, 02 (dois) servidores, um Microsoft e outro Linux CentOS, e a configuração do servidor gerenciador dos clientes das estações de trabalho e servidores (EPO), e com a transferência de conhecimento para os três analistas de rede da Instituição farão as demais atualizações;
- Depois de concluída a instalação será necessário fazer o deploy do novo agente para os 12 (doze) computadores.
- Instalação e configuração do McAfee Virusscan-for-linux em pelo menos um servidor com versão CentOS do Sistema Operacional Linux;
- Ao final da instalação / configuração, a licitante deverá entregar a documentação completa e detalhada dos serviços executados;

II.3.2. Treinamento

Deverá ser fornecido treinamento dos produtos ofertados, na modalidade **hands on**, para todas as ferramentas implementadas para até 03 pessoas, a serem designadas pela Superintendência de TI, onde deve contemplar:

Estratégias de implantação de regras de segurança e gerenciamento e monitoramento no Servidor EPO, tratando basicamente dos módulos de manutenção e de epidemia de vírus.

- Desenvolver estratégia para a distribuição do Agente do ePO nos desktops e servidores da empresa;
- Desenvolvimento de política de segurança para desktop;
- Desenvolvimento de estratégia de atualizações de agentes, a fim de minimizar o impacto na rede e no desempenho dos desktops;
- Interpretação e programação dos relatórios do ePO;
- Procedimentos de contenção de epidemias (outbreaks)

CLÁUSULA III – PRAZOS E LOCAL DE ENTREGA

III.1. A entrega do produto deverá ocorrer no prazo máximo de 15 (quinze) dias, a contar da assinatura do contrato.

III.2. O prazo para implantação dos serviços não deverá ultrapassar 30 (trinta) dias a contar da entrega do produto;

III.3. Todas as licenças devem ser entregues na Fundação Seade, localizada na AV. Cásper Líbero, 464, Centro - São Paulo/SP - CEP 01033- 000, aos cuidados da SUTIN - Superintendência de Tecnologia da Informação, ou diferente do indicado e dentro do perímetro urbano, conforme aviso da SUTIN.

III.3.1. As licenças serão tecnicamente aceitas pela SUTIN que emitirá Termo de Recebimento Definitivo ou Recibo.

CLÁUSULA IV – OBRIGAÇÕES DA CONTRATANTE

IV.1. A **Fundação SEADE** compromete-se em ceder os profissionais e os recursos necessários para a implantação das soluções adquirida e dar o apoio necessário ao gerenciamento e a aprovação formal dos resultados.

CLÁUSULA V – PREÇOS

V.1 Para todos os efeitos legais e jurídicos, as partes contratantes dão ao presente contrato o valor total de R$_____ (_____), sendo certo que no valor estão incluídos todos os custos diretos e indiretos, inclusive transporte e materiais, bem como os encargos, benefícios e despesas indiretas (BDI) e demais despesas de qualquer natureza.

CLÁUSULA VI – DOS RECURSOS ORÇAMENTÁRIOS

VI.1. A despesa com a execução do presente contrato onerará os recursos consignados no Programa de Trabalho:_____, Natureza de Despesa: _____, Fonte: _____.

CLÁUSULA VII- DO PRAZO DE VIGÊNCIA

VII.1 O presente contrato terá vigência de 12 (doze) meses.

VII.2 O prazo referido sob VII.1 acima poderá ser prorrogado por período igual período, até o limite de 48 (quarenta e oito) meses, nos termos e condições permitidos pela legislação vigente.

VII.3 A CONTRATADA poderá se opor à prorrogação de que trata o item VII.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.

VII.4 Não obstante o prazo estipulado no item VII.1 acima, a vigência contratual nos exercícios subsequentes à assinatura deste contrato estará sujeita à condição resolutiva, consubstanciada na existência de recursos aprovados nas respectivas leis orçamentárias de cada exercício, para atender as respectivas despesas.

VII.5 Ocorrendo a resolução do contrato, com base na condição estipulada no item VII.4 desta cláusula, a CONTRATADA não terá direito a qualquer espécie de indenização.

VII.6 A prorrogação do prazo de vigência contratual será formalizada mediante celebração de termo de aditamento ao contrato, respeitadas as condições previstas em lei.

CLÁUSULA VIII – DAS CONDIÇÕES DE PAGAMENTO

VIII.1 O pagamento do valor será efetuado 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.

VIII.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.

VIII.3 Constitui condição para a realização do pagamento 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 do pagamento.

VIII.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.

VIII.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.

VIII.6 O valor da prestação devida pela FUNDAÇÃO SEADE será reajustado anualmente, mediante a aplicação da seguinte fórmula paramétrica:

$$R = Po.[(\frac{IPC}{IPCo}) - 1]$$

Onde:

R = parcela de reajuste

Po = preço inicial do contrato no mês de referência dos preços, ou preço do contrato no mês de aplicação do último reajuste.

IPC/IPCo = variação do IPC FIPE – Índice de Preço ao Consumidor, ocorrida entre o mês de referência de preços, ou no mês do último reajuste aplicado e o mês de aplicação do reajuste.

VIII.7 A periodicidade anual, de que trata o subitem 6 deste item VIII, será contada a partir da data de apresentação da proposta.

CLÁUSULA IX - DA GARANTIA CONTRATUAL

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

CLÁUSULA X – DA RESCISÃO E RECONHECIMENTO DOS DIREITOS DA FUNDAÇÃO SEADE

X.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.

Parágrafo único - 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.

CLAÚSULA XI - DAS SANÇÕES PARA O CASO DE INADIMPLEMENTO

XI.1. A Contratada 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.

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

CLÁUSULA XII – DA 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 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 – DO 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 para que produza todos os efeitos de direito, na presença das testemunhas abaixo identificadas.

São Paulo,

FUNDAÇÃO SISTEMA ESTADUAL DE ANÁLISE DE DADOS - SEADE

_____
MARIA HELENA GUIMARÃES DE CASTRO
Diretora Executiva

EMPRESA CONTRATADA

_____
REPRESENTANTE LEGAL
Cargo

Testemunhas:

1._____
NOME:
RG:

2._____
NOME:
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 011/2015

Eu (**nome completo)**, representante legal da empresa **(razão social da proponente)**, participante do processo licitatório, na modalidade de **PREGÃO ELETRÔNICO Nº 011/2015** 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 011/2015

Eu (**nome completo)**, representante legal da empresa **(razão social da proponente)**, participante do processo licitatório, na modalidade de **PREGÃO ELETRÔNICO Nº 011/2015** 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 Nº011/2015

Eu (**nome completo)**, representante legal da empresa **(razão social da proponente)**, participante do processo licitatório, na modalidade de **PREGÃO ELETRÔNICO Nº 011/2015** 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 011/2015

Eu (**nome completo)**, representante legal da empresa **(razão social da proponente)**, participante do processo licitatório, na modalidade de **PREGÃO ELETRÔNICO Nº 011/2015** 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 Valor 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.