

AVISO DE ABERTURA DE LICITAÇÃO

Acha-se aberta no **CENTRO ESTADUAL DE EDUCAÇÃO TECNOLÓGICA PAULA SOUZA**, a licitação na modalidade de **PREGÃO ELETRÔNICO Nº 025/2018**, tipo **MENOR PREÇO**, OC.102401100632018OC00065, referente ao Processo nº **6756/17**, a ser realizada por intermédio do sistema eletrônico de contratações, denominado **“Bolsa Eletrônica de Compras do Governo do Estado de São Paulo – BEC/SP”**, cujo objeto é a **AQUISIÇÃO E ATUALIZAÇÃO DE USO DE SOFTWARE; APLICATIVOS: SUITE DE PROTEÇÃO DE ENDPOINTS, HORAS DE CONSULTORIA, TREINAMENTO E SUPORTE**, a realização do pregão será no dia 11 de abril de 2018, a partir das 09:00 horas, no endereço eletrônico www.bec.sp.gov.br. O edital na íntegra, estará disponível para consulta e/ou retirada no site www.bec.sp.gov.br e www.cps.sp.gov.br.

São Paulo, 27 de março de 2018.

FÁBIO ROBERTO IGRISSIS
Subscritor do Edital

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almoxarifado

EDITAL DE PREGÃO ELETRÔNICO n.º 025/2018

PROCESSO nº 6756/17

OFERTA DE COMPRA N° 102401100632018OC00065

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

DATA DO INÍCIO DO PRAZO PARA ENVIO DA PROPOSTA ELETRÔNICA: 28/03/2018

DATA E HORA DA ABERTURA DA SESSÃO PÚBLICA: 11/04/2018 – as 09h00min

O **CENTRO ESTADUAL DE EDUCAÇÃO TECNOLÓGICA PAULA SOUZA**, por intermédio da Diretora Superintendente, a Prof^a Laura M. J. Laganá, RG. 7.715.675-4, e do CPF. 005.923.818-62, usando a competência delegada pelos artigos 3º e 7º, inciso I, do Decreto estadual nº 47.297, de 06 de novembro de 2002, c.c. artigo 8º, do Decreto estadual nº 49.722, de 24 de junho de 2005, torna público que se acha aberta, nesta unidade, situada na **Rua dos Andradas, 140 - Santa Ifigênia - São Paulo/SP**, 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 n.º 025/2018**, do tipo **MENOR PREÇO**, objetivando a **AQUISIÇÃO E ATUALIZAÇÃO DE USO DE SOFTWARE; APLICATIVOS: SUITE DE PROTEÇÃO DE ENDPOINTS, HORAS DE CONSULTORIA, TREINAMENTO E SUPORTE**, que será regida pela Lei federal n.º 10.520, de 17 de julho de 2002, pelo Decreto n.º 49.722, de 24 de junho de 2005, pelo regulamento anexo à Resolução n.º CC-27, de 25/05/2006, aplicando-se, subsidiariamente, no que couberem, as disposições da Lei federal n.º 8.666, de 21 de junho de 1993, do Decreto estadual n.º 47.297, de 06 de novembro de 2002, do regulamento anexo à Resolução CEGP10, de 19 de novembro de 2002, 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, 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.

1.	DO OBJETO
-----------	------------------

- 1.1. A presente licitação tem por objeto a **AQUISIÇÃO E ATUALIZAÇÃO DE USO DE SOFTWARE; APLICATIVOS: SUITE DE PROTEÇÃO DE ENDPOINTS, HORAS DE CONSULTORIA, TREINAMENTO E SUPORTE**, conforme especificações constantes do Termo de Referência que integra este edital como **ANEXO I**.

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almoxarifado

2. DA PARTICIPAÇÃO

2.1. Poderão participar do certame todos os interessados em contratar com a Administração Estadual que estejam registrados no CAUFESP, que atuem 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.

2.1.1. 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.

2.1.2. O registro no CAUFESP é gratuito. As informações a respeito das condições exigidas e dos procedimentos a serem cumpridos para a inscrição no Cadastro, para o credenciamento de representantes e para a obtenção de senha de acesso estão disponíveis no endereço eletrônico www.bec.sp.gov.br.

2.2. Não será admitida a participação, neste certame licitatório, de pessoas físicas ou jurídicas:

2.2.1. Que estejam com o direito de licitar e contratar temporariamente suspenso, ou que tenham sido impedidas de licitar e contratar com a Administração Pública estadual, direta e indireta, com base no artigo 87, inciso III, da Lei Federal nº 8.666/1993 e no artigo 7º da Lei Federal nº 10.520/2002;

2.2.2. Que tenham sido declaradas inidôneas pela Administração Pública federal, estadual ou municipal, nos termos do artigo 87, inciso IV, da Lei Federal nº 8.666/1993;

2.2.3. Que possuam vínculos de natureza técnica, comercial, econômica, financeira ou trabalhista com a autoridade competente, o Pregoeiro, o subscritor do edital ou algum dos membros da respectiva equipe de apoio, nos termos do artigo 9º da Lei Federal nº 8.666/1993;

2.2.4. Que não tenham representação legal no Brasil com poderes expressos para receber citação e responder administrativamente ou judicialmente;

2.2.5. Que estejam reunidas em consórcio ou sejam controladoras, coligadas ou subsidiárias entre si;

2.2.6. Que tenham sido proibidas pelo Plenário do CADE de participar de licitações promovidas pela Administração Pública federal, estadual, municipal, direta e indireta, em virtude de prática de infração à ordem econômica, nos termos do artigo 38, inciso II, da Lei Federal nº 12.529/2011;

2.2.7. Que estejam proibidas de contratar com a Administração Pública em virtude de sanção restritiva de direito decorrente de infração administrativa ambiental, nos termos do art. 72, § 8º, inciso V, da Lei Federal nº 9.605/1998;

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almoxarifado

2.2.8. Que tenham sido proibidas de contratar com o Poder Público em razão de condenação por ato de improbidade administrativa, nos termos do artigo 12 da Lei Federal nº 8.429/1992;

2.2.9. Que tenham sido declaradas inidôneas para contratar com a Administração Pública pelo Plenário do Tribunal de Contas do Estado de São Paulo, nos termos do artigo 108, da Lei Complementar Estadual nº 709/1993;

2.2.10. Que tenham sido suspensas temporariamente, impedidas ou declaradas inidôneas para licitar ou contratar com a Administração Pública estadual, direta e indireta, por desobediência à Lei de Acesso à Informação, nos termos do artigo 33, incisos IV e V, da Lei Federal nº 12.527/2011 e do artigo 74, incisos IV e V, do Decreto Estadual nº 58.052/2012;

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

2.4. 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. Em caso de perda ou quebra do sigilo da senha de acesso, caberá ao interessado efetuar o seu cancelamento por meio do sítio eletrônico www.bec.sp.gov.br (opção "CAUFESP"), conforme Resolução CC-27, de 25 de maio de 2006.

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

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

2.7. Para o exercício do direito de preferência de que trata o item 5.6, bem como para a fruição do benefício de habilitação com irregularidade fiscal previsto na alínea "f" do item 5.9, a condição de microempresa, de empresa de pequeno porte ou de cooperativa que preencha as condições estabelecidas no art. 34, da Lei Federal nº 11.488/2007, deverá constar do registro da licitante junto ao CAUFESP, sem prejuízo do disposto nos itens 4.1.4.3 a 4.1.4.5 deste Edital.

3.	DAS PROPOSTAS
-----------	----------------------

3.1. As propostas deverão ser enviadas por meio eletrônico disponível no endereço www.bec.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 a abertura da sessão pública, devendo a licitante, para formulá-las, assinalar a declaração de que cumpre integralmente os requisitos de habilitação constantes do Edital.

3.2. Os preços unitários e total serão ofertados no formulário eletrônico próprio, em moeda corrente nacional, em algarismos, sem inclusão de qualquer encargo financeiro ou previsão inflacionária. Nos preços propostos deverão estar incluídos, além do lucro, todas as despesas

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almoxarifado

e custos diretos ou indiretos relacionados ao fornecimento do objeto da presente licitação, tais como tributos, remunerações, despesas financeiras e quaisquer outras necessárias ao cumprimento do objeto desta licitação, inclusive gastos com transporte.

3.2.1. As propostas não poderão impor condições e deverão limitar-se ao objeto desta licitação, sendo desconsideradas quaisquer alternativas de preço ou qualquer outra condição não prevista no Edital e seus anexos.

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

3.2.3. As microempresas e empresas de pequeno porte impedidas de optar pelo Simples Nacional, ante as vedações previstas na Lei Complementar Federal nº 123/2006, não poderão aplicar os benefícios decorrentes desse regime tributário diferenciado em sua proposta, devendo elaborá-la de acordo com as normas aplicáveis às demais pessoas jurídicas, sob pena de não aceitação dos preços ofertados pelo Pregoeiro.

3.2.3.1. Caso venha a ser contratada, a microempresa ou empresa de pequeno porte na situação descrita no item 3.2.3 deverá requerer ao órgão fazendário competente a sua exclusão do Simples Nacional até o último dia útil do mês subsequente àquele em que celebrado o contrato, nos termos do artigo 30, *caput*, inciso II, e §1º, inciso II, da Lei Complementar Federal nº 123/2006, apresentando à Administração a comprovação da exclusão ou o seu respectivo protocolo.

3.2.3.2. Se a contratada não realizar espontaneamente o requerimento de que trata o item 3.2.3.1, caberá ao ente público contratante comunicar o fato ao órgão fazendário competente, solicitando que a empresa seja excluída de ofício do Simples Nacional, nos termos do artigo 29, inciso I, da Lei Complementar Federal nº 123/2006.

3.3. O preço ofertado permanecerá fixo e irremovível.

3.4. Na ausência de indicação expressa em sentido contrário no **ANEXO II**, o prazo de validade da proposta será de 60 (sessenta) dias contados a partir da data de sua apresentação.

4. DA HABILITAÇÃO

4.1. O julgamento da habilitação se processará mediante o exame dos documentos a seguir relacionados, os quais dizem respeito a:

4.1.1. HABILITAÇÃO JURÍDICA

a) Registro empresarial na Junta Comercial, no caso de empresário individual ou Empresa Individual de Responsabilidade Limitada - EIRELI;

b) Ato constitutivo, estatuto ou contrato social atualizado e registrado na Junta Comercial, em se tratando de sociedade empresária ou cooperativa, devendo o estatuto, no caso das cooperativas, estar adequado à Lei Federal nº 12.690/2012;

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

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almoxarifado

- 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, tratando-se 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) Registro perante a entidade estadual da Organização das Cooperativas Brasileiras, em se tratando de sociedade cooperativa;

4.1.2. REGULARIDADE FISCAL E TRABALHISTA

- a) Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas, do Ministério da Fazenda (CNPJ);
- b) Prova de inscrição no Cadastro de Contribuintes Estadual, relativo à sede ou domicílio da licitante, pertinente ao seu ramo de atividade e compatível com o objeto do certame;
- c) Certificado de regularidade do Fundo de Garantia por Tempo de Serviço (CRF - FGTS);
- d) Certidão negativa, ou positiva com efeitos de negativa, de débitos trabalhistas (CNDT);
- e) Certidão negativa, ou positiva com efeitos de negativa, de Débitos relativos a Créditos Tributários Federais e à Dívida Ativa da União;
- f) Certidão de regularidade de débitos tributários com a Fazenda Estadual;

4.1.3. QUALIFICAÇÃO ECONÔMICO-FINANCEIRA

- a) Certidão negativa de falência, recuperação judicial ou extrajudicial, expedida pelo distribuidor da sede da pessoa jurídica ou do domicílio do empresário individual;
 - a.1). Se a licitante for cooperativa ou sociedade não empresária, a certidão mencionada na alínea “a” deverá ser substituída por certidão negativa de ações de insolvência civil.
 - a.2). Caso o licitante esteja em recuperação judicial ou extrajudicial, deverá ser comprovado o acolhimento do plano de recuperação judicial ou a homologação do plano de recuperação extrajudicial, conforme o caso.

4.1.4. DECLARAÇÕES E OUTRAS COMPROVAÇÕES

4.1.4.1. Declaração subscrita por representante legal da licitante, em conformidade com o modelo constante do **ANEXO III.1**, atestando que:

- a) se encontra em situação regular perante o Ministério do Trabalho no que se refere a observância do disposto no inciso XXXIII do artigo 7.º da Constituição Federal, na forma do Decreto Estadual nº. 42.911/1998;

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almoxarifado

b) inexistente impedimento legal para licitar ou contratar com a Administração;

4.1.4.2. Declaração subscrita por representante legal da licitante, em conformidade com o modelo constante do **ANEXO III.2**, afirmando que sua proposta foi elaborada de maneira independente e que conduz seus negócios de forma a coibir fraudes, corrupção e a prática de quaisquer outros atos lesivos à Administração Pública, nacional ou estrangeira, em atendimento à Lei Federal nº 12.846/2013 e ao Decreto Estadual nº 60.106/2014.

4.1.4.3. Em se tratando de microempresa ou de empresa de pequeno porte, declaração subscrita por representante legal da licitante, em conformidade com o modelo constante do **ANEXO III.3**, declarando seu enquadramento nos critérios previstos no artigo 3º da Lei Complementar Federal nº 123/2006, bem como sua não inclusão nas vedações previstas no mesmo diploma legal.

4.1.4.4. Em se tratando de cooperativa que preencha as condições estabelecidas no art. 34, da Lei Federal nº 11.488/2007, declaração subscrita por representante legal da licitante, em conformidade com o modelo constante do **ANEXO III.4**, declarando que seu estatuto foi adequado à Lei Federal nº 12.690/2012 e que auferir Receita Bruta até o limite definido no inciso II do *caput* do art. 3º da Lei Complementar Federal nº 123/2006.

4.1.4.5. Além das declarações exigidas nos itens 4.1.4.3 e 4.1.4.4, a comprovação da condição de microempresa, de empresa de pequeno porte ou de cooperativa que preencha as condições estabelecidas no art. 34, da Lei Federal nº 11.488/2007, deverá ser realizada da seguinte forma:

4.1.4.5.1. Se sociedade empresária, pela apresentação de certidão expedida pela Junta Comercial competente;

4.1.4.5.2. Se sociedade simples, pela apresentação da “Certidão de Breve Relato de Registro de Enquadramento de Microempresa ou Empresa de Pequeno Porte”, expedida pelo Cartório de Registro de Pessoas Jurídicas;

4.1.4.5.3. Se sociedade cooperativa, pela Demonstração do Resultado do Exercício ou documento equivalente que comprove Receita Bruta até o limite definido no inciso II do *caput* do art. 3º da Lei Complementar Federal nº 123/2006.

4.2. DISPOSIÇÕES GERAIS

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

4.2.2. O Pregoeiro, a seu critério, poderá diligenciar para esclarecer dúvidas ou confirmar o teor das declarações solicitadas no item 4.1.4 deste Edital e das comprovações de qualificação econômico-financeira e de qualificação técnica (caso exigidas nos itens 4.1.3 e 4.1.5), aplicando-se, em caso de falsidade, as sanções penais e administrativas pertinentes.

4.2.3. Caso o objeto contratual venha a ser cumprido por filial da licitante, os documentos exigidos no item 4.1.2 deverão ser apresentados tanto pela matriz quanto pelo estabelecimento

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almoxarifado

que executará o objeto do contrato.

5. DA SESSÃO PÚBLICA E DO JULGAMENTO

5.1. 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.

5.2. A análise das propostas pelo Pregoeiro se limitará ao atendimento das condições estabelecidas neste Edital e seus anexos e à legislação vigente.

5.2.1. Serão desclassificadas as propostas:

- a) cujo objeto não atenda as especificações, prazos e condições fixados neste Edital;
- b) que apresentem preço baseado exclusivamente em proposta das demais licitantes;
- c) apresentadas por licitante impedida de participar, nos termos do item 2.2 deste edital.

5.2.2. A desclassificação se dará por decisão motivada do Pregoeiro, observado o disposto no artigo 43, §3º, da Lei Federal nº 8.666/1993.

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

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

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

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

5.4.1. Os lances deverão ser formulados exclusivamente por meio do sistema eletrônico em valores distintos e decrescentes, inferiores à proposta de menor preço ou ao último valor apresentado pela própria licitante ofertante, observada em ambos os casos a redução mínima fixado no item 5.4.2, aplicável, inclusive, em relação ao primeiro formulado, prevalecendo o primeiro lance recebido, quando ocorrerem 02 (dois) ou mais lances do mesmo valor.

5.4.2. O valor de redução mínima entre os lances será de **R\$ 7.118,00 (sete mil, cento e dezoito reais)** e incidirá sobre o **valor total do lote**.

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

5.4.3.1. A duração da etapa de lances será prorrogada automaticamente pelo sistema, visando à continuidade da disputa, quando houver lance admissível ofertado nos últimos 03 (três) minutos do período de que trata o item 5.4.3 ou nos sucessivos períodos de prorrogação automática.

5.4.3.2. Não havendo novos lances ofertados nas condições estabelecidas no item 5.4.3.1, a duração da prorrogação encerrar-se-á, automaticamente, quando atingido

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almoxarifado

o terceiro minuto contado a partir do registro no sistema do último lance que ensejar prorrogação.

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

5.4.4.1. dos lances admitidos e dos inválidos, horários de seus registros no sistema e respectivos valores;

5.4.4.2. do tempo restante para o encerramento da etapa de lances.

5.4.5. A etapa de lances será considerada encerrada findos os períodos de duração indicados no item 5.4.3.

5.5. Encerrada a etapa de lances, o sistema divulgará a nova grade ordenatória contendo a classificação final, em ordem crescente de valores, considerando o último preço admitido de cada licitante.

5.6. Com base na classificação a que alude o item 5.5, será assegurada às licitantes microempresas, empresas de pequeno porte e cooperativas que preencham as condições estabelecidas no artigo 34, da Lei Federal nº 11.488/2007, preferência à contratação, observadas as seguintes regras:

5.6.1. A microempresa, empresa de pequeno porte ou cooperativa que preencha as condições estabelecidas no artigo 34, da Lei Federal nº 11.488/2007, 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. Caso haja propostas empatadas, a convocação recairá sobre a licitante vencedora de sorteio.

5.6.2. 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 11.488/2007, cujos valores das propostas se enquadrem nas condições indicadas no item 5.6.1.

5.6.3. Caso a detentora da melhor oferta, de acordo com a classificação de que trata o item 5.5, seja microempresa, empresa de pequeno porte ou cooperativa que preencha as condições estabelecidas no artigo 34, da Lei Federal nº 11.488/2007, não será assegurado o direito de preferência, passando-se, desde logo, à negociação do preço.

5.7. O Pregoeiro poderá negociar com o autor da oferta de menor valor mediante troca de mensagens abertas no sistema, com vistas à redução do preço.

5.8. Após a negociação, se houver, o Pregoeiro examinará a aceitabilidade do menor preço, decidindo motivadamente a respeito.

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almoxarifado

5.8.1. A aceitabilidade dos preços será aferida a partir dos preços de mercado vigentes na data da apresentação das propostas, apurados mediante pesquisa realizada pelo órgão licitante, que será juntada aos autos por ocasião do julgamento.

5.8.2. Não serão aceitas as propostas que tenham sido apresentadas por microempresas ou empresas de pequeno porte impedidas de optar pelo Simples Nacional e que, não obstante, tenham considerado os benefícios desse regime tributário diferenciado.

5.8.3. Na mesma sessão pública, o Pregoeiro solicitará da licitante detentora da melhor oferta o envio, no campo próprio do sistema, da planilha de proposta detalhada, elaborada de acordo com o modelo do **ANEXO II** deste Edital, contendo os preços unitários e o novo valor total para a contratação a partir do valor total final obtido no certame.

5.8.3.1. A planilha de proposta deverá conter indicação da procedência, marca e modelo do produto ofertado, observadas as especificações do Termo de Referência constante do **ANEXO I**.

5.8.3.2. O Pregoeiro poderá a qualquer momento solicitar às licitantes os esclarecimentos que julgar necessários.

5.8.3.3. A critério do Pregoeiro, a sessão pública poderá ser suspensa por até 02 (dois) dias úteis para a apresentação da planilha de proposta em conformidade com o modelo do **ANEXO II**.

5.8.3.4. Se a licitante detentora da melhor oferta deixar de cumprir a obrigação estabelecida no item 5.8.3, sua proposta não será aceita pelo Pregoeiro.

5.8.3.5 No formulário eletrônico de encaminhamento da proposta deverá(ão) ser anexado(s) arquivo contendo: **catálogo, contendo as especificações do produto.**

5.8.4. Antes da apreciação dos documentos de habilitação, o pregoeiro poderá suspender a sessão pública para análise do catálogo apresentado pelo licitante detentor da melhor oferta.

5.8.4.1. O catálogo será avaliado pela área técnica, verificando-se a conformidade de suas disposições com a descrição e as especificações técnicas constantes do Termo de Referência.

5.8.4.1.1. se o catálogo for aceito, o Pregoeiro retomará a sessão pública, informando os demais licitantes dessa decisão e prosseguirá para avaliação dos requisitos de habilitação.

5.8.4.1.2. se o catálogo for rejeitado, ou não for entregue, a proposta será desclassificada e o Pregoeiro retomará a sessão pública, convocando o licitante detentor da segunda melhor oferta a apresentar planilha de proposta detalhada, elaborada de acordo com o modelo do ANEXO II deste Edital, acompanhada de catálogo, na forma do subitem 5.8.4.

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almoxarifado

5.8.4.2. A decisão que aceitar ou rejeitar o catálogo será formalizada por despacho fundamentado.

5.9. Considerada aceitável a oferta de menor preço e aprovado o catálogo, 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 4 deste Edital;
- b) Caso os dados e informações constantes no CAUFESP não atendam aos requisitos estabelecidos no item 4 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. Essa verificação será certificada pelo Pregoeiro na ata da sessão pública, devendo ser anexados aos autos os documentos obtidos por meio eletrônico, salvo impossibilidade devidamente certificada e justificada;
- c) A licitante poderá suprir eventuais omissões ou sanear falhas relativas ao cumprimento dos requisitos e condições de habilitação estabelecidos neste Edital mediante a apresentação de documentos, preferencialmente por correio eletrônico a ser fornecido pelo Pregoeiro no chat do sistema, desde que os envie no curso da própria sessão pública e antes de ser proferida decisão sobre a habilitação. As declarações solicitadas no item 4.1.4 e as comprovações de qualificação técnica, caso exigida no item 4.1.5, serão obrigatoriamente apresentadas por correio eletrônico, sem prejuízo do disposto no item 5.9, “a”, “b” e “c” 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 5.9, 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 no endereço indicado no preâmbulo deste Edital, em até 02 (dois) dias após o encerramento da sessão pública, sob pena de invalidade do respectivo ato de habilitação e aplicação das penalidades cabíveis;
- f) A comprovação da regularidade fiscal de microempresas, empresas de pequeno porte ou cooperativas que preencham as condições estabelecidas no artigo 34 da Lei Federal nº 11.488/2007 será exigida apenas para efeito de celebração do contrato. Não obstante, a apresentação de todas as certidões e documentos exigidos para a comprovação da regularidade fiscal será obrigatória na fase de habilitação, ainda que apresentem alguma restrição ou impedimento.
- f.1) A prerrogativa tratada na alínea “f” abrange apenas a regularidade fiscal do licitante enquadrado como microempresa, empresa de pequeno porte ou cooperativa que preencha as condições estabelecidas no artigo 34 da Lei Federal nº 11.488/2007, não abrangendo a regularidade trabalhista (item 4.1.2, alínea “d”) nem os demais requisitos de habilitação exigidos neste Edital, os quais deverão ser comprovados durante o certame licitatório e na forma prescrita neste item 5.9.

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almoxarifado

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

h) Havendo necessidade de maior prazo para analisar os documentos exigidos, o Pregoeiro suspenderá a sessão, informando no chat eletrônico a nova data e horário para sua continuidade.

i) 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. O Pregoeiro deverá, ainda, informar o teor dos documentos recebidos por meio eletrônico.

5.10. A licitante habilitada nas condições da alínea “f” do item 5.9 deverá comprovar sua regularidade fiscal sob pena de decadência do direito à contratação, sem prejuízo da aplicação das sanções cabíveis, 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.

5.11. Ocorrendo a habilitação na forma indicada na alínea “f”, do item 5.9, a sessão pública será suspensa pelo Pregoeiro, observados os prazos previstos no item 5.10 para que a licitante vencedora possa comprovar a regularidade fiscal.

5.12. Por ocasião da retomada da sessão, o Pregoeiro decidirá motivadamente sobre a comprovação ou não da regularidade fiscal de que trata o item 5.10, ou sobre a prorrogação de prazo para a mesma comprovação.

5.13. 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 itens 5.10 a 5.12, o Pregoeiro, respeitada a ordem de classificação de que trata o item 5.5, 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.

6. DO RECURSO, DA ADJUDICAÇÃO E DA HOMOLOGAÇÃO

6.1. Divulgado o vencedor ou, se for o caso, saneada a irregularidade fiscal nos moldes dos itens 5.10 a 5.12, o Pregoeiro informará às licitantes por meio de mensagem lançada no sistema que poderão interpor recurso, imediata e motivadamente, por meio eletrônico, utilizando exclusivamente o campo próprio disponibilizado no sistema.

6.1.1. O prazo fixado para a manifestação da intenção de interposição de recurso por meio eletrônico será de 05 (cinco) minutos.

6.2. Havendo interposição de recurso o Pregoeiro informará aos recorrentes que poderão apresentar memoriais contendo as razões recursais no prazo de 03 (três) dias úteis após o encerramento da sessão pública, sob pena de preclusão. Os demais licitantes poderão apresentar contrarrazões ao(s) recurso(s) interposto(s) no prazo comum de 03 (três) dias úteis contados a partir do término do prazo para apresentação, pelo(s) recorrente(s), dos memoriais

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almoxarifado

recursais, sendo-lhes assegurada vista aos autos do processo no endereço indicado pela Unidade Compradora.

6.3. Os memoriais de recurso e as contrarrazões serão oferecidos por meio eletrônico no sítio www.bec.sp.gov.br, opção "RECURSO". A apresentação de documentos relativos às peças antes indicadas, se houver, será efetuada mediante protocolo dentro dos prazos estabelecidos no item 6.2.

6.4. A falta de interposição do recurso na forma prevista no item 6.1 importará na decadência do direito de recorrer, podendo o Pregoeiro adjudicar o objeto do certame ao vencedor na própria sessão pública e, em seguida, propor à autoridade competente a homologação do procedimento licitatório.

6.5. 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.

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

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

7.	DA DESCONEXÃO COM O SISTEMA ELETRÔNICO
-----------	---

7.1. 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.

7.2. 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.

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

8.	DOS PRAZOS, DAS CONDIÇÕES E DO LOCAL DE ENTREGA DO OBJETO DA LICITAÇÃO
-----------	---

8.1. O objeto desta licitação deverá ser executado em conformidade com as especificações constantes do Termo de Referência, que constitui **Anexo I** deste Edital, correndo por conta da contratada as despesas necessárias à sua execução, em especial as relativas a seguros, transporte, tributos, encargos trabalhistas e previdenciários decorrentes da execução do objeto do contrato.

8.2. A execução dos serviços deverá ter início na data indicada no termo de contrato.

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almoxarifado

9. DAS CONDIÇÕES DE RECEBIMENTO DO OBJETO

9.1. As condições de recebimento do objeto são aquelas definidas pelo termo de contrato, cuja minuta constitui o **ANEXO V** deste Edital.

10. DA FORMA DE PAGAMENTO

10.1. Os pagamentos serão efetuados em conformidade com o termo de contrato, cuja minuta constitui o **ANEXO V** deste Edital.

11. DA CONTRATAÇÃO

11.1. A contratação decorrente deste certame licitatório será formalizada mediante a assinatura de termo de contrato, cuja minuta integra este Edital como **ANEXO V**.

11.1.1. Se, por ocasião da celebração do contrato, algum dos documentos apresentados pela adjudicatária para fins de comprovação da regularidade fiscal ou trabalhista estiver com o prazo de validade expirado, a Unidade Compradora verificará a situação por meio eletrônico hábil de informações e certificará a regularidade nos autos do processo, anexando ao expediente os documentos comprobatórios, salvo impossibilidade devidamente justificada.

11.1.2. Se não for possível atualizar os documentos referidos no item 11.1.1 por meio eletrônico hábil de informações, a adjudicatária será notificada para, no prazo de 02 (dois) dias úteis, comprovar a sua situação de regularidade mediante a apresentação das certidões respectivas com prazos de validade em plena vigência, sob pena de a contratação não se realizar.

11.1.3. Constitui condição para a celebração da contratação, bem como para a realização dos pagamentos dela decorrentes, a inexistência de registros em nome da adjudicatária no “Cadastro Informativo dos Créditos não Quitados de Órgãos e Entidades Estaduais – CADIN ESTADUAL”. Esta condição será considerada cumprida se a devedora comprovar que os respectivos registros se encontram suspensos, nos termos do artigo 8º, §§ 1º e 2º. da Lei Estadual nº 12.799/2008.

11.1.4. O “Sistema Eletrônico de Aplicação e Registro de Sanções Administrativas – e-Sanções”, no endereço www.esancoes.sp.gov.br, e o “Cadastro Nacional de Empresas Inidôneas e Suspensas – CEIS”, no endereço <http://www.portaltransparencia.gov.br/ceis>, deverão ser consultados previamente à celebração da contratação, observado o disposto nos itens 2.2.1 e 2.2.2 deste Edital.

11.1.5. Constituem, igualmente, condições para a celebração do contrato:

a) a indicação de gestor encarregado de representar a adjudicatária com exclusividade perante o contratante, caso se trate de sociedade cooperativa;

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almoxarifado

b) a apresentação do(s) documento(s) que a adjudicatária, à época do certame licitatório, houver se comprometido a exibir antes da celebração do contrato por meio de declaração específica, caso exigida no item 4.1.4.6 deste Edital.

11.2. A adjudicatária deverá, no prazo de 5 (cinco) dias corridos contados da data da convocação, comparecer no local e horário indicados pela Unidade Compradora para assinatura do termo de contrato. O prazo para assinatura poderá ser prorrogado por igual período por solicitação justificada do interessado e aceita pela Administração.

11.3. As demais licitantes classificadas serão convocadas para participar de nova sessão pública do pregão, com vistas à celebração do contrato, quando a adjudicatária:

11.3.1. Deixar de comprovar sua regularidade fiscal, nos moldes do item 5.10, ou na hipótese de invalidação do ato de habilitação com base no disposto na alínea “e” do item 5.9;

11.3.2. For convocada dentro do prazo de validade de sua proposta e não apresentar a situação regular de que tratam os itens 11.1.1 a 11.1.5 deste Edital.

11.3.3. Recusar-se a assinar o contrato ou não comparecer no horário e local indicados para a sua assinatura;

11.3.4. For proibida de participar desta licitação, nos termos do item 2.2 deste Edital;

11.4 A nova sessão de que trata o item 11.3 será realizada em prazo não inferior a 03 (três) dias úteis contados da publicação do aviso no Diário Oficial do Estado de São Paulo.

11.4.1. O aviso será também divulgado nos endereços eletrônicos www.bec.sp.gov.br e www.imesp.com.br, opção “NEGÓCIOS PÚBLICOS”.

11.4.2. Na nova sessão, respeitada a ordem de classificação, observar-se-ão as disposições dos itens 5.7 a 5.10 e 6.1 a 6.7 deste Edital.

12. DAS SANÇÕES PARA O CASO DE INADIMPLEMENTO
--

12.1. Ficará impedida de licitar e contratar com a Administração direta e indireta do Estado de São Paulo, pelo prazo de até 05 (cinco) anos, a pessoa física ou jurídica, que praticar quaisquer atos previstos no artigo 7º da Lei Federal nº 10.520/2002, sem prejuízo da responsabilidade civil ou criminal, quando couber.

12.2. A sanção de que trata o subitem anterior poderá ser aplicada juntamente com as multas previstas no **ANEXO IV** deste Edital, garantido o exercício de prévia e ampla defesa, e deverá ser registrada no CAUFESP, no “Sistema Eletrônico de Aplicação e Registro de Sanções Administrativas – e-Sanções”, no endereço www.esancoes.sp.gov.br, e também no “Cadastro Nacional de Empresas Inidôneas e Suspensas – CEIS”, no endereço <http://www.portaltransparencia.gov.br/ceis>.

12.3. As sanções são autônomas e a aplicação de uma não exclui a de outra.

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almoxarifado

12.4. O contratante poderá descontar das faturas os valores correspondentes às multas que eventualmente lhe forem aplicadas por descumprimento de obrigações estabelecidas neste Edital, seus anexos ou no termo de contrato.

12.5. A prática de atos que atentem contra o patrimônio público nacional ou estrangeiro, contra princípios da administração pública, ou que de qualquer forma venham a constituir fraude ou corrupção, durante a licitação ou ao longo da execução do contrato, será objeto de instauração de processo administrativo de responsabilização nos termos da Lei Federal nº 12.846/2013 e do Decreto Estadual nº 60.106/2014, sem prejuízo da aplicação das sanções administrativas previstas nos artigos 87 e 88 da Lei Federal nº 8.666/1993, e no artigo 7º da Lei Federal nº 10.520/2002.

13. DA GARANTIA DE EXECUÇÃO CONTRATUAL

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

14. DAS IMPUGNAÇÕES E DOS PEDIDOS DE ESCLARECIMENTOS

14.1. Qualquer pessoa poderá pedir esclarecimentos ou impugnar o ato convocatório deste Pregão Eletrônico em até 02 (dois) dias úteis anteriores à data fixada para a abertura da sessão pública.

14.2. As impugnações e os pedidos de esclarecimentos serão formulados por meio eletrônico, em campo próprio do sistema, encontrado na opção "EDITAL".

14.3. As impugnações serão decididas pelo subscritor do Edital e os pedidos de esclarecimentos respondidos pelo Pregoeiro até o dia útil anterior à data fixada para a abertura da sessão pública.

14.4. Acolhida a impugnação contra o ato convocatório, será designada nova data para realização da sessão pública, se for o caso.

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

14.6. As decisões das impugnações e as respostas aos pedidos de esclarecimentos serão entranhados aos autos do processo licitatório e estarão disponíveis para consulta por qualquer interessado.

14.7. A ausência de impugnação implicará na aceitação tácita, pelo licitante, das condições previstas neste Edital e em seus anexos, em especial no Termo de Referência e na minuta de termo de contrato.

15. DAS DISPOSIÇÕES GERAIS

15.1. 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.

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almoxarifado

15.2. Os casos omissos serão solucionados pelo Pregoeiro e as questões relativas ao sistema, pelo Departamento de Contratações Eletrônicas, da Secretaria da Fazenda.

15.3. Das sessões públicas de processamento do Pregão serão lavradas atas circunstanciadas, observado o disposto no artigo 14, inciso IX, do Regulamento anexo à Resolução CC-27/2006, a serem assinadas pelo Pregoeiro e pela equipe de apoio.

15.4. O sistema manterá sigilo quanto à identidade das licitantes:

15.4.1. Para o Pregoeiro, até a etapa de negociação com o autor da melhor oferta;

15.4.2. Para os demais participantes, até a etapa de habilitação;

15.5. Será excluído do certame o licitante que, por quaisquer meios, antes ou durante a sessão pública, franqueie, permita ou possibilite a sua identificação para a Unidade Compradora, para o Pregoeiro ou para os demais participantes em qualquer momento, desde a publicação do aviso até a conclusão da etapa de negociação, especialmente no preenchimento do formulário eletrônico para a entrega das propostas.

15.6. A exclusão de que trata o item anterior dar-se-á por meio de desclassificação do licitante na etapa "Análise de Propostas" e/ou pela não aceitabilidade do preço pelo pregoeiro na etapa "Análise da Aceitabilidade de Preço".

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

15.7.1. As falhas passíveis de saneamento na documentação apresentada pelo licitante são aquelas cujo conteúdo retrate situação fática ou jurídica já existente na data da abertura da sessão pública deste Pregão.

15.7.2. O desatendimento de exigências formais não essenciais não importará no afastamento do licitante, desde que seja possível o aproveitamento do ato, observados os princípios da isonomia e do interesse público.

15.8. 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 "NEGÓCIOS PÚBLICOS" e www.bec.sp.gov.br, opção "PREGÃO ELETRÔNICO".

15.9. 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.

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almoxarifado

16. DOS ANEXOS

16. Integram o presente Edital:

- ANEXO I -** TERMO DE REFERÊNCIA;
- ANEXO II -** MODELO DE PLANILHA DE PROPOSTA;
- ANEXO III -** MODELOS DE DECLARAÇÕES;
- ANEXO IV -** CÓPIA DA RESOLUÇÃO SDECTI Nº 12;
- ANEXO V -** MINUTA DE CONTRATO

São Paulo, 27 de março de 2018.

FÁBIO ROBERTO IGRISSIS
Subscritor do Edital

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almoxarifado

ANEXO I
TERMO DE REFERÊNCIA

1. Servidor de Administração e Console Administrativa

1.1 Compatibilidade:

- 1.1.1. Microsoft Windows Server 2008 (Todas edições);
- 1.1.2. Microsoft Windows Server 2008 x64 SP1 (Todas edições);
- 1.1.3. Microsoft Windows Server 2008 R2 (Todas edições);
- 1.1.4. Microsoft Windows Server 2012 (Todas edições);
- 1.1.5. Microsoft Windows Server 2012 R2 (Todas edições);
- 1.1.6. Microsoft Windows Small Business Server 2008 (Todas edições);
- 1.1.7. Microsoft Windows Small Business Server 2011 (Todas edições);
- 1.1.8. Microsoft Windows 7 Professional / Enterprise / Ultimate;
- 1.1.9. Microsoft Windows 7 Professional / Enterprise / Ultimate x64;
- 1.1.10. Microsoft Windows 8 Professional / Enterprise;
- 1.1.11. Microsoft Windows 8 Professional / Enterprise x64;
- 1.1.12. Microsoft Windows 8.1 Professional / Enterprise;
- 1.1.13. Microsoft Windows 8.1 Professional / Enterprise x64.

1.2. Suporta as seguintes plataformas virtuais:

- 1.2.1. 1.2.2. Microsoft Hyper-V: 2008, 2008 R2, 2012, 2012 R2;
- 1.2.6. Oracle VM VirtualBox 4.0.4-70112 (Somente logon como convidado)

1.3. Características:

- 1.3.1. A console deve ser acessada via WEB (HTTPS) ou MMC;
- 1.3.2. Console deve ser baseada no modelo cliente/servidor;
- 1.3.3. Compatibilidade com Windows Failover Clustering ou outra solução de alta disponibilidade;
- 1.3.4. Deve permitir a atribuição de perfis para os administradores da Solução de Antivírus;
- 1.3.5. Console deve ser totalmente integrada com suas funções e módulos caso haja a necessidade no futuro de adicionar novas tecnologias tais como, criptografia;
- 1.3.6. As licenças deverão ser perpétuas, ou seja, expirado a validade da mesma o produto deverá permanecer funcional para a proteção contra códigos maliciosos utilizando as definições até o momento da expiração da licença;
- 1.3.7. Capacidade de remover remotamente e automaticamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores;
- 1.3.8. Capacidade de instalar remotamente a solução de antivírus nas estações e servidores Windows, através de compartilhamento administrativo, login script e/ou GPO de Active Directory;
- 1.3.9. Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria;
- 1.3.10. A solução de gerência deve permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas;
- 1.3.11. Através da solução de gerência, deve ser possível verificar qual licença está aplicada para determinado computador;
- 1.3.12. A solução de gerência centralizada deve permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle;

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almoxarifado

- 1.3.13. Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux e Mac) protegidos pela solução antivírus;
- 1.3.14. Capacidade de gerar pacotes customizados (auto executáveis) contendo a licença e configurações do produto;
- 1.3.15. Capacidade de atualizar os pacotes de instalação com as últimas vacinas;
- 1.3.16. Deve ser capaz de fazer instalações a partir de arquivos executáveis utilizando a console de gerenciamento
- 1.3.17. A comunicação entre o cliente e o servidor de administração deve ser criptografada;
- 1.3.18. Deve permitir a realocação de máquinas novas na rede para um determinado grupo sem ter um agente ou endpoint instalado utilizando um dos seguintes parâmetros:
 - Nome do computador;
 - Nome do domínio;
 - Range de IP;
 - Sistema Operacional;
 - Máquina virtual.
- 1.3.19. Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas;
- 1.3.20. Capacidade de monitorar diferentes subnets de rede a fim de encontrar máquinas novas para serem adicionadas à proteção;
- 1.3.21. Capacidade de monitorar grupos de trabalhos já existentes e quaisquer grupos de trabalho que forem criados na rede, a fim de encontrar máquinas novas para serem adicionadas a proteção;
- 1.3.22. Capacidade de, assim que detectar máquinas novas no Active Directory, subnets ou grupos de trabalho, automaticamente importar a máquina para a estrutura de proteção da console e verificar se possui o antivírus instalado. Caso não possuir, deve instalar o antivírus automaticamente;
- 1.3.23. Capacidade de agrupar máquinas por características comuns, sem a necessidade de movê-las de seus grupos originais
- 1.3.24. Capacidade de definir políticas de configurações diferentes por grupos de estações, permitindo que sejam criados subgrupos e com função de herança de políticas entre grupos e subgrupos;
- 1.3.25. Deve fornecer as seguintes informações dos computadores:
 - 1.3.25.1. Se o antivírus está instalado;
 - 1.3.25.2. Se o antivírus está iniciado;
 - 1.3.25.3. Se o antivírus está atualizado;
 - 1.3.25.4. Minutos/horas desde a última conexão da máquina com o servidor administrativo;
 - 1.3.25.5. Minutos/horas desde a última atualização de vacinas;
 - 1.3.25.6. Data e horário da última verificação executada na máquina;
 - 1.3.25.7. Versão do antivírus instalado na máquina;
 - 1.3.25.8. Data e horário de quando a máquina foi ligada;
 - 1.3.25.9. Quantidade de vírus encontrados;
 - 1.3.25.10. Nome do computador;
 - 1.3.25.11. Domínio ou grupo de trabalho do computador;
 - 1.3.25.12. Data e horário da última atualização de vacinas;
 - 1.3.25.13. Sistema operacional com Service Pack;
 - 1.3.25.14. Quantidade de processadores;
 - 1.3.25.15. Quantidade de memória RAM;
 - 1.3.25.16. Usuário(s) logado(s) naquele momento;
 - 1.3.25.17. Endereço IP;

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almoxarifado

- 1.3.25.18. Informação de hardware como: processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de áudio, adaptadores de rede, monitores, drives de CD/DVD;
- 1.3.25.19. Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterá-las;
- 1.3.25.20. Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como:
 - 1.3.25.21. Alteração de Gateway Padrão;
 - 1.3.25.22. Alteração de subrede;
 - 1.3.25.23. Alteração de domínio;
 - 1.3.25.24. Alteração de servidor DHCP;
 - 1.3.25.25. Alteração de servidor DNS;
 - 1.3.25.26. Alteração de servidor WINS;
 - 1.3.25.27. Alteração de subrede;
 - 1.3.25.28. Resolução de Nome;
 - 1.3.25.29. Disponibilidade de endereço de conexão SSL;
- 1.3.26. Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet;
- 1.3.27. Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes;
- 1.3.28. Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus;
- 1.3.29. Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos;
- 1.3.30. Capacidade de eleger qualquer computador cliente como repositório de vacinas e de pacotes de instalação, sem que seja necessária a instalação de um servidor administrativo completo.
- 1.3.31. Capacidade de fazer deste repositório de vacinas um gateway para conexão com o servidor de administração, para que outras máquinas que não consigam conectar-se diretamente ao servidor possam usar este gateway para receber e enviar informações ao servidor administrativo;
- 1.3.32. Capacidade de exportar relatórios para os seguintes tipos de arquivos: PDF, HTML e XML;
- 1.3.33. Capacidade de gerar traps SNMP para monitoramento de eventos;
- 1.3.34. Capacidade de enviar e-mails para contas específicas em caso de algum evento;
- 1.3.35. Deve possuir documentação da estrutura do banco de dados para geração de relatórios a partir de ferramentas específicas de consulta (Crystal Reports, por exemplo).
- 1.3.36. Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado intervalo de tempo);
- 1.3.37. Capacidade de realizar atualização incremental de vacinas nos computadores clientes;
- 1.3.38. Deve armazenar localmente e enviar ao servidor de gerência a ocorrência de vírus com os seguintes dados, no mínimo:
 - Nome do vírus;
 - Nome do arquivo infectado;
 - Data e hora da detecção;
 - Nome da máquina ou endereço IP;
 - Ação realizada.

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almoxarifado

- 1.3.39. Capacidade de realizar inventário de hardware de todas as máquinas clientes.
- 1.3.40. Suportar máquinas com arquitetura 32 bits e 64 bits.

Estações Windows

1.3 Compatibilidade:

- 1.3.41 Microsoft Windows 7 Professional/Enterprise/Ultimate x86 / x64 e posterior;
- 1.3.42 Microsoft Windows 8 Professional/Enterprise x86 / x64;
- 1.3.43 Microsoft Windows 8.1 Pro / Enterprise x86 / x64;
- 1.3.44 Microsoft Windows 10 Pro / Enterprise x86 / x64.

1.4 Características:

- 1.4.41 Deve prover as seguintes proteções:
 - 1.4.41.5 Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc.) que verifique qualquer arquivo criado, acessado ou modificado;
 - 1.4.41.6 Antivírus de Web (módulo para verificação de sites e downloads contra vírus);
 - 1.4.41.7 Antivírus de E-mail (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos);
 - 1.4.41.8 Antivírus de Mensagens Instantâneas
 - 1.4.41.9 O Endpoint deve possuir opção para rastreamento por linha de comando, parametrizável, com opção de limpeza;
 - 1.4.41.10 Firewall com IDS;
 - 1.4.41.11 Autoproteção (contra-ataques aos serviços/processos do antivírus);
 - 1.4.41.12 Controle de dispositivos externos;
 - 1.4.41.13 Controle de acesso a sites por categoria;
 - 1.4.41.14 Controle de acesso a sites por horário;
 - 1.4.41.15 Controle de acesso a sites por usuários;
 - 1.4.41.16 Controle de execução de aplicativos;
- 1.4.42 Capacidade de escolher quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
- 1.4.43 As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários diariamente e em caso de novas ameaças disponibilizar vacinas extras.
- 1.4.44 Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade.
- 1.4.45 Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex.: "Win32.Trojan.banker") para que qualquer objeto detectado com o veredicto escolhido seja ignorado;
- 1.4.46 Capacidade de adicionar aplicativos a uma lista de "aplicativos confiáveis", onde as atividades de rede, atividades de disco e acesso ao registro do Windows não serão monitoradas;
- 1.4.47 Possibilidade desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);
- 1.4.48 Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
- 1.4.49 Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção.
- 1.4.50 Capacidade de verificar somente arquivos novos e alterados;

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almoxarifado

- 1.4.51 Capacidade de verificar objetos usando heurística;
- 1.4.52 Capacidade de agendar uma pausa na verificação;
- 1.4.53 Deve permitir a filtragem de conteúdo de URL avançada efetuando a classificação dos sites em categorias;
- 1.4.54 O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
 - 1.4.54.5 Perguntar o que fazer, ou;
 - 1.4.54.6 Bloquear acesso ao objeto;
 - 1.4.54.6.1 Apagar o objeto ou tentar desinfecção (de acordo com a configuração pré-estabelecida pelo administrador);
 - 1.4.54.6.2 Caso positivo de desinfecção:
 - 1.4.54.6.2.1 Restaurar o objeto para uso;
 - 1.4.54.6.3 Caso negativo de desinfecção:
 - 1.4.54.6.3.1 Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);
- 1.4.55 Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar uma cópia do objeto;
- 1.4.56 Capacidade de verificar e-mails recebidos e enviados;
- 1.4.57 Capacidade de verificar arquivos de ICQ, MSN, AIM e IRC contra vírus e links phishings;
- 1.4.58 Capacidade de verificar links inseridos em e-mails contra phishings;
- 1.4.59 Capacidade de verificar tráfego nos browsers: Internet Explorer, Firefox e Opera;
- 1.4.60 Capacidade de verificação de corpo e anexos de e-mails usando heurística;

- 1.4.61 O antivírus de e-mail, ao encontrar um objeto potencialmente perigoso, deve:
 - 1.4.61.5 Perguntar o que fazer, ou;
 - 1.4.61.6 Bloquear o e-mail;
 - 1.4.61.6.1 Apagar o objeto ou tentar desinfecção (de acordo com a configuração pré-estabelecida pelo administrador);
 - 1.4.61.6.2 Caso positivo de desinfecção:
 - 1.4.61.6.2.1 Restaurar o e-mail para o usuário;
 - 1.4.61.6.3 Caso negativo de desinfecção:
 - 1.4.61.6.3.1 Mover para quarentena ou apagar o objeto (de acordo com a configuração pré-estabelecida pelo administrador);
- 1.4.62 Caso o e-mail conter código que parece ser, mas não é definitivamente malicioso, o mesmo deve ser mantido em quarentena;
- 1.4.63 Possibilidade de verificar todos os e-mails;
- 1.4.64 Capacidade de filtrar anexos de e-mail, apagando-os ou renomeando-os de acordo com a configuração feita pelo administrador;
- 1.4.65 Capacidade de verificação de tráfego HTTP e qualquer script do Windows Script Host (JavaScript, Visual Basic Script, etc.), usando heurísticas;
- 1.4.66 Deve ter suporte total ao protocolo IPv6;
- 1.4.67 Capacidade de alterar as portas monitoradas pelos módulos de Web e E-mail;
- 1.4.68 Na verificação de tráfego web, caso encontrado código malicioso o programa deve:
 - 1.4.68.5 Perguntar o que fazer, ou;
 - 1.4.68.6 Bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio, ou;
 - 1.4.68.7 Permitir acesso ao objeto;
- 1.4.69 Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus de web;
- 1.4.70 Deve possuir módulo que analise as ações de cada aplicação em execução no computador, gravando as ações executadas e comparando-as com sequências

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almoxarifado

- características de atividades perigosas. Tais registros de sequências devem ser atualizados juntamente com as vacinas;
- 1.4.71 Deve possuir módulo que analise cada macro de VBA executada, procurando por sinais de atividade maliciosa;
 - 1.4.72 Deve possuir módulo que analise qualquer tentativa de edição, exclusão ou gravação do registro, de forma que seja possível escolher chaves específicas para serem monitoradas e/ou bloqueadas;
 - 1.4.73 Deve possuir bloqueio de *Phishings*;
 - 1.4.74 Capacidade de distinguir diferentes subnets e conceder opção de ativar ou não o firewall para uma subnet específica;
 - 1.4.75 Deve possuir módulo IDS (*Intrusion Detection System*) para proteção contra *port scans* e exploração de vulnerabilidades de softwares. A base de dados de análise deve ser atualizada juntamente com as vacinas;
 - 1.4.76 O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:
 - 1.4.76.5 Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;
 - 1.4.76.6 Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.
 - 1.4.77 Deve possuir módulo que habilite ou não o funcionamento dos seguintes dispositivos externos, no mínimo:
 - 1.4.77.5 Discos de armazenamento locais;
 - 1.4.77.6 Armazenamento removível;
 - 1.4.77.7 Impressoras;
 - 1.4.77.8 CD/DVD;
 - 1.4.77.9 Drives de disquete;
 - 1.4.77.10 Modems;
 - 1.4.77.11 Dispositivos de fita;
 - 1.4.77.12 Dispositivos multifuncionais;
 - 1.4.77.13 Leitores de smart card;
 - 1.4.77.14 Dispositivos de sincronização via ActiveSync (Windows CE, Windows Mobile, etc.);
 - 1.4.77.15 Wi-Fi;
 - 1.4.77.16 Adaptadores de rede externos;
 - 1.4.77.17 Dispositivos MP3 ou smartphones;
 - 1.4.77.18 Dispositivos Bluetooth;
 - 1.4.77.19 Câmeras e Scanners.
 - 1.4.78 Capacidade de liberar acesso a um dispositivo e usuários por um período de tempo específico, sem a necessidade de desabilitar a proteção e o gerenciamento central ou de intervenção local do administrador na máquina do usuário;
 - 1.4.79 Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por usuário;
 - 1.4.80 Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por agendamento;
 - 1.4.81 Capacidade de configurar novos dispositivos por Class ID/Hardware ID;
 - 1.4.82 Capacidade de limitar o acesso a sites da internet por categoria, por conteúdo (vídeo, áudio, etc.), com possibilidade de configuração por usuário ou grupos de usuários e agendamento;
 - 1.4.83 Capacidade de bloquear execução de aplicativo que está em armazenamento externo;

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almoxarifado

- 1.4.84 Capacidade de limitar o acesso dos aplicativos a recursos do sistema, como chaves do registro e pastas/arquivos do sistema, por categoria, fabricante ou nível de confiança do aplicativo;
- 1.4.85 Capacidade de, em caso de epidemia, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web;
- 1.4.86 Capacidade de, caso o computador cliente saia da rede corporativa, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web.
- 1.4.87 Deve possuir capacidade de inspecionar arquivos suspeitos e detectar comportamentos maliciosos utilizando técnicas de “machine learning”;

2 Estações Mac OS X

2.1 Compatibilidade:

- 2.1.1 Mac OS X 10.11 (El Capitan);
- 2.1.2 Mac OS X 10.10 (Yosemite);
- 2.1.3 Mac OS X 10.9 (Mavericks).

2.2 Características:

- 2.2.1 Deve prover proteção residente para arquivos (anti-spyware, anti-trojan, anti-malware, etc.) que verifique qualquer arquivo criado, acessado ou modificado;
- 2.2.2 Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
- 2.2.3 A instalação e primeira execução do produto deve ser feita sem necessidade de reinicialização do computador, de modo que o produto funcione com toda sua capacidade;
- 2.2.4 As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários diariamente. Quando ocorrer ameaças extras, a vacina deve ser disponibilizada de hora em hora;
- 2.2.5 Capacidade de voltar para a base de dados de vacina anterior;
- 2.2.6 Capacidade de varrer a quarentena automaticamente após cada atualização de vacinas;
- 2.2.7 Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex.: “Win32.Trojan.banker”) para que qualquer objeto detectado com o veredicto escolhido seja ignorado;
- 2.2.8 Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);
- 2.2.9 Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;
- 2.2.10 Capacidade de verificar somente arquivos novos e alterados;
- 2.2.11 Capacidade de verificar objetos usando heurística;
- 2.2.12 Capacidade de agendar uma pausa na verificação;
- 2.2.13 O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
 - 2.2.13.1 Perguntar o que fazer, ou;
 - 2.2.13.2 Bloquear acesso ao objeto;
 - 2.2.13.3 Apagar o objeto ou tentar desinfecá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
 - 2.2.13.4 Caso positivo de desinfecção:

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almoxarifado

- 2.2.13.4.1.1 Restaurar o objeto para uso;
- 2.2.13.4.2 Caso negativo de desinfecção:
 - 2.2.13.4.2.1 Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);
- 2.2.14 Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
- 2.2.15 Capacidade de verificar arquivos de formato de email;
- 2.2.16 Possibilidade de trabalhar com o produto pela linha de comando, com no mínimo opções para atualizar as vacinas, iniciar uma varredura, para o antivírus e iniciar o antivírus pela linha de comando;
- 2.2.17 Capacidade de ser instalado, removido e administrado pela mesma console central de gerenciamento.

3 Estações de trabalho Linux

3.1 Compatibilidade:

3.1.1 Plataforma 32-bits:

- 3.1.1.1 Red Hat Enterprise Linux 5.8 Desktop;
- 3.1.1.2 Red Hat Enterprise Linux 6.2 Desktop;
- 3.1.1.3 CentOS-6.2;
- 3.1.1.4 SUSE Linux Enterprise Desktop 10 SP4;
- 3.1.1.5 SUSE Linux Enterprise Desktop 11 SP2;
- 3.1.1.6 Ubuntu 12.04 LTS.

3.1.2 Plataforma 64-bits:

- 3.1.2.1 Red Hat Enterprise Linux 5.8;
- 3.1.2.2 Red Hat Enterprise Linux 6.2 Desktop;
- 3.1.2.3 CentOS-6.2;
- 3.1.2.4 SUSE Linux Enterprise Desktop 10 SP4;
- 3.1.2.5 SUSE Linux Enterprise Desktop 11 SP2;
- 3.1.2.6 Ubuntu 12.04 LTS.

3.2 Características:

- 3.2.1 Deve prover as seguintes proteções:
 - 3.2.1.1 Antivírus de arquivos residente (anti-spyware, anti-trojan, anti-malware, etc.) que verifique qualquer arquivo criado, acessado ou modificado;
 - 3.2.1.2 As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;
- 3.2.2 Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
 - 3.2.2.1 Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
 - 3.2.2.2 Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfetar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;
 - 3.2.2.3 Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;
 - 3.2.2.4 Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados.

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almoxarifado

- 3.2.3 Em caso erros, deve ter capacidade de criar *logs* automaticamente, sem necessidade de outros softwares;
- 3.2.4 Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
- 3.2.5 Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;
- 3.2.6 Capacidade de verificar objetos usando heurística;
- 3.2.7 Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;
- 3.2.8 Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).

4 Servidores Windows

4.1 Compatibilidade:

4.2 Plataforma 32-bits:

- 4.2.1 Microsoft Windows Server 2008 Standard / Enterprise / DataCenter (SP1 ou posterior);
- 4.2.2 Microsoft Windows Server 2008 Core Standard / Enterprise / DataCenter (SP1 ou posterior).
- 4.2.3 Plataforma 64-bits:
- 4.2.4 Microsoft Windows Server 2008 Standard / Enterprise / DataCenter (SP1 ou posterior);
- 4.2.5 Microsoft Windows Server 2008 Core Standard / Enterprise / DataCenter (SP1 ou posterior);
- 4.2.6 Microsoft Windows Server 2008 R2 Standard / Enterprise / DataCenter (SP1 ou posterior);
- 4.2.7 Microsoft Windows Server 2008 R2 Core Standard / Enterprise / DataCenter (SP1 ou posterior);
- 4.2.8 Microsoft Windows Storage Server 2008 R2;
- 4.2.9 Microsoft Windows Hyper-V Server 2008 R2 (SP1 ou posterior);
- 4.2.10 Microsoft Windows Server 2012 Essentials / Standard / Foundation / Datacenter;
- 4.2.11 Microsoft Windows Server 2012 R2 Essentials / Standard / Foundation / Datacenter;
- 4.2.12 Microsoft Windows Server 2012 Core Essentials / Standard / Foundation / Datacenter;
- 4.2.13 Microsoft Windows Server 2012 R2 Core Essentials / Standard / Foundation / Datacenter;
- 4.2.14 Microsoft Windows Storage Server 2012 (Todas edições);
- 4.2.15 Microsoft Windows Storage Server 2012 R2 (Todas edições);
- 4.2.16 Microsoft Windows Hyper-V Server 2012;
- 4.2.17 Microsoft Windows Hyper-V Server 2012 R2.

4.3 Características:

- 4.3.1 Deve prover as seguintes proteções:
 - 4.3.1.1 Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc.) que verifique qualquer arquivo criado, acessado ou modificado;
 - 4.3.1.2 Auto-proteção contra-ataques aos serviços/processos do antivírus;
 - 4.3.1.3 Firewall com IDS;

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almoxarifado

- 4.3.2 Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
- 4.3.3 As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;
- 4.3.4 Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
 - 4.3.4.1 Gerenciamento de status de tarefas;
 - 4.3.4.2 Gerenciamento de tarefa (criar ou excluir tarefas de verificação);
 - 4.3.4.3 Leitura de configurações;
 - 4.3.4.4 Modificação de configurações;
 - 4.3.4.5 Visualização de relatórios;
 - 4.3.4.6 Gerenciamento de relatórios;
 - 4.3.4.7 Gerenciamento de permissões (adicionar/excluir permissões acima);
- 4.3.5 O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:
 - 4.3.5.1 Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;
 - 4.3.5.2 Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.
- 4.3.6 Em caso de erros, deve ter capacidade de criar *logs* e *traces* automaticamente, sem necessidade de outros softwares;
- 4.3.7 Capacidade de configurar níveis de verificação diferentes para cada pasta, grupo de pastas ou arquivos do servidor;
- 4.3.8 Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;
- 4.3.9 Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex.: "Win32.Trojan.banker") para que qualquer objeto detectado com o veredicto escolhido seja ignorado;
- 4.3.10 Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
- 4.3.11 Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;
- 4.3.12 Capacidade de verificar somente arquivos novos e alterados;
- 4.3.13 Capacidade de escolher qual tipo de objeto composto será verificado (ex: arquivos comprimidos, arquivos auto descompressores, .PST, arquivos compactados por compactadores binários, etc.);
 - 4.3.14 Capacidade de verificar objetos usando heurística;
 - 4.3.15 Capacidade de configurar diferentes ações para diferentes tipos de ameaças;
 - 4.3.16 Capacidade de agendar uma pausa na verificação;
 - 4.3.17 Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;
 - 4.3.18 O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
 - 4.3.18.1 Perguntar o que fazer, ou;
 - 4.3.18.2 Bloquear acesso ao objeto;
 - 4.3.18.2.1 Apagar o objeto ou tentar desinfecá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
 - 4.3.18.2.2 Caso positivo de desinfecção:
 - 4.3.18.2.2.1 Restaurar o objeto para uso;
 - 4.3.18.2.2.3 Caso negativo de desinfecção:

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almoxarifado

- 4.3.18.2.3.1 Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);
- 4.3.19 Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
- 4.3.20 Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;
- 4.3.21 Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;
- 4.3.22 Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa.

5 Servidores Linux

5.1 Compatibilidade:

Plataforma 32-bits:

- 5.1.1 Red Hat Enterprise Linux Server 5.x;
- 5.1.2 Red Hat® Enterprise Linux® Server 6.x (6.0 - 6.6);
- 5.1.3 CentOS 6.x (6.0 - 6.6);
- 5.1.4 SUSE® Linux Enterprise Server 11 SP3;
- 5.1.5 Ubuntu Server 12.04 LTS;
- 5.1.6 Ubuntu Server 14.04 LTS;
- 5.1.7 Ubuntu Server 14.10;
- 5.1.8 Oracle Linux 6.5;

Plataforma 64-bits:

- 5.1.9 Red Hat Enterprise Linux Server 5.x;
- 5.1.10 Red Hat Enterprise Linux Server 6.x (6.0 - 6.6);
- 5.1.11 Red Hat Enterprise Linux Server 7;
- 5.1.12 CentOS-6.x (6.0 - 6.6);
- 5.1.13 CentOS-7.0;
- 5.1.14 SUSE Linux Enterprise Server 11 SP3;
- 5.1.15 SUSE Linux Enterprise Server 12;
- 5.1.16 Novell Open Enterprise Server 11 SP1;
- 5.1.17 Novell Open Enterprise Server 11 SP2;
- 5.1.18 Ubuntu Server 12.04 LTS;
- 5.1.19 Ubuntu Server 14.04 LTS;
- 5.1.20 Ubuntu Server 14.10;
- 5.1.21 Oracle Linux 6.5;
- 5.1.22 Oracle Linux 7.0;

6.2. Características:

- 6.2.1. Deve prover as seguintes proteções:
 - 6.2.1.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc.) que verifique qualquer arquivo criado, acessado ou modificado;
 - 6.2.1.2. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;
- 6.2.2. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almoxarifado

- 6.2.2.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
- 6.2.3. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
- 6.2.3.1. Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;
- 6.2.3.2. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados;
- 6.2.4. Em caso erros, deve ter capacidade de criar *logs* automaticamente, sem necessidade de outros softwares;
- 6.2.5. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
- 6.2.6. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;
- 6.2.7. Capacidade de verificar objetos usando heurística;
- 6.2.8. Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).

6.3. Características:

- 6.3.1. Deve possuir proteção em tempo real para arquivos acessados, criados ou modificados;
- 6.3.2. Deve possuir verificação manual e agendada de acordo com a configuração do administrador;
- 6.3.3. Capacidade de realizar update de maneira automática, via internet ou LAN;
- 6.3.4. Capacidade de fazer um rollback das vacinas;
- 6.3.5. Capacidade de mover arquivos suspeitos ou infectados para área de quarentena;
- 6.3.6. Capacidade de criar logs detalhados e salvar resultados das verificações agendadas;
- 6.3.7. Capacidade de notificar o administrador de varreduras concluídas e sobre objetos maliciosos encontrados no servidor, utilizando e-mail.

7. Criptografia

7.1. Compatibilidade:

- 7.1.1. Microsoft Windows 7 Professional/Enterprise/Ultimate;
- 7.1.2. Microsoft Windows 7 Professional/Enterprise/Ultimate x64;
- 7.1.3. Microsoft Windows 8 Professional/Enterprise;
- 7.1.4. Microsoft Windows 8 Professional/Enterprise x64;
- 7.1.5. Microsoft Windows 8.1 Professional / Enterprise;
- 7.1.6. Microsoft Windows 8.1 Professional / Enterprise x64;
- 7.1.7. Microsoft Windows 10 Pro x86 / x64;
- 7.1.8. Microsoft Windows 10 Enterprise x86 /x64.

7.2. Características:

- 7.2.1. O acesso ao recurso criptografado (arquivo, pasta ou disco) deve ser garantido mesmo em caso o usuário tenha esquecido a senha, através de procedimentos de recuperação;
- 7.2.2. Utilizar, no mínimo, algoritmo AES com chave de 256 bits;
- 7.2.3. Capacidade de criptografar completamente o disco rígido da máquina, adicionando um ambiente de Pré-boot para autenticação do usuário;
- 7.2.4. Capacidade de utilizar *Single Sign-On* para a autenticação de Pré-boot;

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almoxarifado

- 7.2.5. Permitir criar vários usuários de autenticação Pré-boot;
- 7.2.6. Capacidade de criar um usuário de autenticação Pré-boot comum com uma senha igual para todas as máquinas a partir da console de gerenciamento;
- 7.2.7. Capacidade de criptografar drives removíveis de acordo com regra criada pelo administrador, com as opções:
 - 7.2.7.1. Criptografar somente os arquivos novos que forem copiados para o disco removível, sem modificar os arquivos já existentes;
 - 7.2.7.2. Criptografar todos os arquivos individualmente;
 - 7.2.7.3. Criptografar o dispositivo inteiro, de maneira que não seja possível listar os arquivos e pastas armazenadas;
 - 7.2.7.4. Criptografar o dispositivo em modo portátil, permitindo acessar os arquivos em máquinas de terceiros através de uma senha;
- 7.2.8. Capacidade de selecionar pastas e arquivos (por tipo, ou extensão) para serem criptografados automaticamente. Nesta modalidade, os arquivos devem estar acessíveis para todas as máquinas gerenciadas pela mesma console de maneira transparente para os usuários;
- 7.2.9. Capacidade de criar regras de exclusões para que certos arquivos ou pastas nunca sejam criptografados;
- 7.2.10. Capacidade de selecionar aplicações que podem ou não ter acesso aos arquivos criptografados;
- 7.2.11. Verifica compatibilidade de hardware antes de aplicar a criptografia;
- 7.2.12. Possibilita estabelecer parâmetros para a senha de criptografia;
- 7.2.13. Bloqueia o reuso de senhas;
- 7.2.14. Bloqueia a senha após um número de tentativas pré-estabelecidas;
- 7.2.15. Capacidade de permitir o usuário solicitar permissão a determinado arquivo criptografado para o administrador mediante templates customizados;
- 7.2.16. Permite criar exclusões para não criptografar determinados “discos rígidos” através de uma busca por nome do computador ou nome do dispositivo
- 7.2.17. Permite criptografar as seguintes pastas pré-definidas: “meus documentos”, “Favoritos”, “Desktop”, “Arquivos temporários” e “Arquivos do Outlook”;
- 7.2.18. Permite utilizar variáveis de ambiente para criptografar pastas customizadas;
- 7.2.19. Capacidade de criptografar arquivos por grupos de extensão, tais como: Documentos do office, Document, arquivos de áudio, etc.;
- 7.2.20. Permite criar um grupo de extensões de arquivos a serem criptografados;
- 7.2.21. Capacidade de criar regra de criptografia para arquivos gerados por aplicações;
- 7.2.22. Permite criptografia de dispositivos móveis mesmo quando o endpoint não possuir comunicação com a console de gerenciamento.

8. Gerenciamento de Sistemas

- 8.1. Capacidade de registrar mudanças de hardware nas máquinas gerenciadas;
- 8.2. Capacidade de gerenciar um inventário de hardware, com a possibilidade de cadastro de dispositivos
- 8.3. Possibilita fazer distribuição de software de forma manual e agendada;
- 8.4. Suporta modo de instalação silenciosa;
- 8.5. Suporte a pacotes MSI, exe, bat, cmd e outros padrões de arquivos executáveis;
- 8.6. Possibilita fazer a distribuição através de agentes de atualização;
- 8.7. Utiliza tecnologia multicast para evitar tráfego na rede;
- 8.8. O licenciamento deve ser único tanto para servidores quanto para estações de trabalho

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almoxarifado

- 8.9. As licenças deverão ser perpétuas, ou seja, expirado a validade da mesma o produto deverá permanecer funcional para a proteção contra códigos maliciosos utilizando as definições até o momento da expiração do contrato.
- 8.10. A console de gerenciamento poderá ser instalada em um ambiente na nuvem (Azure, AWS, Google, etc.).
- 8.11. Capacidade de gerenciar dispositivos da nuvem e localmente.
- 8.12. Deve possuir uma console de gerenciamento via WEB

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almoxarifado

ANEXO I. "A"

Servidor de Administração e Console Administrativa
Compatibilidade:

- 1.1.1 Microsoft Windows Server 2008 (Todas edições);
- 1.1.2 Microsoft Windows Server 2008 x64 SP1 (Todas edições);
- 1.1.3 Microsoft Windows Server 2008 R2 (Todas edições);
- 1.1.4 Microsoft Windows Server 2012 (Todas edições);
- 1.1.5 Microsoft Windows Server 2012 R2 (Todas edições);
- 1.1.6 Microsoft Windows Small Business Server 2008 (Todas edições);
- 1.1.7 Microsoft Windows Small Business Server 2011 (Todas edições);
- 1.1.8 Microsoft Windows 7 Professional / Enterprise / Ultimate;
- 1.1.9 Microsoft Windows 7 Professional / Enterprise / Ultimate x64;
- 1.1.10 Microsoft Windows 8 Professional / Enterprise;
- 1.1.11 Microsoft Windows 8 Professional / Enterprise x64;
- 1.1.12 Microsoft Windows 8.1 Professional / Enterprise;
- 1.1.13 Microsoft Windows 8.1 Professional / Enterprise x64.

1.2 Suporta as seguintes plataformas virtuais:

- 1.2.2. Microsoft Hyper-V: 2008, 2008 R2, 2012, 2012 R2;
- 1.2.6. Oracle VM VirtualBox 4.0.4-70112 (Somente logon como convidado);

1.3 Características:

- 1.3.1 A console deve ser acessada via WEB (HTTPS) ou MMC;
- 1.3.2 Console deve ser baseada no modelo cliente/servidor;
- 1.3.3 Compatibilidade com Windows Failover Clustering ou outra solução de alta disponibilidade;
- 1.3.4 Deve permitir a atribuição de perfis para os administradores da Solução de Antivírus;
- 1.3.5 Console deve ser totalmente integrada com suas funções e módulos caso haja a necessidade no futuro de adicionar novas tecnologias tais como, criptografia;
- 1.3.6 As licenças deverão ser perpétuas, ou seja, expirado a validade da mesma o produto deverá permanecer funcional para a proteção contra códigos maliciosos utilizando as definições até o momento da expiração da licença;
- 1.3.7 Capacidade de remover remotamente e automaticamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores;
- 1.3.8 Capacidade de instalar remotamente a solução de antivírus nas estações e servidores Windows, através de compartilhamento administrativo, login script e/ou GPO de Active Directory;
- 1.3.9 Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria;
- 1.3.10 A solução de gerência deve permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas;
- 1.3.11 Através da solução de gerência, deve ser possível verificar qual licença está aplicada para determinado computador;
- 1.3.12 A solução de gerência centralizada deve permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle;
- 1.3.13 Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux e Mac) protegidos pela solução antivírus;

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almoxarifado

- 1.3.14 Capacidade de gerar pacotes customizados (auto executáveis) contendo a licença e configurações do produto;
- 1.3.15 Capacidade de atualizar os pacotes de instalação com as últimas vacinas;
- 1.3.16 Deve ser capaz de fazer instalações a partir de arquivos executáveis utilizando a console de gerenciamento
- 1.3.17 A comunicação entre o cliente e o servidor de administração deve ser criptografada;
- 1.3.18 Deve permitir a realocação de máquinas novas na rede para um determinado grupo sem ter um agente ou endpoint instalado utilizando um dos seguintes parâmetros:
 - Nome do computador;
 - Nome do domínio;
 - Range de IP;
 - Sistema Operacional;
 - Máquina virtual.
- 1.3.19 Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas;
- 1.3.20 Capacidade de monitorar diferentes subnets de rede a fim de encontrar máquinas novas para serem adicionadas à proteção;
- 1.3.21 Capacidade de monitorar grupos de trabalhos já existentes e quaisquer grupos de trabalho que forem criados na rede, a fim de encontrar máquinas novas para serem adicionadas a proteção;
- 1.3.22 Capacidade de, assim que detectar máquinas novas no Active Directory, subnets ou grupos de trabalho, automaticamente importar a máquina para a estrutura de proteção da console e verificar se possui o antivírus instalado. Caso não possuir, deve instalar o antivírus automaticamente;
- 1.3.23 Capacidade de agrupar máquinas por características comuns, sem a necessidade de movê-las de seus grupos originais
- 1.3.24 Capacidade de definir políticas de configurações diferentes por grupos de estações, permitindo que sejam criados subgrupos e com função de herança de políticas entre grupos e subgrupos;
- 1.3.25 Deve fornecer as seguintes informações dos computadores:
 - 1.3.25.1 Se o antivírus está instalado;
 - 1.3.25.2 Se o antivírus está iniciado;
 - 1.3.25.3 Se o antivírus está atualizado;
 - 1.3.25.4 Minutos/horas desde a última conexão da máquina com o servidor administrativo;
 - 1.3.25.5 Minutos/horas desde a última atualização de vacinas;
 - 1.3.25.6 Data e horário da última verificação executada na máquina;
 - 1.3.25.7 Versão do antivírus instalado na máquina;
 - 1.3.25.8 Data e horário de quando a máquina foi ligada;
 - 1.3.25.9 Quantidade de vírus encontrados;
 - 1.3.25.10 Nome do computador;
 - 1.3.25.11 Domínio ou grupo de trabalho do computador;
 - 1.3.25.12 Data e horário da última atualização de vacinas;
 - 1.3.25.13 Sistema operacional com Service Pack;
 - 1.3.25.14 Quantidade de processadores;
 - 1.3.25.15 Quantidade de memória RAM;
 - 1.3.25.16 Usuário(s) logado(s) naquele momento;
 - 1.3.25.17 Endereço IP;

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almoxarifado

- 1.3.25.18 Informação de hardware como: processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de áudio, adaptadores de rede, monitores, drives de CD/DVD;
- 1.3.26 Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterá-las;
- 1.3.27 Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como:
- 1.3.27.1 Alteração de Gateway Padrão;
- 1.3.27.2 Alteração de subrede;
- 1.3.27.3 Alteração de domínio;
- 1.3.27.4 Alteração de servidor DHCP;
- 1.3.27.5 Alteração de servidor DNS;
- 1.3.27.6 Alteração de servidor WINS;
- 1.3.27.7 Alteração de subrede;
- 1.3.27.8 Resolução de Nome;
- 1.3.27.9 Disponibilidade de endereço de conexão SSL;
- 1.3.28 Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet;
- 1.3.29 Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes;
- 1.3.30 Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus;
- 1.3.31 Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos;
- 1.3.32 Capacidade de eleger qualquer computador cliente como repositório de vacinas e de pacotes de instalação, sem que seja necessária a instalação de um servidor administrativo completo.
- 1.3.33 Capacidade de fazer deste repositório de vacinas um gateway para conexão com o servidor de administração, para que outras máquinas que não consigam conectar-se diretamente ao servidor possam usar este gateway para receber e enviar informações ao servidor administrativo;
- 1.3.34 Capacidade de exportar relatórios para os seguintes tipos de arquivos: PDF, HTML e XML;
- 1.3.35 Capacidade de gerar traps SNMP para monitoramento de eventos;
- 1.3.36 Capacidade de enviar e-mails para contas específicas em caso de algum evento;
- 1.3.37 Deve possuir documentação da estrutura do banco de dados para geração de relatórios a partir de ferramentas específicas de consulta (Crystal Reports, por exemplo).
- 1.3.38 Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado intervalo de tempo);
- 1.3.39 Capacidade de realizar atualização incremental de vacinas nos computadores clientes;
- 1.3.40 Deve armazenar localmente e enviar ao servidor de gerência a ocorrência de vírus com os seguintes dados, no mínimo:
- Nome do vírus;
 - Nome do arquivo infectado;
 - Data e hora da detecção;
 - Nome da máquina ou endereço IP;
 - Ação realizada.

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almoxarifado

- 1.3.41 Capacidade de realizar inventário de hardware de todas as máquinas clientes.
- 1.3.42 Suportar máquinas com arquitetura 32 bits e 64 bits.
- 1.3.43 Módulo de Resposta

2 Estações Windows

2.1 Compatibilidade:

- 2.1.1 Microsoft Windows 7 Professional/Enterprise/Ultimate x86 / x64 e posterior;
- 2.1.2 Microsoft Windows 8 Professional/Enterprise x86 / x64;
- 2.1.3 Microsoft Windows 8.1 Pro / Enterprise x86 / x64;
- 2.1.4 Microsoft Windows 10 Pro / Enterprise x86 / x64.

2.2 Características:

- 2.2.1 Deve prover as seguintes proteções:
 - 2.2.1.1 Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc.) que verifique qualquer arquivo criado, acessado ou modificado;
 - 2.2.1.2 Antivírus de Web (módulo para verificação de sites e downloads contra vírus);
 - 2.2.1.3 Antivírus de E-mail (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos);
 - 2.2.1.4 Antivírus de Mensagens Instantâneas
 - 2.2.1.5 O Endpoint deve possuir opção para rastreamento por linha de comando, parametrizável, com opção de limpeza;
 - 2.2.1.6 Firewall com IDS;
 - 2.2.1.7 Autoproteção (contra-ataques aos serviços/processos do antivírus);
 - 2.2.1.8 Controle de dispositivos externos;
 - 2.2.1.9 Controle de acesso a sites por categoria;
 - 2.2.1.10 Controle de acesso a sites por horário;
 - 2.2.1.11 Controle de acesso a sites por usuários;
 - 2.2.1.12 Controle de execução de aplicativos;
- 2.2.2 Capacidade de escolher quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
- 2.2.3 As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários diariamente e em caso de novas ameaças disponibilizar vacinas extras.
- 2.2.4 Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade.
- 2.2.5 Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: "Win32.Trojan.banker") para que qualquer objeto detectado com o veredicto escolhido seja ignorado;
- 2.2.6 Capacidade de adicionar aplicativos a uma lista de "aplicativos confiáveis", onde as atividades de rede, atividades de disco e acesso ao registro do Windows não serão monitoradas;
- 2.2.7 Possibilidade desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);
- 2.2.8 Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
- 2.2.9 Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção.
- 2.2.10 Capacidade de verificar somente arquivos novos e alterados;

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almoxarifado

- 2.2.11 Capacidade de verificar objetos usando heurística;
- 2.2.12 Capacidade de agendar uma pausa na verificação;
- 2.2.13 Deve permitir a filtragem de conteúdo de URL avançada efetuando a classificação dos sites em categorias;
- 2.2.14 O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
 - 2.2.14.1 Perguntar o que fazer, ou;
 - 2.2.14.2 Bloquear acesso ao objeto;
 - 2.2.14.2.1 Apagar o objeto ou tentar desinfecção (de acordo com a configuração pré-estabelecida pelo administrador);
 - 2.2.14.2.2 Caso positivo de desinfecção:
 - 2.2.14.2.2.1 Restaurar o objeto para uso;
 - 2.2.14.2.3 Caso negativo de desinfecção:
 - 2.2.14.2.3.1 Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);
- 2.2.15 Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar uma cópia do objeto;
- 2.2.16 Capacidade de verificar e-mails recebidos e enviados;
- 2.2.17 Capacidade de verificar arquivos de ICQ, MSN, AIM e IRC contra vírus e links phishings;
- 2.2.18 Capacidade de verificar links inseridos em e-mails contra phishings;
- 2.2.19 Capacidade de verificar tráfego nos browsers: Internet Explorer, Firefox e Opera;
- 2.2.20 Capacidade de verificação de corpo e anexos de e-mails usando heurística;
- 2.2.21 O antivírus de e-mail, ao encontrar um objeto potencialmente perigoso, deve:
 - 2.2.21.1 Perguntar o que fazer, ou;
 - 2.2.21.2 Bloquear o e-mail;
 - 2.2.21.2.1 Apagar o objeto ou tentar desinfecção (de acordo com a configuração pré-estabelecida pelo administrador);
 - 2.2.21.2.2 Caso positivo de desinfecção:
 - 2.2.21.2.2.1 Restaurar o e-mail para o usuário;
 - 2.2.21.2.3 Caso negativo de desinfecção:
 - 2.2.21.2.3.1 Mover para quarentena ou apagar o objeto (de acordo com a configuração pré-estabelecida pelo administrador);
- 2.2.22 Caso o e-mail conter código que parece ser, mas não é definitivamente malicioso, o mesmo deve ser mantido em quarentena;
- 2.2.23 Possibilidade de verificar todos os e-mails;
- 2.2.24 Capacidade de filtrar anexos de e-mail, apagando-os ou renomeando-os de acordo com a configuração feita pelo administrador;
- 2.2.25 Capacidade de verificação de tráfego HTTP e qualquer script do Windows Script Host (JavaScript, Visual Basic Script, etc.), usando heurísticas;
- 2.2.26 Deve ter suporte total ao protocolo IPv6;
- 2.2.27 Capacidade de alterar as portas monitoradas pelos módulos de Web e E-mail;
- 2.2.28 Na verificação de tráfego web, caso encontrado código malicioso o programa deve:
 - 2.2.28.1 Perguntar o que fazer, ou;
 - 2.2.28.2 Bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio, ou;
 - 2.2.28.3 Permitir acesso ao objeto;
- 2.2.29 Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus de web;
- 2.2.30 Deve possuir módulo que analise as ações de cada aplicação em execução no computador, gravando as ações executadas e comparando-as com sequências

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almoxarifado

- características de atividades perigosas. Tais registros de sequências devem ser atualizados juntamente com as vacinas;
- 2.2.31 Deve possuir módulo que analise cada macro de VBA executada, procurando por sinais de atividade maliciosa;
- 2.2.32 Deve possuir módulo que analise qualquer tentativa de edição, exclusão ou gravação do registro, de forma que seja possível escolher chaves específicas para serem monitoradas e/ou bloqueadas;
- 2.2.33 Deve possuir bloqueio de *Phishings*;
- 2.2.34 Capacidade de distinguir diferentes subnets e conceder opção de ativar ou não o firewall para uma subnet específica;
- 2.2.35 Deve possuir módulo IDS (*Intrusion Detection System*) para proteção contra *port scans* e exploração de vulnerabilidades de softwares. A base de dados de análise deve ser atualizada juntamente com as vacinas;
- 2.2.36 O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:
- 2.2.36.1 Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;
- 2.2.36.2 Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.
- 2.2.37 Deve possuir módulo que habilite ou não o funcionamento dos seguintes dispositivos externos, no mínimo:
- 2.2.37.1 Discos de armazenamento locais;
- 2.2.37.2 Armazenamento removível;
- 2.2.37.3 Impressoras;
- 2.2.37.4 CD/DVD;
- 2.2.37.5 Drives de disquete;
- 2.2.37.6 Modems;
- 2.2.37.7 Dispositivos de fita;
- 2.2.37.8 Dispositivos multifuncionais;
- 2.2.37.9 Leitores de smart card;
- 2.2.37.10 Dispositivos de sincronização via ActiveSync (Windows CE, Windows Mobile, etc.);
- 2.2.37.11 Wi-Fi;
- 2.2.37.12 Adaptadores de rede externos;
- 2.2.37.13 Dispositivos MP3 ou smartphones;
- 2.2.37.14 Dispositivos Bluetooth;
- 2.2.37.15 Câmeras e Scanners.
- 2.2.38 Capacidade de liberar acesso a um dispositivo e usuários por um período de tempo específico, sem a necessidade de desabilitar a proteção e o gerenciamento central ou de intervenção local do administrador na máquina do usuário;
- 2.2.39 Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por usuário;
- 2.2.40 Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por agendamento;
- 2.2.41 Capacidade de configurar novos dispositivos por Class ID/Hardware ID;
- 2.2.42 Capacidade de limitar o acesso a sites da internet por categoria, por conteúdo (vídeo, áudio, etc.), com possibilidade de configuração por usuário ou grupos de usuários e agendamento;
- 2.2.43 Capacidade de bloquear execução de aplicativo que está em armazenamento externo;

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almoxarifado

- 2.2.44 Capacidade de limitar o acesso dos aplicativos a recursos do sistema, como chaves do registro e pastas/arquivos do sistema, por categoria, fabricante ou nível de confiança do aplicativo;
- 2.2.45 Capacidade de, em caso de epidemia, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web;
- 2.2.46 Capacidade de, caso o computador cliente saia da rede corporativa, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web.

3 Estações Mac OS X

3.1 Compatibilidade:

- 3.2 Mac OS X 10.11 (El Capitan);
- 3.3 Mac OS X 10.10 (Yosemite);
- 3.4 Mac OS X 10.9 (Mavericks).

3.5 Características:

- 3.5.1 Deve prover proteção residente para arquivos (anti-spyware, anti-trojan, anti-malware, etc.) que verifique qualquer arquivo criado, acessado ou modificado;
- 3.5.2 Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
- 3.5.3 A instalação e primeira execução do produto deve ser feita sem necessidade de reinicialização do computador, de modo que o produto funcione com toda sua capacidade;
- 3.5.4 As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários diariamente. Quando ocorrer ameaças extras, a vacina deve ser disponibilizada de hora em hora;
- 3.5.5 Capacidade de voltar para a base de dados de vacina anterior;
- 3.5.6 Capacidade de varrer a quarentena automaticamente após cada atualização de vacinas;
- 3.5.7 Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: "Win32.Trojan.banker") para que qualquer objeto detectado com o veredicto escolhido seja ignorado;
- 3.5.8 Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);
- 3.5.9 Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;
- 3.5.10 Capacidade de verificar somente arquivos novos e alterados;
- 3.5.11 Capacidade de verificar objetos usando heurística;
- 3.5.12 Capacidade de agendar uma pausa na verificação;
- 3.5.13 O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
 - 3.5.13.1 Perguntar o que fazer, ou;
 - 3.5.13.2 Bloquear acesso ao objeto;
 - 3.5.13.2.1 Apagar o objeto ou tentar desinfecá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
 - 3.5.13.2.2 Caso positivo de desinfecção:

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almoxarifado

- 3.5.13.2.2.1 Restaurar o objeto para uso;
- 3.5.13.2.3 Caso negativo de desinfecção:
 - 3.5.13.2.3.1 Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);
- 3.5.14 Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
- 3.5.15 Capacidade de verificar arquivos de formato de email;
- 3.5.16 Possibilidade de trabalhar com o produto pela linha de comando, com no mínimo opções para atualizar as vacinas, iniciar uma varredura, para o antivírus e iniciar o antivírus pela linha de comando;
- 3.5.17 Capacidade de ser instalado, removido e administrado pela mesma console central de gerenciamento.

4 Estações de trabalho Linux

4.1 Compatibilidade:

4.1.1 Plataforma 32-bits:

- 4.1.1.1 Red Hat Enterprise Linux 5.8 Desktop;
- 4.1.1.2 Red Hat Enterprise Linux 6.2 Desktop;
- 4.1.1.3 CentOS-6.2;
- 4.1.1.4 SUSE Linux Enterprise Desktop 10 SP4;
- 4.1.1.5 SUSE Linux Enterprise Desktop 11 SP2;
- 4.1.1.6 Ubuntu 12.04 LTS.

4.1.2 Plataforma 64-bits:

- 4.1.2.1 Red Hat Enterprise Linux 5.8;
- 4.1.2.2 Red Hat Enterprise Linux 6.2 Desktop;
- 4.1.2.3 CentOS-6.2;
- 4.1.2.4 SUSE Linux Enterprise Desktop 10 SP4;
- 4.1.2.5 SUSE Linux Enterprise Desktop 11 SP2;
- 4.1.2.6 Ubuntu 12.04 LTS.

4.2 Características:

- 4.2.1 Deve prover as seguintes proteções:
 - 4.2.1.1 Antivírus de arquivos residente (anti-spyware, anti-trojan, anti-malware, etc.) que verifique qualquer arquivo criado, acessado ou modificado;
 - 4.2.1.2 As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;
- 4.2.2 Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
 - 4.2.2.1 Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
 - 4.2.2.2 Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfetar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;
 - 4.2.2.3 Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almoxarifado

- 4.2.2.4 Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados.
- 4.2.3 Em caso erros, deve ter capacidade de criar *logs* automaticamente, sem necessidade de outros softwares;
- 4.2.4 Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
- 4.2.5 Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;
- 4.2.6 Capacidade de verificar objetos usando heurística;
- 4.2.7 Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;
- 4.2.8 Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).

5 Servidores Windows

5.1 Compatibilidade:

5.2 Plataforma 32-bits:

- 5.2.1 Microsoft Windows Server 2008 Standard / Enterprise / DataCenter (SP1 ou posterior);
 - 5.2.2 Microsoft Windows Server 2008 Core Standard / Enterprise / DataCenter (SP1 ou posterior).
- ### **5.3 Plataforma 64-bits:**
- 5.3.1 Microsoft Windows Server 2008 Standard / Enterprise / DataCenter (SP1 ou posterior);
 - 5.3.2 Microsoft Windows Server 2008 Core Standard / Enterprise / DataCenter (SP1 ou posterior);
 - 5.3.3 Microsoft Windows Server 2008 R2 Standard / Enterprise / DataCenter (SP1 ou posterior);
 - 5.3.4 Microsoft Windows Server 2008 R2 Core Standard / Enterprise / DataCenter (SP1 ou posterior);
 - 5.3.5 Microsoft Windows Storage Server 2008 R2;
 - 5.3.6 Microsoft Windows Hyper-V Server 2008 R2 (SP1 ou posterior);
 - 5.3.7 Microsoft Windows Server 2012 Essentials / Standard / Foundation / Datacenter;
 - 5.3.8 Microsoft Windows Server 2012 R2 Essentials / Standard / Foundation / Datacenter;
 - 5.3.9 Microsoft Windows Server 2012 Core Essentials / Standard / Foundation / Datacenter;
 - 5.3.10 Microsoft Windows Server 2012 R2 Core Essentials / Standard / Foundation / Datacenter;
 - 5.3.11 Microsoft Windows Storage Server 2012 (Todas edições);
 - 5.3.12 Microsoft Windows Storage Server 2012 R2 (Todas edições);
 - 5.3.13 Microsoft Windows Hyper-V Server 2012;
 - 5.3.14 Microsoft Windows Hyper-V Server 2012 R2.

5.4 Características:

- 5.4.1 Deve prover as seguintes proteções:
 - 5.4.1.1 Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc.) que verifique qualquer arquivo criado, acessado ou modificado;
 - 5.4.1.2 Auto-proteção contra-ataques aos serviços/processos do antivírus;

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almoxarifado

- 5.4.1.3 Firewall com IDS;
- 5.4.2 Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
- 5.4.3 As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;
- 5.4.4 Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
 - 5.4.4.1 Gerenciamento de status de tarefas;
 - 5.4.4.2 Gerenciamento de tarefa (criar ou excluir tarefas de verificação);
 - 5.4.4.3 Leitura de configurações;
 - 5.4.4.4 Modificação de configurações;
 - 5.4.4.5 Visualização de relatórios;
 - 5.4.4.6 Gerenciamento de relatórios;
 - 5.4.4.7 Gerenciamento de permissões (adicionar/excluir permissões acima);
- 5.4.5 O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:
 - 5.4.5.1 Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;
 - 5.4.5.2 Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.
- 5.4.6 Em caso de erros, deve ter capacidade de criar *logs* e *traces* automaticamente, sem necessidade de outros softwares;
- 5.4.7 Capacidade de configurar níveis de verificação diferentes para cada pasta, grupo de pastas ou arquivos do servidor;
- 5.4.8 Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;
- 5.4.9 Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: "Win32.Trojan.banker") para que qualquer objeto detectado com o veredicto escolhido seja ignorado;
- 5.4.10 Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
- 5.4.11 Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;
- 5.4.12 Capacidade de verificar somente arquivos novos e alterados;
- 5.4.13 Capacidade de escolher qual tipo de objeto composto será verificado (ex: arquivos comprimidos, arquivos auto descompressores, .PST, arquivos compactados por compactadores binários, etc.);
- 5.4.14 Capacidade de verificar objetos usando heurística;
- 5.4.15 Capacidade de configurar diferentes ações para diferentes tipos de ameaças;
- 5.4.16 Capacidade de agendar uma pausa na verificação;
- 5.4.17 Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;
- 5.4.18 O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
 - 5.4.18.1 Perguntar o que fazer, ou;
 - 5.4.18.2 Bloquear acesso ao objeto;
 - 5.4.18.2.1 Apagar o objeto ou tentar desinfecção (de acordo com a configuração pré-estabelecida pelo administrador);
 - 5.4.18.2.2 Caso positivo de desinfecção:

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almojarifado

- 5.4.18.2.2.1 Restaurar o objeto para uso;
- 5.4.18.2.3 Caso negativo de desinfecção:
- 5.4.18.2.3.1 Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);
- 5.4.19 Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
- 5.4.20 Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;
- 5.4.21 Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;
- 5.4.22 Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa.

6 Servidores Linux

6.1 Compatibilidade:

Plataforma 32-bits:

- 6.1.1 Red Hat Enterprise Linux Server 5.x;
- 6.1.2 Red Hat® Enterprise Linux® Server 6.x (6.0 - 6.6);
- 6.1.3 CentOS 6.x (6.0 - 6.6);
- 6.1.4 SUSE® Linux Enterprise Server 11 SP3;
- 6.1.5 Ubuntu Server 12.04 LTS;
- 6.1.6 Ubuntu Server 14.04 LTS;
- 6.1.7 Ubuntu Server 14.10;
- 6.1.8 Oracle Linux 6.5;

Plataforma 64-bits:

- 6.1.9 Red Hat Enterprise Linux Server 5.x;
- 6.1.10 Red Hat Enterprise Linux Server 6.x (6.0 - 6.6);
- 6.1.11 Red Hat Enterprise Linux Server 7;
- 6.1.12 CentOS-6.x (6.0 - 6.6);
- 6.1.13 CentOS-7.0;
- 6.1.14 SUSE Linux Enterprise Server 11 SP3;
- 6.1.15 SUSE Linux Enterprise Server 12;
- 6.1.16 Novell Open Enterprise Server 11 SP1;
- 6.1.17 Novell Open Enterprise Server 11 SP2;
- 6.1.18 Ubuntu Server 12.04 LTS;
- 6.1.19 Ubuntu Server 14.04 LTS;
- 6.1.20 Ubuntu Server 14.10;
- 6.1.21 Oracle Linux 6.5;
- 6.1.22 Oracle Linux 7.0;

6.2 Características:

- 6.2.1 Deve prover as seguintes proteções:
 - 6.2.1.1 Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc.) que verifique qualquer arquivo criado, acessado ou modificado;
 - 6.2.1.2 As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almoxarifado

- 6.2.2 Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
 - 6.2.2.1 Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
- 6.2.3 Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
 - 6.2.3.1 Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;
 - 6.2.3.2 Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados;
- 6.2.4 Em caso erros, deve ter capacidade de criar *logs* automaticamente, sem necessidade de outros softwares;
- 6.2.5 Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
- 6.2.6 Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;
- 6.2.7 Capacidade de verificar objetos usando heurística;
- 6.2.8 Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).

6.3 Características:

- 6.3.1 Deve possuir proteção em tempo real para arquivos acessados, criados ou modificados;
- 6.3.2 Deve possuir verificação manual e agendada de acordo com a configuração do administrador;
- 6.3.3 Capacidade de realizar update de maneira automática, via internet ou LAN;
- 6.3.4 Capacidade de fazer um rollback das vacinas;
- 6.3.5 Capacidade de mover arquivos suspeitos ou infectados para área de quarentena;
- 6.3.6 Capacidade de criar logs detalhados e salvar resultados das verificações agendadas;
- 6.3.7 Capacidade de notificar o administrador de varreduras concluídas e sobre objetos maliciosos encontrados no servidor, utilizando e-mail.

7 Gerenciamento de Sistemas

- 7.1 Capacidade de registrar mudanças de hardware nas máquinas gerenciadas;
- 7.2 Capacidade de gerenciar um inventário de hardware, com a possibilidade de cadastro de dispositivos
- 7.3 Possibilita fazer distribuição de software de forma manual e agendada;
- 7.4 Suporta modo de instalação silenciosa;
- 7.5 Suporte a pacotes MSI, exe, bat, cmd e outros padrões de arquivos executáveis;
- 7.6 Possibilita fazer a distribuição através de agentes de atualização;
- 7.7 Utiliza tecnologia multicast para evitar tráfego na rede;
- 7.8 O licenciamento deve ser único tanto para servidores quanto para estações de trabalho
- 7.9 As licenças deverão ser perpétuas, ou seja, expirado a validade da mesma o produto deverá permanecer funcional para a proteção contra códigos maliciosos utilizando as definições até o momento da expiração do contrato.
- 7.10 A console de gerenciamento poderá ser instalada em um ambiente na nuvem (Azure, AWS, Google, etc.).
- 7.11 Capacidade de gerenciar dispositivos da nuvem e localmente.
- 7.12 Deve possuir uma console de gerenciamento via WEB

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almoxarifado

ITEM 3

**ESPECIFICAÇÕES TÉCNICAS PARA IMPLEMENTAÇÃO DA SOLUÇÃO DE ANTIVÍRUS
PARA OS COMPUTADORES E SERVIDORES**

1. O Centro Paula Souza proverá um ambiente de homologação adequado para o desenvolvimento do projeto, isolado de seu ambiente de produção;
2. O Centro Paula Souza proverá a infraestrutura adequada para implantação do piloto;
3. O Centro Paula Souza proverá documentação da infraestrutura detalhada para a perfeita validação do ambiente a ser implementado;
4. O Centro Paula Souza proverá acesso aos recursos de informática (Servidores, Estações, Storage, Azure e demais dispositivos) que atenderão ou farão parte deste projeto;
5. Centro Paula Souza disponibilizará toda a infraestrutura necessária;
6. O Centro Paula Souza entregará todos os servidores envolvidos com o sistema operacional implementado, devidamente configurado e com as atualizações aplicadas de acordo com solicitação da CONTRATADA;
7. A equipe técnica do Centro Paula Souza terá acompanhamento do projeto;
8. A console de gerenciamento deverá ser centralizada e configurada na Administração Central em servidores locais ou em nuvem.
9. Todas as máquinas da Administração Central deverão receber a solução de proteção.
10. A console de gerenciamento deverá ficar preparada para se conectar com todas as Unidades do CPS.
11. Durante os trabalhos deverá ser feita a transferência de conhecimento para um recurso do Centro Paula Souza, futuro responsável pela administração das soluções implantadas;
12. Fases do Projeto:
 - a. O projeto deverá ser conduzido em cinco (05) fases, detalhadas nos tópicos abaixo:
 - Iniciação: A contratada deverá criar a visão do projeto e definirá o escopo de trabalho necessário para trazê-la para a realidade;
 - Planejamento: Deverá consistir na elaboração dos processos detalhados a serem utilizados na implantação do projeto;
 - Execução: Consistirá na execução das atividades definidas na fase de planejamento, podendo ser dividida em sub-bases para melhor controle;
 - Estabilização: A solução deverá ser disponibilizada para os usuários do ambiente de produção, sendo efetuados os ajustes necessários para a estabilização da mesma;
 - Encerramento: Deverá ser entregue a documentação do projeto, e coletada a aprovação formal do cliente.
13. **MANUTENÇÃO E SUPORTE TÉCNICO**
 - As licenças de antivírus e servidores deverão possuir manutenção e suporte técnico pelo período de 12 (doze) meses
 - O Centro Paula Souza terá garantia de upgrade durante o período de 12 (doze) meses;
 - Suporte em português ou com serviço de tradução para todos os itens sem restrição de quantidade de chamados durante o período contratado;
 - O suporte técnico será acionado pelo Centro Paula Souza diretamente ao Fabricante em caso de qualquer indisponibilidade da solução;
 - O fabricante deverá disponibilizar 24x7x365 um recurso humano designado para fornecer assistência ao gerenciamento de todos os incidentes de suporte cadastrados junto ao mesmo;
 - Deverá ser fornecido um serviço a nível mundial de monitoramento proativo para ameaças de segurança que encaminhe notificações técnicas via e-mail;

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almoxarifado

- Deve possibilitar a abertura de chamados de suporte, para no mínimo, os seguintes métodos via telefone, e-mail, "website" do fabricante;
- Todos os prazos para atendimento da garantia começarão a ser contados a partir da abertura do chamado independentemente deste ter sido feito via telefone, e-mail, Website do fabricante;
- Dentro do prazo máximo de solução está compreendido o prazo de atendimento;
- Dentro do prazo máximo de atendimento, cabe ao Fabricante dar início, junto ao Contratante, às providências que serão adotadas para a solução do chamado;
- Durante o período de garantia o fornecedor executará, sem ônus adicionais, correções de falhas (bugs) de hardware e software;
- Durante o período de vigência do contrato o CONTRATANTE terá direito, sem ônus adicional, a todas as atualizações de versão e releases dos softwares e firmwares que fazem parte da solução ofertada

14. OBRIGAÇÕES DA CONTRATANTE

- Prover um ambiente de homologação adequado para o desenvolvimento do projeto, isolado de seu ambiente de produção;
- Fornecer a infraestrutura adequada para implantação do piloto e produção.
- Prover acesso aos recursos de informática (Servidores, Storage e demais dispositivos) que atenderão ou farão parte deste projeto;
- Disponibilizar acesso à internet;
- Espaço físico para a acomodação dos consultores;

15. DOS PRAZOS

- A Contratada deverá entregar as licenças no prazo máximo de 30 (trinta) dias a contar da data de assinatura do contrato administrativo;
- A implementação da solução será dívida em fases que será apresentada à Contratada somando 160 horas de atividade.

16. TREINAMENTO

Deverão ser treinados 6 servidores da equipe da Divisão de Informática:

- Cristina Mallia Reis
- Shirlei Mendes dos Santos
- Edilson da Nobrega
- Fernando Correia
- Marcos Vinicius Mota
- Edson Fumio Yamaguti

O treinamento deverá ser fornecido pela própria fabricante em suas dependências por um instrutor certificado. Com carga horária de 40 horas e certificação do fabricante.

Na impossibilidade de um dos servidores fazer parte do treinamento, será indicado um novo participante.

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almojarifado

17. ENTREGA

- A Contratada deverá enviar link para download do Software e orientações através do e-mail dos responsáveis da DI do CPS em uma única vez.
- As licenças de antivírus deverão possuir manutenção e suporte técnico pelo período de 12 (doze) meses.

18. DOS QUANTITATIVOS DO OBJETO

IT	ESPECIFICAÇÃO DO OBJETO	UND. MENS.	QUANT.
1	Suíte de Proteção para Endpoints, de acordo com as especificações técnicas descritas abaixo. Anexo I – Licença perpétua, manutenção 12 meses	Licenças	1.000
2	Suíte de Proteção para Endpoints, de acordo com as especificações técnicas descritas abaixo. Anexo I. “A” – Licença perpétua, manutenção 12 meses	Licenças	45.000
3	Horas de consultoria para implementação da Suíte de Proteção para Endpoints nas estações e servidores da Administração Central e Azure e preparação do ambiente para conectar as Unidades de Ensino	Horas	160
4	Treinamento para 6 participantes da Administração do Centro Paula Souza ministrado pelo Fabricante – 40 horas	Treinamento	6
5	Suporte 24x7 do Fabricante da Suíte de Proteção durante vigência do contrato	Meses	12

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almojarifado

ANEXO II
MODELO DE PLANILHA DE PROPOSTA

Ao
CENTRO ESTADUAL DE EDUCAÇÃO TECNOLÓGICA "PAULA SOUZA"
PREGÃO ELETRONICO N.º ___/___
PROCESSO N.º 6756/17 – CEETEPS

OBJETO: AQUISIÇÃO E ATUALIZAÇÃO DE USO DE SOFTWARE; APLICATIVOS: SUITE DE PROTEÇÃO DE ENDPOINTS, HORAS DE CONSULTORIA, TREINAMENTO E SUPORTE

LOTE 01					
IT	ESPECIFICAÇÃO DO OBJETO	UND. MENS.	QUANT.	PREÇO UNIT.	PREÇO TOTAL
1	Suíte de Proteção para Endpoints, de acordo com as especificações técnicas descritas abaixo. Anexo I – Licença perpétua, manutenção 12 meses	Licenças	1.000		
2	Suíte de Proteção para Endpoints, de acordo com as especificações técnicas descritas abaixo. Anexo I. "A" – Licença perpétua, manutenção 12 meses	Licenças	45.000		
3	Horas de consultoria para implementação da Suíte de Proteção para Endpoints nas estações e servidores da Administração Central e Azure e preparação do ambiente para conectar as Unidades de Ensino	Horas	160		
4	Treinamento para 6 participantes da Administração do Centro Paula Souza ministrado pelo Fabricante – 40 horas	Treinamento	6		
5	Suporte 24x7 do Fabricante da Suíte de Proteção durante vigência do contrato	Meses	12		
VALOR TOTAL DO LOTE				R\$	
CONDIÇÕES GERAIS DE FORNECIMENTO:					
COND. PAGAMENTO:	30 (trinta) dias , conforme cláusulas do edital.				
CONDIÇÕES DE ENTREGA:	Os bens deverão ser entregues conforme as condições estabelecidas no Edital.				
PRAZO VALIDADE PROPOSTA:	60 (sessenta) dias da abertura da proposta.				

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almojarifado

ANEXO III
MODELOS DE DECLARAÇÕES

ANEXO III.1

MODELO A QUE SE REFERE O ITEM 4.1.4.1. DO EDITAL
(em papel timbrado da licitante)

Nome completo: _____

RG nº: _____ CPF nº: _____

DECLARO, sob as penas da Lei, que o licitante _____ (*nome empresarial*), interessado em participar do Pregão Eletrônico nº ___/___, Processo nº **6756/17**:

a) está em situação regular perante o Ministério do Trabalho no que se refere a observância do disposto no inciso XXXIII do artigo 7.º da Constituição Federal, na forma do Decreto Estadual nº. 42.911/1998;

b) não possui impedimento legal para licitar ou contratar com a Administração.

(Local e data).

(Nome/assinatura do representante legal)

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almoxarifado

ANEXO III.2

**DECLARAÇÃO DE ELABORAÇÃO INDEPENDENTE DE PROPOSTA E ATUAÇÃO
CONFORME AO MARCO LEGAL ANTICORRUPÇÃO**

(em papel timbrado da licitante)

Eu, _____, portador do RG nº _____ e do CPF nº _____, representante legal do licitante _____ (*nome empresarial*), interessado em participar do Pregão Eletrônico nº ____/____, Processo nº ____/____, **DECLARO**, sob as penas da Lei, especialmente o artigo 299 do Código Penal Brasileiro, que:

a) a proposta apresentada foi elaborada de maneira independente e o seu conteúdo não foi, no todo ou em parte, direta ou indiretamente, informado ou discutido com qualquer outro licitante ou interessado, em potencial ou de fato, no presente procedimento licitatório;

b) a intenção de apresentar a proposta não foi informada ou discutida com qualquer outro licitante ou interessado, em potencial ou de fato, no presente procedimento licitatório;

c) o licitante não tentou, por qualquer meio ou por qualquer pessoa, influir na decisão de qualquer outro licitante ou interessado, em potencial ou de fato, no presente procedimento licitatório;

d) o conteúdo da proposta apresentada não será, no todo ou em parte, direta ou indiretamente, comunicado ou discutido com qualquer outro licitante ou interessado, em potencial ou de fato, no presente procedimento licitatório antes da adjudicação do objeto;

e) o conteúdo da proposta apresentada não foi, no todo ou em parte, informado, discutido ou recebido de qualquer integrante relacionado, direta ou indiretamente, ao órgão licitante antes da abertura oficial das propostas; e

f) o representante legal do licitante está plenamente ciente do teor e da extensão desta declaração e que detém plenos poderes e informações para firmá-la.

DECLARO, ainda, que a pessoa jurídica que represento conduz seus negócios de forma a coibir fraudes, corrupção e a prática de quaisquer outros atos lesivos à Administração Pública, nacional ou estrangeira, em atendimento à Lei Federal nº 12.846/ 2013 e ao Decreto Estadual nº 60.106/2014, tais como:

I – prometer, oferecer ou dar, direta ou indiretamente, vantagem indevida a agente público, ou a terceira pessoa a ele relacionada;

II – comprovadamente, financiar, custear, patrocinar ou de qualquer modo subvencionar a prática dos atos ilícitos previstos em Lei;

III – comprovadamente, utilizar-se de interposta pessoa física ou jurídica para ocultar ou dissimular seus reais interesses ou a identidade dos beneficiários dos atos praticados;

IV – no tocante a licitações e contratos:

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almoxarifado

- a) frustrar ou fraudar, mediante ajuste, combinação ou qualquer outro expediente, o caráter competitivo de procedimento licitatório público;
 - b) impedir, perturbar ou fraudar a realização de qualquer ato de procedimento licitatório público;
 - c) afastar ou procurar afastar licitante, por meio de fraude ou oferecimento de vantagem de qualquer tipo;
 - d) fraudar licitação pública ou contrato dela decorrente;
 - e) criar, de modo fraudulento ou irregular, pessoa jurídica para participar de licitação pública ou celebrar contrato administrativo;
 - f) obter vantagem ou benefício indevido, de modo fraudulento, de modificações ou prorrogações de contratos celebrados com a administração pública, sem autorização em lei, no ato convocatório da licitação pública ou nos respectivos instrumentos contratuais; ou
 - g) manipular ou fraudar o equilíbrio econômico-financeiro dos contratos celebrados com a administração pública;
- V – dificultar atividade de investigação ou fiscalização de órgãos, entidades ou agentes públicos, ou intervir em sua atuação, inclusive no âmbito das agências reguladoras e dos órgãos de fiscalização do sistema financeiro nacional.

(Local e data).

(Nome/assinatura do representante legal)

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almoxarifado

ANEXO III.3

**DECLARAÇÃO DE ENQUADRAMENTO COMO MICROEMPRESA OU EMPRESA DE
PEQUENO PORTE**

(em papel timbrado da licitante)

**ATENÇÃO: ESTA DECLARAÇÃO DEVE SER APRESENTADA APENAS POR
LICITANTES QUE SEJAM ME/EPP, NOS TERMOS DO ITEM 4.1.4.3. DO EDITAL.**

Eu, _____, portador do RG nº _____ e do CPF
nº _____, representante legal do licitante _____ (*nome
empresarial*), interessado em participar do Pregão Eletrônico nº ____/____, Processo nº **6756/17**,
DECLARO, sob as penas da Lei, o seu enquadramento na condição de Microempresa ou
Empresa de Pequeno Porte, nos critérios previstos no artigo 3º da Lei Complementar Federal
nº 123/2006, bem como sua não inclusão nas vedações previstas no mesmo diploma legal.

(Local e data).

(Nome/assinatura do representante legal)

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almojarifado

ANEXO III.4

**DECLARAÇÃO DE ENQUADRAMENTO COMO COOPERATIVA QUE PREENCHA AS
CONDIÇÕES ESTABELECIDAS NO ART. 34, DA LEI FEDERAL Nº 11.488/2007**
(em papel timbrado da licitante)

ATENÇÃO: ESTA DECLARAÇÃO DEVE SER APRESENTADA APENAS POR LICITANTES QUE SEJAM COOPERATIVAS, NOS TERMOS DO ITEM 4.1.4.4. DO EDITAL.

Eu, _____, portador do RG nº _____ e do CPF nº _____, representante legal do licitante _____ (*nome empresarial*), interessado em participar do Pregão Eletrônico nº ____/____, Processo nº **6756/17**, **DECLARO**, sob as penas da Lei, que:

- a) O Estatuto Social da cooperativa encontra-se adequado à Lei Federal nº 12.690/2012;
- b) A cooperativa auferiu Receita Bruta até o limite definido no inciso II do *caput* do art. 3º da Lei Complementar Federal nº 123/2006, a ser comprovado mediante Demonstração do Resultado do Exercício ou documento equivalente;

(Local e data).

(Nome/assinatura do representante legal)

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almojarifado

ANEXO IV
RESOLUÇÃO REFERENTE A PENALIDADES

RESOLUÇÃO SDECTI Nº 12, DE 28-3-2014.

Dispõe sobre a aplicação da penalidade de multa prevista nas Leis federais nº 8.666, de 21 de junho de 1993 e nº 10.520, de 17 de julho de 2002, e na Lei estadual nº 6.544, de 22 de novembro de 1989, no âmbito da Secretaria de Desenvolvimento Econômico, Ciência, Tecnologia e Inovação.

O SECRETÁRIO DE DESENVOLVIMENTO ECONÔMICO, CIÊNCIA, TECNOLOGIA E INOVAÇÃO, com fundamento no disposto no artigo 3º do Decreto nº 31.138, de 09 de janeiro de 1990, RESOLVE:

Art. 1º. Na aplicação das multas previstas nos artigos 79, 80 e 81, inciso II, da Lei Estadual nº 6.544, de 22, de novembro de 1989, nos artigos 86 e 87, inciso II, da Lei Federal nº 8.666, de 21, de junho de 1993, e no artigo 7º da Lei Federal nº 10.520, de 17, de julho de 2002, serão observadas as disposições desta Resolução.

Art. 2º. A recusa injustificada do adjudicatário em assinar o contrato, aceitar ou retirar o instrumento equivalente dentro do prazo estabelecido pela Administração, caracteriza o descumprimento total da obrigação assumida, sujeitando-o à aplicação de multa, na forma estabelecida no artigo 5º desta Resolução.

Art. 3º. O atraso injustificado na execução do objeto do contrato sujeitará o contratado à multa de mora, observado o seguinte:

I - em se tratando de compras ou de prestação de serviços não contínuos:

a) para atrasos de até 30 (trinta) dias: multa de 0,2% (dois décimos por cento) por dia de atraso, calculados sobre o valor global do contrato;

b) para atrasos superiores a 30 (trinta) dias: multa de 0,4% (quatro décimos por cento) por dia de atraso, calculados sobre o valor global do contrato;

II - em se tratando de execução de obras ou de serviços de engenharia:

a) para contratos com valor de até R\$ 100.000,00 (cem mil reais): multa de 0,2% (dois décimos por cento) por dia de atraso, calculados sobre o valor da parcela da obrigação contratual não cumprida;

b) para contratos com valor de R\$ 100.000,01 (cem mil reais e um centavo) até R\$ 500.000,00 (quinhentos mil reais): multa de 0,3% (três décimos por cento) por dia de atraso, calculados sobre o valor da obrigação contratual não cumprida; e

c) para contratos com valor de igual ou superior a R\$ 500.000,01 (quinhentos mil reais e um centavo): multa de 0,4% (quatro décimos por cento) por dia de atraso, calculados sobre o valor diário do contrato;

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almojarifado

III – em se tratando de serviços contínuos: multa de 30% (trinta por cento) por dia de inexecução, calculados sobre o valor diário do contrato.

§1º O valor das multas previstas neste artigo não poderá exceder a 25% (vinte e cinco por cento) do saldo financeiro ainda não realizado do contrato.

§2º A multa pelo atraso injustificado na execução do objeto do contrato será calculada a partir do primeiro dia útil seguinte àquele em que a obrigação avençada deveria ter sido cumprida.

Art. 4º. A inexecução parcial do contrato sujeitará o contratado à multa de mora, observado o seguinte:

I – em se tratando de compras ou de prestação de serviços não contínuos: multa de 10% (dez por cento) incidente sobre o valor da parcela não cumprida do contrato;

II – em se tratando de execução de obras ou serviços de engenharia ou de serviços contínuos:

a) para contratos com valor de até R\$ 100.000,00 (cem mil reais): multa de 30% (trinta por cento) incidente sobre o valor da parcela não cumprida do contrato;

b) para contratos com valor de R\$ 100.000,01 (cem mil reais e um centavo) até R\$ 500.000,00 (quinhentos mil reais): multa de 20% (vinte por cento) incidente sobre o valor da parcela não cumprida do contrato;

c) para contratos com valor igual ou superior a R\$ 500.000,01 (quinhentos mil reais e um centavo): multa de 10% (dez por cento) incidente sobre o valor da parcela não cumprida do contrato;

III– em se tratando de serviços contínuos: multa de 20% (vinte por cento) por dia de inexecução, calculados sobre o valor diário do contrato.

Art. 5º. A inexecução total do contrato sujeitará o contratado à multa de mora, observado o seguinte:

I – em se tratando de compras ou de prestação de serviços contínuos ou não: multa de 20% (vinte por cento) incidente sobre o valor global do contrato;

II – em se tratando de execução de obras ou serviços de engenharia ou de serviços contínuos:

a) para contratos com valor de até R\$ 100.000,00 (cem mil reais): multa de 20% (vinte por cento) incidente sobre o valor global do contrato;

b) para contratos com valor de R\$ 100.000,01 (cem mil reais e um centavo) até R\$ 500.000,00 (quinhentos mil reais): multa de 15% (quinze por cento) incidente sobre o valor global do contrato;

c) para contratos com valor igual ou superior a R\$ 500.000,01 (quinhentos mil reais e um centavo): multa de 10% (dez por cento) incidente sobre o valor global do contrato.

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almoxarifado

Art. 6º. Configurada a ocorrência de hipótese ensejadora de aplicação da penalidade de multa, o adjudicatário ou o contratado será notificado para, querendo, apresentar defesa prévia no prazo de 5 (cinco) dias úteis, contados do primeiro dia subsequente à data da sua notificação.

§1º Recebida a defesa, a autoridade competente deverá se manifestar motivadamente sobre o acolhimento ou rejeição das razões apresentadas, concluindo pela aplicação ou não da penalidade, dando ciência inequívoca ao adjudicatário ou contratado.

§2º A decisão que dispuser sobre a aplicação da multa será publicada no Diário Oficial do Estado e deverá conter o respectivo valor, o prazo para seu pagamento e a data a partir da qual o valor da multa sofrerá correção monetária.

§3º O adjudicatário ou o contratado será notificado da decisão, da qual caberá recurso a ser apresentado no prazo de 5 (cinco) dias úteis, contados da data do recebimento da notificação.

§4º A decisão do recurso será publicada no Diário Oficial do Estado, sem prejuízo da notificação do adjudicatário ou contratado.

Art. 7º. Ao término do regular processo administrativo, garantidos o contraditório e a ampla defesa, a multa aplicada será descontada da garantia do respectivo contratado.

§1º Se a multa aplicada for superior ao valor da garantia prestada, além da perda desta, o contratado responderá por sua complementação, mediante descontos nos pagamentos eventualmente devidos pela Administração até sua total quitação.

§2º Inexistindo pagamentos a serem realizados, o contratado recolherá o valor ao cofre público estadual, na forma prevista na legislação em vigor.

§3º Decorrido o prazo estabelecido sem o pagamento da multa aplicada serão adotadas as providências pertinentes voltadas à sua cobrança judicial.

Art. 8º. As multas de que trata esta Resolução serão aplicadas sem prejuízo da cominação das demais sanções administrativas previstas na Lei Federal nº 8.666, de 1993, na Lei Federal nº 10.520, de 2002 e na Lei Estadual 6.544, de 1989.

Art. 9º. Os editais de licitação deverão fazer menção expressa às normas estabelecidas nesta Resolução, cujo texto deverá integrar os respectivos editais e contratos, na forma de anexo.

Art. 10. As disposições desta Resolução aplicam-se também às contratações resultantes de procedimentos de dispensa ou de inexigibilidade de licitação.

Art. 11. Esta Resolução entrará em vigor na data da sua publicação, ficando revogada a Resolução SCTDE -1, de 22 de fevereiro de 1994.

(*) Republicada por ter saído, no DOE , de 29-03-2014, Seção I, páginas, 116 e 117, com incorreções no original.

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almoxarifado

ANEXO V
MINUTA DE CONTRATO

CONTRATO: Nº - ____/20__
PROCESSO Nº 6756/17

TERMO DE CONTRATO CELEBRADO ENTRE O CENTRO ESTADUAL DE EDUCAÇÃO TECNOLÓGICA "PAULA SOUZA" - CEETEPS, POR MEIO DO(A) _____ E TENDO POR OBJETO A AQUISIÇÃO E ATUALIZAÇÃO DE USO DE SOFTWARE; APLICATIVOS: SUITE DE PROTEÇÃO DE ENDPOINTS, HORAS DE CONSULTORIA, TREINAMENTO E SUPORTE, COM ENTREGA PARCELADA.

O CENTRO ESTADUAL DE EDUCAÇÃO TECNOLÓGICA "PAULA SOUZA", inscrita no CNPJ nº 62.823.257/0001-09, com sede a Rua dos Andradas, 140, Santa Ifigênia – São Paulo – SP, doravante designado(a) "CONTRATANTE", neste ato representada pela sua Diretora Superintendente, a Professora Laura M. J. Laganá, RG nº RG. 7.715.675-4 e CPF nº CPF. 005.923.818-62, no uso da competência conferida pelo Decreto-Lei Estadual nº 233, de 28 de abril de 1970, e _____, inscrita no CNPJ sob nº _____, com sede _____, a seguir denominada "CONTRATADA", neste ato representada pelo Senhor(a) _____, portador do RG nº _____ e CPF nº _____, em face da adjudicação efetuada no Pregão Eletrônico indicado em epígrafe, celebram o presente TERMO DE CONTRATO, sujeitando-se às disposições previstas na Lei Federal nº 10.520/2002, no Decreto Estadual nº 49.722/2005 e pelo regulamento anexo à Resolução CC-27, de 25 de maio de 2006, aplicando-se, subsidiariamente, no que couberem, as disposições da Lei Federal nº 8.666/1993, do Decreto Estadual nº 47.297/2002, do regulamento anexo à Resolução CEGP-10, de 19 de novembro de 2002, e demais normas regulamentares aplicáveis à espécie, mediante as seguintes cláusulas e condições que reciprocamente outorgam e aceitam:

CLÁUSULA PRIMEIRA - DO OBJETO

Constitui objeto do presente instrumento a **AQUISIÇÃO E ATUALIZAÇÃO DE USO DE SOFTWARE; APLICATIVOS: SUITE DE PROTEÇÃO DE ENDPOINTS, HORAS DE CONSULTORIA, TREINAMENTO E SUPORTE**, conforme detalhamento e especificações técnicas constantes do Termo de Referência, da proposta da CONTRATADA e demais documentos constantes do processo administrativo em epígrafe.

PARÁGRAFO ÚNICO

O objeto contratual executado deverá atingir o fim a que se destina, com eficácia e qualidade requeridas.

CLÁUSULA TERCEIRA – DO PRAZO DE EXECUÇÃO

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almojarifado

O objeto do presente contrato deverá ser realizado em 12 (doze) meses, contados da data estabelecida para o início dos serviços.

PARÁGRAFO PRIMEIRO

O prazo mencionado no caput poderá ser prorrogado nas hipóteses previstas no §1º do artigo 57, da Lei nº 8.666/1993, mediante termo de aditamento, atendido o estabelecido no §2º do referido dispositivo legal.

PARÁGRAFO SEGUNDO

Não obstante o prazo estipulado no caput, a vigência nos exercícios subsequentes ao da celebração do contrato estará sujeita à condição resolutiva, consubstanciada esta na inexistência de recursos aprovados nas respectivas Leis Orçamentárias de cada exercício para atender as respectivas despesas.

PARÁGRAFO TERCEIRO

Ocorrendo a resolução do contrato, com base na condição estipulada no Parágrafo Segundo desta Cláusula, a CONTRATADA não terá direito a qualquer espécie de indenização.

CLÁUSULA TERCEIRA - DAS OBRIGAÇÕES DA CONTRATADA

À CONTRATADA, além das obrigações constantes do Termo de Referência, que constitui Anexo I do Edital indicado no preâmbulo, e daquelas estabelecidas em lei, em especial as definidas nos diplomas federal e estadual sobre licitações, cabe:

I - zelar pela fiel execução deste contrato, utilizando-se de todos os recursos materiais e humanos necessários;

II - designar o responsável pelo acompanhamento da execução das atividades e pelos contatos com o CONTRATANTE;

III - responder pelos encargos trabalhistas, previdenciários, fiscais, comerciais e tributários, resultantes da execução deste contrato, nos termos do artigo 71 da Lei Federal nº 8.666/1993;

IV - manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação indicada no preâmbulo deste termo;

V - dar ciência imediata e por escrito ao CONTRATANTE de qualquer anormalidade que verificar na execução do contrato;

VI - prestar ao CONTRATANTE, por escrito, os esclarecimentos solicitados e atender prontamente as reclamações sobre a execução do contrato;

VII - responder por quaisquer danos, perdas ou prejuízos causados diretamente ao CONTRATANTE ou a terceiros decorrentes da execução do contrato;

VIII - manter seus empregados identificados por meio de crachás, com fotografia recente;

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almojarifado

IX - prestar a garantia técnica para o objeto deste contrato, nos termos do Termo de Referência.

IX - manter seus empregados identificados por meio de crachás, com fotografia recente;

X - substituir qualquer integrante de sua equipe cuja permanência no local de execução do contrato for julgada inconveniente, da solicitação justificada formulada pelo CONTRATANTE;

XI - prestar a garantia técnica para o objeto deste contrato, nos termos do Termo de Referência.

PARÁGRAFO PRIMEIRO

A CONTRATADA não poderá oferecer, dar ou se comprometer a dar a quem quer que seja, tampouco aceitar ou se comprometer a aceitar de quem quer que seja, por conta própria ou por intermédio de outrem, qualquer pagamento, doação, compensação, vantagens financeiras ou benefícios de qualquer espécie relacionados de forma direta ou indireta ao objeto deste contrato, o que deve ser observado, ainda, pelos seus prepostos, colaboradores e eventuais subcontratados, caso permitida a subcontratação.

PARÁGRAFO SEGUNDO

Em atendimento à Lei Federal nº 12.846/2013 e ao Decreto Estadual nº 60.106/2014, a CONTRATADA se compromete a conduzir os seus negócios de forma a coibir fraudes, corrupção e quaisquer outros atos lesivos à Administração Pública, nacional ou estrangeira, abstendo-se de práticas como as seguintes:

I – prometer, oferecer ou dar, direta ou indiretamente, vantagem indevida a agente público, ou a terceira pessoa a ele relacionada;

II – comprovadamente, financiar, custear, patrocinar ou de qualquer modo subvencionar a prática dos atos ilícitos previstos em Lei;

III – comprovadamente, utilizar-se de interposta pessoa física ou jurídica para ocultar ou dissimular seus reais interesses ou a identidade dos beneficiários dos atos praticados;

IV – no tocante a licitações e contratos:

a) frustrar ou fraudar, mediante ajuste, combinação ou qualquer outro expediente, o caráter competitivo de procedimento licitatório público;

b) impedir, perturbar ou fraudar a realização de qualquer ato de procedimento licitatório público;

c) afastar ou procurar afastar licitante, por meio de fraude ou oferecimento de vantagem de qualquer tipo;

d) fraudar licitação pública ou contrato dela decorrente;

e) criar, de modo fraudulento ou irregular, pessoa jurídica para participar de licitação pública ou celebrar contrato administrativo;

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almoxarifado

f) obter vantagem ou benefício indevido, de modo fraudulento, de modificações ou prorrogações de contratos celebrados com a administração pública, sem autorização em lei, no ato convocatório da licitação pública ou nos respectivos instrumentos contratuais; ou

g) manipular ou fraudar o equilíbrio econômico-financeiro dos contratos celebrados com a administração pública;

V – dificultar atividade de investigação ou fiscalização de órgãos, entidades ou agentes públicos, ou intervir em sua atuação, inclusive no âmbito das agências reguladoras e dos órgãos de fiscalização do sistema financeiro nacional.

PARÁGRAFO TERCEIRO

O descumprimento das obrigações previstas nos Parágrafos Primeiro e Segundo desta Cláusula Terceira poderá submeter a CONTRATADA à rescisão unilateral do contrato, a critério da CONTRATANTE, sem prejuízo da aplicação das sanções penais e administrativas cabíveis e, também, da instauração do processo administrativo de responsabilização de que tratam a Lei Federal nº 12.846/2013 e o Decreto Estadual nº 60.106/2014.

CLÁUSULA QUARTA - DAS OBRIGAÇÕES E DAS RESPONSABILIDADES DA CONTRATADA

À CONTRATADA, além das obrigações constantes do Termo de Referência, que constitui **ANEXO I** do Edital indicado no preâmbulo, e daquelas estabelecidas em lei, em especial as definidas nos diplomas federal e estadual sobre licitações, cabe:

I - zelar pela fiel execução deste contrato, utilizando-se de todos os recursos materiais e humanos necessários;

II – designar o responsável pelo acompanhamento da execução das atividades, em especial da regularidade técnica e disciplinar da atuação da equipe técnica alocada, e pelos contatos com o CONTRATANTE;

III - cumprir as disposições legais e regulamentares municipais, estaduais e federais que interfiram na execução dos serviços;

IV - manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação indicada no preâmbulo deste termo;

V - dar ciência imediata e por escrito ao CONTRATANTE de qualquer anormalidade que verificar na execução dos serviços;

VI - prestar ao CONTRATANTE, por escrito, os esclarecimentos solicitados e atender prontamente as reclamações sobre seus serviços;

VII - responder por quaisquer danos, perdas ou prejuízos causados diretamente ao CONTRATANTE ou a terceiros decorrentes da execução do contrato, não excluindo ou reduzindo essa responsabilidade a fiscalização do CONTRATANTE em seu acompanhamento;

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almoxarifado

VIII - responder pelos encargos trabalhistas, previdenciários, fiscais, comerciais e tributários, resultantes da execução deste contrato, nos termos do artigo 71 da Lei Federal nº 8.666/1993;

IX - manter seus profissionais identificados por meio de crachá com fotografia recente;

X - substituir qualquer integrante de sua equipe cuja permanência nos serviços for julgada inconveniente, no prazo máximo de 05 (cinco) dias úteis, contado da solicitação justificada formulada pelo CONTRATANTE;

XI - arcar com despesas decorrentes de infrações de qualquer natureza praticadas por seus empregados durante a execução dos serviços, ainda que no recinto da sede do CONTRATANTE;

XII - apresentar, quando exigido pelo CONTRATANTE, os comprovantes de pagamentos de salários, apólices de seguro contra acidente de trabalho, quitação de suas obrigações trabalhistas e previdenciárias, relativas aos seus empregados, que prestam ou tenham prestado serviços objeto do presente contrato;

XIII - identificar todos os equipamentos e materiais de sua propriedade, de forma a não serem confundidos com similares de propriedade do CONTRATANTE;

XIV - obedecer às normas e rotinas do CONTRATANTE, em especial as que disserem respeito à segurança, à guarda, à manutenção e à integridade das informações existentes ou geradas durante a execução dos serviços;

XV - implantar, de forma adequada, a planificação, execução e supervisão permanente dos serviços, de maneira a não interferir nas atividades do CONTRATANTE, respeitando suas normas de conduta;

XVI - reexecutar os serviços sempre que solicitado pelo CONTRATANTE, quando estiverem em desacordo com as técnicas e procedimentos aplicáveis;

XVII - guardar sigilo em relação às informações ou documentos de qualquer natureza de que venha a tomar conhecimento, respondendo, administrativa, civil e criminalmente por sua indevida divulgação e incorreta ou inadequada utilização;

XVIII - manter bens e equipamentos necessários à realização dos serviços, de qualidade comprovada, em perfeitas condições de uso, em quantidade adequada à boa execução dos trabalhos, cuidando para que os equipamentos elétricos sejam dotados de sistema de proteção, de modo a evitar danos na rede elétrica;

XIX - submeter à CONTRATANTE relatório mensal sobre a prestação dos serviços, relatando todos os serviços realizados, eventuais problemas verificados e qualquer fato relevante sobre a execução do objeto contratual;

XX - fornecer à equipe alocada para a execução dos serviços os equipamentos de proteção individual adequados à atividade, o necessário treinamento e fiscalizar sua efetiva utilização;

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almoxarifado

XXI - prestar os serviços por intermédio da equipe indicada nos documentos apresentados na fase de habilitação, a título de qualificação técnica, quando exigida.

PARÁGRAFO PRIMEIRO

A CONTRATADA não poderá oferecer, dar ou se comprometer a dar a quem quer que seja, tampouco aceitar ou se comprometer a aceitar de quem quer que seja, por conta própria ou por intermédio de outrem, qualquer pagamento, doação, compensação, vantagens financeiras ou benefícios de qualquer espécie relacionados de forma direta ou indireta ao objeto deste contrato, o que deve ser observado, ainda, pelos seus prepostos, colaboradores e eventuais subcontratados, caso permitida a subcontratação.

PARÁGRAFO SEGUNDO

Em atendimento à Lei Federal nº 12.846/2013 e ao Decreto Estadual nº 60.106/2014, a CONTRATADA se compromete a conduzir os seus negócios de forma a coibir fraudes, corrupção e quaisquer outros atos lesivos à Administração Pública, nacional ou estrangeira, abstendo-se de práticas como as seguintes:

- I – prometer, oferecer ou dar, direta ou indiretamente, vantagem indevida a agente público, ou a terceira pessoa a ele relacionada;
- II – comprovadamente, financiar, custear, patrocinar ou de qualquer modo subvencionar a prática dos atos ilícitos previstos em Lei;
- III – comprovadamente, utilizar-se de interposta pessoa física ou jurídica para ocultar ou dissimular seus reais interesses ou a identidade dos beneficiários dos atos praticados;
- IV – no tocante a licitações e contratos:
 - a) frustrar ou fraudar, mediante ajuste, combinação ou qualquer outro expediente, o caráter competitivo de procedimento licitatório público;
 - b) impedir, perturbar ou fraudar a realização de qualquer ato de procedimento licitatório público;
 - c) afastar ou procurar afastar licitante, por meio de fraude ou oferecimento de vantagem de qualquer tipo;
 - d) fraudar licitação pública ou contrato dela decorrente;
 - e) criar, de modo fraudulento ou irregular, pessoa jurídica para participar de licitação pública ou celebrar contrato administrativo;
 - f) obter vantagem ou benefício indevido, de modo fraudulento, de modificações ou prorrogações de contratos celebrados com a administração pública, sem autorização em lei, no ato convocatório da licitação pública ou nos respectivos instrumentos contratuais; ou

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almoxarifado

g) manipular ou fraudar o equilíbrio econômico-financeiro dos contratos celebrados com a administração pública;

V – dificultar atividade de investigação ou fiscalização de órgãos, entidades ou agentes públicos, ou intervir em sua atuação, inclusive no âmbito das agências reguladoras e dos órgãos de fiscalização do sistema financeiro nacional.

PARÁGRAFO TERCEIRO

O descumprimento das obrigações previstas nos Parágrafos Primeiro e Segundo desta Cláusula Terceira poderá submeter a CONTRATADA à rescisão unilateral do contrato, a critério da CONTRATANTE, sem prejuízo da aplicação das sanções penais e administrativas cabíveis e, também, da instauração do processo administrativo de responsabilização de que tratam a Lei Federal nº 12.846/2013 e o Decreto Estadual nº 60.106/2014.

CLÁUSULA QUINTA - DAS OBRIGAÇÕES DO CONTRATANTE

Ao CONTRATANTE cabe:

I - exercer a fiscalização dos serviços, designando servidor responsável pelo acompanhamento da execução contratual e, ainda, pelos contatos com a CONTRATADA;

II - fornecer à CONTRATADA todos os dados e informações necessários à execução do objeto do contrato;

III - efetuar os pagamentos devidos, de acordo com o estabelecido neste ajuste;

IV - expedir autorização de serviços, com antecedência mínima de 03 (três) dias úteis da data de início de sua execução.

V- permitir aos técnicos e profissionais da CONTRATADA acesso às áreas físicas envolvidas na execução deste contrato, observadas as normas de segurança;

CLÁUSULA SEXTA - DA FISCALIZAÇÃO DO CONTRATO

O CONTRATANTE exercerá a fiscalização dos serviços contratados por intermédio do gestor do contrato de modo a assegurar o efetivo cumprimento das obrigações ajustadas.

PARÁGRAFO PRIMEIRO

A fiscalização não exclui e nem reduz a integral responsabilidade da CONTRATADA, mesmo perante terceiros, por quaisquer irregularidades constatadas na execução do objeto contratado, inexistindo, em qualquer hipótese, corresponsabilidade por parte do CONTRATANTE.

PARAGRAFO SEGUNDO

A ausência de comunicação, por parte do CONTRATANTE, referente a irregularidades ou falhas, não exime a CONTRATADA do regular cumprimento das obrigações previstas neste contrato e no **ANEXO I** do Edital.

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almoxarifado

CLÁUSULA NONA – DO RECEBIMENTO DO OBJETO

O objeto deste contrato, em cada uma de suas parcelas mensais, será recebido provisoriamente em até 05 (cinco) dias úteis, contados da data de recepção pela Administração do relatório de execução dos serviços do mês acompanhado da nota fiscal/fatura representativa da prestação dos serviços.

PARÁGRAFO PRIMEIRO

Havendo rejeição dos serviços, no todo ou em parte, a CONTRATADA deverá refazê-los no prazo estabelecido pelo CONTRATANTE, observando as condições estabelecidas para a prestação.

PARÁGRAFO SEGUNDO

Na impossibilidade de serem refeitos os serviços rejeitados, ou na hipótese de não serem os mesmos executados, o valor respectivo será descontado da importância mensal devida à CONTRATADA, sem prejuízo da aplicação das sanções cabíveis.

PARÁGRAFO TERCEIRO

O recebimento do objeto dar-se-á definitivamente no prazo de 05 (cinco) dias úteis, após o recebimento provisório, ou da data de conclusão das correções efetuadas com base no disposto no Parágrafo Primeiro desta Cláusula, uma vez verificada a execução satisfatória dos serviços, mediante Termo de Recebimento Definitivo ou Recibo, firmado pelo servidor responsável.

CLÁUSULA SÉTIMA – DO PREÇOS

A CONTRATADA obriga-se a fornecer o objeto deste contrato pelo preço total de R\$ _____ (_____), **mediante os seguintes valores unitários:**

IT	ESPECIFICAÇÃO DO OBJETO	UND. MENS.	QUANT.	PREÇO UNIT.	PREÇO TOTAL
1	Suíte de Proteção para Endpoints, de acordo com as especificações técnicas descritas abaixo. Anexo I – Licença perpétua, manutenção 12 meses	Licenças	1.000		
2	Suíte de Proteção para Endpoints, de acordo com as especificações técnicas descritas abaixo. Anexo I. “A” – Licença perpétua, manutenção 12 meses	Licenças	45.000		
3	Horas de consultoria para implementação da Suíte de Proteção para Endpoints nas estações e servidores da Administração Central e Azure e preparação do ambiente para	Horas	160		

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almoxarifado

	conectar as Unidades de Ensino				
4	Treinamento para 6 participantes da Administração do Centro Paula Souza ministrado pelo Fabricante – 40 horas	Treinamento	6		
5	Suporte 24x7 do Fabricante da Suíte de Proteção durante vigência do contrato	Meses	12		
VALOR TOTAL				R\$	

PARÁGRAFO PRIMEIRO

Nos preços acima estão incluídos, além do lucro, todas as despesas e custos diretos e indiretos relacionados ao fornecimento, tais como tributos, remunerações, despesas financeiras e quaisquer outras necessárias ao cumprimento do objeto desta licitação, inclusive gastos com transporte.

PARÁGRAFO SEGUNDO

Caso a CONTRATADA seja optante pelo Simples Nacional e, por causa superveniente à contratação, perca as condições de enquadramento como microempresa ou empresa de pequeno porte ou, ainda, torne-se impedida de beneficiar-se desse regime tributário diferenciado por incorrer em alguma das vedações previstas na Lei Complementar Federal nº 123/2006, não poderá deixar de cumprir as obrigações avençadas perante a Administração, tampouco requerer o reequilíbrio econômico-financeiro, com base na alegação de que a sua proposta levou em consideração as vantagens daquele regime tributário diferenciado.

PARAGRAFO TERCEIRO

Os preços contratados permanecerão fixos e irrevogáveis.

CLAUSULA OITAVA – DOS RECURSOS ORÇAMENTÁRIOS

No presente exercício as despesas decorrentes desta contratação irão onerar o crédito orçamentário desta Autarquia, UGE **102401**, PROGRAMA DE TRABALHO: **12 363 1039 5292 000**, FONTE DE RECURSO: **001 001 001**, NATUREZA DE DESPESA: **33 90 88 07**.

CLÁUSULA NONA - DOS PAGAMENTOS

Os pagamentos serão efetuados em 30 (trinta) dias, contados da apresentação de cada nota fiscal/fatura no protocolo da CONTRATANTE, à vista do respectivo “Termo de Recebimento Definitivo” ou “Recibo”, em conformidade com a Cláusula Sexta deste instrumento.

PARAGRAFO SEGUNDO

Constitui condição para a realização dos pagamentos a inexistência de registros em nome da contratada no “Cadastro Informativo dos Créditos não Quitados de Órgãos e Entidades Estaduais – CADIN ESTADUAL”, o qual deverá ser consultado por ocasião da realização de cada pagamento. O cumprimento desta condição poderá se dar pela comprovação, pela

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almojarifado

contratada, de que os registros estão suspensos, nos termos do artigo 8º da Lei Estadual nº 12.799/2008.

PARAGRAFO TERCEIRO

Os pagamentos serão feitos mediante crédito aberto em conta corrente em nome da contratada no Banco do Brasil S/A.

PARAGRAFO QUARTO

Havendo atraso nos pagamentos, incidirá correção monetária sobre o valor devido na forma da legislação aplicável, bem como juros moratórios, a razão de 0,5% (meio por cento) ao mês, calculados “pró-rata tempore”, em relação ao atraso verificado.

PARAGRAFO QUINTO

A(s) Nota(s) Fiscal/fatura deverá ser emitida em nome do CENTRO ESTADUAL DE EDUCAÇÃO TECNOLÓGICA "PAULA SOUZA" – RUA DOS ANDRADAS, 140 – SANTA IFIGENIA - CEP. 01208-000 – SÃO PAULO/SP - CNPJ Nº 62.823.257/0001-09, INSCRIÇÃO ESTADUAL ISENTA, encaminhada à cada unidade recebedora, de que obrigatoriamente deverá constar:

- nº do contrato;**
- nº nota de empenho;**
- nº do processo; e**
- identificação da Unidade.**

CLÁUSULA DÉCIMA – DA ALTERAÇÃO DA QUANTIDADE DO OBJETO CONTRATADO

A CONTRATADA fica obrigada a aceitar, nas mesmas condições contratadas, os acréscimos ou supressões que se fizerem necessários no objeto, a critério exclusivo do CONTRATANTE, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

PARÁGRAFO ÚNICO

Eventual alteração será obrigatoriamente formalizada pela celebração de prévio termo aditivo ao presente instrumento, respeitadas as disposições da Lei Federal nº 8.666/1993.

CLÁUSULA DÉCIMA PRIMEIRA – DA RESCISÃO

O contrato poderá ser rescindido, na forma, com as consequências e pelos motivos previstos nos artigos 77 a 80 e 86 a 88, da Lei Federal nº 8.666/1993.

PARÁGRAFO ÚNICO

A CONTRATADA reconhece desde já os direitos do CONTRATANTE nos casos de rescisão administrativa, prevista no artigo 79 da Lei Federal nº 8.666/1993.

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almojarifado

CLÁUSULA DÉCIMA SEGUNDA - DAS SANÇÕES PARA O CASO DE INADIMPLEMENTO

A CONTRATADA ficará impedida de licitar e contratar com a Administração direta e indireta do Estado de São Paulo, pelo prazo de até 05 (cinco) anos, se vier a praticar quaisquer atos previstos no artigo 7º da Lei Federal nº 10.520, de 17 de julho de 2002, sem prejuízo da responsabilidade civil ou criminal, quando couber.

PARÁGRAFO PRIMEIRO

A sanção de que trata o *caput* desta Cláusula poderá ser aplicada juntamente com as multas previstas no **ANEXO IV** do Edital indicado no preâmbulo deste instrumento, garantido o exercício de prévia e ampla defesa, e deverá ser registrada no CAUFESP, no “Sistema Eletrônico de Aplicação e Registro de Sanções Administrativas – e-Sanções”, no endereço www.esancoes.sp.gov.br, e também no “Cadastro Nacional de Empresas Inidôneas e Suspensas – CEIS”, no endereço <http://www.portaltransparencia.gov.br/ceis>.

PARÁGRAFO SEGUNDO

As sanções são autônomas e a aplicação de uma não exclui a de outra.

PARÁGRAFO TERCEIRO

O CONTRATANTE reserva-se no direito de descontar das faturas os valores correspondentes às multas que eventualmente forem aplicadas por descumprimento de cláusulas contratuais, ou, quando for o caso, efetuará a cobrança judicialmente.

PARÁGRAFO QUARTO

A prática de atos que atentem contra o patrimônio público nacional ou estrangeiro, contra princípios da administração pública, ou que de qualquer forma venham a constituir fraude ou corrupção, durante a licitação ou ao longo da execução do contrato, será objeto de instauração de processo administrativo de responsabilização nos termos da Lei Federal nº 12.846/ 2013 e do Decreto Estadual nº 60.106/2014, sem prejuízo da aplicação das sanções administrativas previstas nos artigos 87 e 88 da Lei Federal nº 8.666/1993, e no artigo 7º da Lei Federal nº 10.520/2002.

CLÁUSULA DÉCIMA TERCEIRA - DA GARANTIA DE EXECUÇÃO CONTRATUAL

Não será exigida a apresentação de garantia para a contratação que constitui objeto do presente instrumento.

CLÁUSULA DÉCIMA QUARTA - DISPOSIÇÕES FINAIS

Fica ajustado, ainda, que:

- a) o Edital mencionado no preâmbulo e seus anexos.
- b) a proposta apresentada pela CONTRATADA;

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almojarifado

II. Aplicam-se às omissões deste contrato as disposições normativas indicadas no preâmbulo deste Termo de Contrato e demais disposições regulamentares pertinentes.

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

E assim, por estarem as partes justas e contratadas, foi lavrado o presente instrumento **02 (duas) vias** de igual teor e forma que, lido e achado conforme pela CONTRATADA e pela CONTRATANTE, vai por elas assinado para que produza todos os efeitos de Direito, na presença das testemunhas abaixo identificadas.

São Paulo, ____ de _____ de 2018.

CONTRATANTE

CONTRATADA

TESTEMUNHAS:

Nome:

RG:

Nome:

RG:



Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almoxarifado

ANEXO A
TERMO DE REFERÊNCIA

[...]

Administração Central
Departamento de Material e Patrimônio
Divisão de Compras e Almojarifado

ANEXO B
TERMO DE CIÊNCIA E DE NOTIFICAÇÃO

CONTRATANTE: **CEETEPS - CENTRO ESTADUAL DE EDUCAÇÃO TECNOLÓGICA
"PAULA SOUZA"**

CONTRATADA:

CONTRATO: Nº ____/20__

OBJETO: **AQUISIÇÃO E ATUALIZAÇÃO DE USO DE SOFTWARE; APLICATIVOS:
SUITE DE PROTEÇÃO DE ENDPOINTS, HORAS DE CONSULTORIA,
TREINAMENTO E SUPORTE**

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

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

São Paulo, __ de _____ de 20__.

CONTRATANTE

NOME: _____

CARGO: _____

EMAIL _____

INSTITUCIONAL: _____

EMAIL PESSOAL: _____

ASSINATURA

CONTRADADA

NOME: _____

CARGO: _____

EMAIL _____

INSTITUCIONAL: _____

EMAIL PESSOAL: _____

ASSINATURA