FUNDAÇÃO CASA
CENTRO DE ATENDIMENTO
SOCIOEDUCATIVO AO ADOLESCENTE

PROCESSO SDE n.° 0404/2019
PREGÃO ELETRÔNICO SDE n.° 044/2019
CONTRATO SCO n.° 019/2019

TERMO DE CONTRATO CELEBRADO ENTRE A FUNDAÇÃO CASA E A EMPRESA BRASOFTWARE INFORMÁTICA LTDA, TENDO POR OBJETO A AQUISIÇÃO DE RENOVAÇÃO DA SOLUÇÃO ANTIVÍRUS KASPERSKY END-POINT SECURITY FOR BUSINESS ADVANCED.

I - CONTRATANTE: **FUNDAÇÃO CENTRO DE ATENDIMENTO SOCIOEDUCATIVO AO ADOLESCENTE - FUNDAÇÃO CASA-SP**, instituída pela Lei n.º 185, de 12 de dezembro de 1973, com respectivas alterações, inscrita no Cadastro Nacional da Pessoa Jurídica do Ministério da Fazenda sob o n.º 44.480.283/0001-91, sediada na Rua Florêncio de Abreu, n.º 848 – Luz - São Paulo - Capital, neste ato representada pelo senhor Paulo Dimas Debellis Mascaretti, Secretário da Justiça e Cidadania, respondendo pelo expediente da Fundação CASA, nos termos do Decreto de 02-01-2019, publicado no DOE de 03-01-2019 e por seu Diretor Administrativo Interino Aurélio Olímpio de Souza, nomeado nos termos da Portaria Administrativa n.º 948/2018, doravante denominada simplesmente **CONTRATANTE**.

II - CONTRATADA: **BRASOFTWARE INFORMÁTICA LTDA**, pessoa jurídica de direito privado, inscrita no Cadastro Nacional de Pessoa Jurídica do Ministério da Fazenda sob o n.º 57.142.978/0001-05, localizada na Rua Marina La Regina, n.º 227, 3º andar, salas 11 a 15, Centro, Poá - SP, CEP 08550-210, neste ato representada por sua procuradora Sra. **Viviani Hupp de Oliveira**, portadora da Cédula de Identidade n.º 29.899.950-X SSP/SP e inscrita no CPF/MF sob o n.º 169.328.378-62, conforme consta do Instrumento Particular de Procuração, doravante denominada simplesmente **CONTRATADA**.

PREÂMBULO

Pelo presente instrumento e na melhor forma de direito, as partes acima mencionadas e qualificadas têm entre si justo e acertado o presente Termo de Contrato, objetivando a renovação da solução antivírus Kaspersky End-Point Security for Business Advanced, no qual se submetem as partes às cláusulas e condições adiante estipuladas, que reciprocamente se outorgam e aceitam e que darão integral cumprimento, por si, seus herdeiros ou sucessores, a qualquer título.

A lavratura do presente contrato decorre de licitação promovida na modalidade PREGÃO, em sua forma ELETRÔNICA, de n.º SDE 044/2019, advinda da CI nº. 003/2019 - DTI, que deu origem ao Processo SDE n.º 0404/2019, realizada com arrimo nas disposições contidas na Lei federal nº. 10.520, de 17 de julho de 2002, Decreto estadual nº 49.722, de 24 de junho de 2005 e Resolução da Casa Civil n.º 27, de 25 de maio de 2006, aplicando-se subsidiariamente, o Decreto estadual n.º 47.297, de 06 de novembro de 2002 e a Portaria Normativa n.º 063, de 06 de agosto de 2003, sujeitando-se, as partes contratantes às normas estabelecidas na Lei federal n.º 8.666 de 21 de junho de 1993 e na Lei estadual n.º 6.544, de 22 de novembro de 1989, com alterações respectivas, bem como, pelas demais normas legais e regulamentares vigentes aplicáveis à matéria, e as cláusulas contratuais que reciprocamente se outorgam e aceitam:

CLÁUSULA PRIMEIRA - DO OBJETO

Constitui objeto do presente instrumento a renovação da solução antivírus Kaspersky End-Point Security for Business Advanced conforme detalhamento e especificações técnicas constantes do Memorial Descritivo, da proposta da CONTRATADA e demais documentos constantes do processo administrativo em epígrafe.

CLÁUSULA SEGUNDA – DOS PRAZOS, LOCAIS E CONDIÇÕES DE ENTREGA

O contrato deverá ser executado fielmente pelas partes de acordo com as cláusulas contratuais aqui avençadas e ainda pelos preceitos legais de direito público, aplicando-lhes, supletivamente, os princípios da Teoria Geral dos Contratos e as disposições de direito privado, na forma do art. 54, da Lei federal n.º 8.666/93 c.c. XII, do mesmo diploma legal.

PARÁGRAFO PRIMEIRO

A renovação das licenças deverá ser efetuada no prazo de até 30 (trinta) dias corridos, contados do recebimento, por parte da CONTRATADA, da Ordem de Fornecimento. Os serviços de instalação, configuração e treinamento do software deverão ser iniciados após a entrega das renovações das licenças, mediante Ordem de Início expedida pela Contratante.

I - Juntamente com a entrega dos bens, deverá ser apresentado a documentação do Plano Técnico do Projeto e a Implementação do mesmo.

PARÁGRAFO SEGUNDO

A entrega do objeto deste contrato, bem com a instalação e configuração completa da renovação das licenças da solução deverá ser feita na Divisão de Tecnologia da Informação – DTI da CONTRATANTE, situada a Rua Florêncio de Abreu n.º 848 – 5º andar - Luz - São Paulo - SP – CEP 01030-001 - Telefone (11) 2927-9255.

PARÁGRAFO TERCEIRO

Correrão por conta da CONTRATADA todas as despesas diretas ou indiretas relacionadas ao objeto, tais como embalagens, seguros, transportes, tributos, encargos trabalhistas e previdenciários, decorrentes do fornecimento.

PARÁGRAFO QUARTO

A CONTRATADA deverá observar, para a entrega dos bens, todas as condições estabelecidas no Memorial Descritivo – **Anexo I** ao presente instrumento, com a regular apresentação dos documentos ali elencados.

CLÁUSULA TERCEIRA - DAS OBRIGAÇÕES E DAS RESPONSABILIDADES DA CONTRATADA

À CONTRATADA, além das obrigações constantes do Memorial Descritivo, 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 n° 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;

IX - prestar a garantia técnica para o objeto deste contrato, nos termos do Memorial Descritivo.

X - não divulgar dados ou informações a que venha a ter acesso, salvo expressamente autorizados pelo CONTRATANTE.

XI - Se a contratada for cooperativa, deverá indicar, por ocasião da celebração do contrato, o nome do gestor encarregado de representá-la com exclusividade perante o contratante.

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

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 DO CONTRATANTE

Ao CONTRATANTE cabe:

I - indicar formalmente o servidor responsável pelo acompanhamento e fiscalização da execução do ajuste 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 - permitir aos técnicos e profissionais da CONTRATADA acesso às áreas físicas envolvidas na execução deste contrato, observadas as normas de segurança.

CLÁUSULA QUINTA - DA FISCALIZAÇÃO DO CONTRATO

O CONTRATANTE exercerá a fiscalização contratual 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.

PARÁGRAFO 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.

CLÁUSULA SEXTA – DAS CONDIÇÕES DE RECEBIMENTO DO OBJETO

O objeto da presente licitação poderá ser recebido provisoriamente em até 05 (cinco) dias úteis, contados da data da entrega dos bens, acompanhado da respectiva nota fiscal/fatura.

PARÁGRAFO PRIMEIRO

Por ocasião da entrega, a CONTRATADA deverá colher no comprovante respectivo a data, o nome, o cargo, a assinatura e o número do Registro Geral (RG), emitido pela Secretaria de Segurança Pública, ou documento equivalente, do servidor do CONTRATANTE responsável pelo recebimento.

PARÁGRAFO SEGUNDO

Constatadas irregularidades no objeto contratual, o CONTRATANTE poderá:

I. Se disser respeito à especificação, rejeitá-lo no todo ou em parte, determinando sua substituição ou rescindindo a contratação, sem prejuízo das penalidades cabíveis. Na hipótese de substituição, a CONTRATADA deverá fazê-la em conformidade com a indicação do CONTRATANTE, no prazo máximo de 05 (cinco) dias úteis, contados da notificação por escrito, mantido o preço inicialmente contratado;

II. Se disser respeito à diferença de quantidade ou de partes, determinar sua complementação ou rescindir a contratação, sem prejuízo das penalidades cabíveis. Na hipótese de complementação, a CONTRATADA deverá fazê-la em conformidade com a indicação do CONTRATANTE, no prazo máximo de 05 (cinco) dias úteis, contados da notificação por escrito, mantido o preço inicialmente contratado.

PARÁGRAFO TERCEIRO
O recebimento do objeto dar-se-á definitivamente no prazo de 05 (cinco) dias úteis dias úteis após o recebimento provisório, uma vez verificado o atendimento integral da quantidade e das especificações contratadas, mediante "Termo de Recebimento Definitivo" ou "Recibo", firmado pelo servidor responsável.

CLÁUSULA SÉTIMA - DOS PREÇOS

A CONTRATADA obriga-se a fornecer o objeto deste contrato mediante o preço unitário de R$ 68,14 (sessenta e oito reais e quatorze centavos) para o item 01 e R$ 231.370,00 (duzentos e trinta e um mil, trezentos e setenta reais) para o item 02, perfazendo o total de **R$ 538.000,00 (quinhentos e trinta e oito mil reais)**.

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.

PARÁGRAFO TERCEIRO
Os preços contratados permanecerão fixos e irreajustáveis.

CLÁUSULA OITAVA – DOS RECURSOS ORÇAMENTÁRIOS

No presente exercício as despesas decorrentes desta contratação irão onerar o crédito orçamentário 001001001, de classificação funcional programática 14.122.1729.5904.0000 e categoria econômica 3.3.90.40.90.

CLÁUSULA NONA – DOS PAGAMENTOS

A CONTRATADA deverá emitir nota fiscal eletrônica (Modelo 55), e/ou nota fiscal conjugada, nos termos das legislações vigentes, em nome da CONTRATANTE, em 02 (duas) vias, nas quais deverá constar o número do procedimento licitatório. Em se tratando de serviço enquadrado na Lista Anexa à Lei Complementar nº 116 de 31/07/2003, com as alterações introduzidas pela Lei Complementar nº 157, de 29/12/2016, deverá a CONTRATADA emitir nota fiscal eletrônica de prestação de serviço, em cumprimento ao que dispuser a legislação onde a empresa estiver domiciliada/estabelecida.

a) A(s) nota(s) fiscal(is) emitida(s) pela CONTRATADA, deverá(ão) atender ao disposto no RICMS - Livro VI - Dos Anexos - Anexo I - Isenções, artigos 55 a 63 - Órgãos Públicos, discriminando no corpo da(s) nota(s) fiscal(is)/fatura o número do Decreto e o desconto no preço do valor equivalente ao imposto dispensado, resultando o valor líquido da nota fiscal igual ao valor final proposto pela CONTRATADA.

PARÁGRAFO PRIMEIRO

O pagamento será efetuado, mediante a apresentação dos originais da(s) nota(s) fiscal(is)/fatura à CONTRATANTE, inscrita no Cadastro Nacional de Pessoa Jurídica do Ministério da Fazenda sob o n.º 44.480.283/0001-91, situada na Rua Florêncio de Abreu, n.º 848 – 3º andar - Bairro Luz – São Paulo - SP – CEP 01030-001, em conformidade com a Cláusula Nona deste instrumento.

PARÁGRAFO SEGUNDO

O pagamento será realizado mediante depósito na conta corrente bancária em nome da CONTRATADA no Banco do Brasil S/A, de acordo com as seguintes condições:

I - em 30 (trinta) dias, contados da data de entrega da nota fiscal/fatura, ou de sua reapresentação em caso de incorreções, na forma e local previstos nesta Cláusula.

II - A discriminação dos valores dos serviços deverá ser reproduzida na nota fiscal/fatura apresentada para efeito de pagamento.

III - Quando for constatada irregularidade na Nota Fiscal/Fatura, será imediatamente solicitada à CONTRATADA carta de correção para regularização de erro ocorrido na emissão do documento fiscal, de acordo com o Comunicado SINIEF 01, de 30/03/2007, que deverá ser encaminhada ao gestor da CONTRATANTE no prazo de 02 (dois) dias e desde que o erro não esteja relacionado aos seguintes fatores:

a) Variáveis que determinam o valor do imposto tais como: base de cálculo, alíquota, diferença de preço, quantidade, valor da operação ou da prestação.

b) Correção de dados cadastrais que impliquem mudança do remetente ou do destinatário.

c) Data de emissão ou de saída.

IV - Caso a CONTRATADA não apresente carta de correção no prazo estipulado, o prazo para pagamento mencionado será recontado, a partir da data da sua apresentação.

PARÁGRAFO TERCEIRO
Havendo atraso no pagamento, 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 *pro rata temporis*, em relação ao atraso verificado.

PARÁGRAFO QUARTO
Constitui condição para a realização do pagamento a inexistência de registros em nome da CONTRATADA no "Cadastro Informativo dos Créditos não Quitados de Órgãos e Entidades Estaduais – CADIN ESTADUAL", o qual deverá ser consultado por ocasião da realização de cada pagamento. O cumprimento desta condição poderá se dar pela comprovação, pela CONTRATADA, de que os registros estão suspensos, nos termos do artigo 8º da Lei Estadual nº 12.799/2008.

PARAGRAFO QUINTO
A CONTRATANTE poderá, por ocasião do pagamento, efetuar a retenção de tributos determinada por lei, ainda que não haja indicação de retenção na nota fiscal apresentada ou que se refira a retenções não realizadas em meses anteriores.

PARÁGRAFO SEXTO
O recolhimento do Imposto sobre Serviços de Qualquer Natureza – ISSQN deverá ser feito em consonância com o artigo 3º e demais disposições da Lei Complementar Federal nº 116/2003, e respeitando as seguintes determinações:

I - Quando da celebração do contrato, a CONTRATADA deverá indicar a legislação municipal aplicável aos serviços por ela prestados, relativamente ao ISSQN, esclarecendo, expressamente, sobre a eventual necessidade de retenção do tributo, pelo tomador dos serviços;

II - Caso se mostre exigível, à luz da legislação municipal, a retenção do ISSQN pelo tomador dos serviços:

a) O CONTRATANTE, na qualidade de responsável tributário, deverá reter a quantia correspondente do valor da nota-fiscal, fatura, recibo ou documento de cobrança equivalente apresentada e recolher a respectiva importância em nome da CONTRATADA no prazo previsto na legislação municipal.

b) Para tanto, a CONTRATADA deverá destacar o valor da retenção, a título de "RETENÇÃO PARA O ISS" ao emitir a nota fiscal, fatura, recibo ou documento de cobrança equivalente. Considera-se preço do serviço a receita bruta a ele correspondente, sem nenhuma dedução.

III - Caso, por outro lado, não haja previsão de retenção do ISSQN pelo tomador dos serviços:

a) A CONTRATADA deverá apresentar declaração da Municipalidade competente com a indicação de sua data-limite de recolhimento ou, se for o caso, da condição de isenção;

b) Mensalmente a CONTRATADA deverá apresentar comprovante de recolhimento do ISSQN por meio de cópias das guias correspondentes ao serviço executado e deverá estar referenciado à data de emissão da nota fiscal, fatura ou documento de cobrança equivalente;

c) Caso, por ocasião da apresentação da nota fiscal, da fatura ou do documento de cobrança equivalente, não haja decorrido o prazo legal para recolhimento do ISSQN, poderão ser apresentadas cópias das guias de recolhimento referentes ao mês imediatamente anterior, devendo a CONTRATADA apresentar a documentação devida quando do vencimento do prazo legal para o recolhimento.

d) a não apresentação dessas comprovações assegura ao CONTRATANTE o direito de sustar o pagamento respectivo e/ou os pagamentos seguintes.

PARÁGRAFO SÉTIMO
Por ocasião da apresentação da Nota Fiscal/Fatura, a CONTRATADA deverá apresentar as seguintes certidões:

a) Certificado de regularidade do Fundo de Garantia por Tempo de Serviço (CRF - FGTS).

b) Certidão negativa, ou positiva com efeitos de negativa, de débitos trabalhistas (CNDT).

c) Certidão negativa, ou positiva com efeitos de negativa, de Débitos relativos a Créditos Tributários Federais e à Dívida Ativa da União.

d) Certidão emitida pela Fazenda Municipal da sede ou domicílio da licitante que comprove a regularidade de débitos tributários relativos ao Imposto sobre Serviços de Qualquer Natureza – ISSQN.

e) Certidão emitida pela Fazenda Estadual da sede ou domicílio da licitante que comprove a regularidade de débitos tributários relativos ao Imposto sobre Operações relativas à Circulação de Mercadorias e sobre Prestações de Serviços de Transporte Interestadual, Intermunicipal e de Comunicação – ICMS.

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.

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 prestação de garantia para a contratação que constitui objeto do presente instrumento.

CLÁUSULA DÉCIMA QUARTA - DA VIGÊNCIA CONTRATUAL

A vigência deste Contrato será contada a partir da data de sua assinatura, até o término final do prazo das atualizações dos softwares, que é de 36 (trinta e seis) meses após a renovação.

PARÁGRAFO PRIMEIRO

Inobstante o prazo de vigência contratual, permanecerão vigentes as obrigações contratuais da CONTRATADA relacionadas à prestação de garantia do(s) produtos(s) fornecido(s), bem como aquelas relacionadas à prestação de suporte, conforme informado na declaração do fabricante do(s) produto(s), de acordo com o previsto no Memorial Descritivo – Anexo I do edital e deste Termo de Contrato.

FUNDAÇÃO CASA
CENTRO DE ATENDIMENTO
SOCIOEDUCATIVO AO ADOLESCENTE

CLÁUSULA DÉCIMA QUINTA – DISPOSIÇÕES FINAIS

Fica ajustado, ainda, que:

I. Consideram-se partes integrantes do presente Termo de Contrato, como se nele estivessem transcritos:

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

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 em 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, 24 de JUNHO de 2019.

CONTRATANTE: FUNDAÇÃO CENTRO DE ATENDIMENTO SOCIOEDUCATIVO AO ADOLESCENTE – FUNDAÇÃO CASA

Paulo Dimas Debellis Mascaretti
Secretário da Justiça e Cidadania
Respondendo pelo Expediente da Fundação CASA

Aurélio Olímpio de Souza
Diretor Administrativo Interino

CONTRATADA: BRASOFTWARE INFORMÁTICA LTDA

Viviani Hupp de Oliveira
Procuradora

TESTEMUNHAS:

Paulo César Crusca Júnior
Gerente Administrativo

Romes Aziz Sabbag
Diretor de Divisão

FUNDAÇÃO CASA
CENTRO DE ATENDIMENTO
SOCIOEDUCATIVO AO ADOLESCENTE

ANEXO I

MEMORIAL DESCRITIVO

CONTRATAÇÃO DE EMPRESA PARA RENOVAÇÃO DA SOLUÇÃO ANTIVIRUS KASPERSKY END-POINT SECURITY FOR BUSINESS ADVANCED.

AGRUPAMENTO		SERVICO DE AQUISIÇÃO/ATUALIZAÇÃO DE USO DE SOFTWARE-AGRUPAMENTO DE PRECOS PARA PREGAO ELETRONICO		12662-4 (543) 33904090 0830
ITEM	**QUANT.**	**UNIDADE**	**DESCRIÇÃO**	**SIAFISICO**
01	4.500	UNIDADE	Kaspersky Endpoint Security For Business – Advanced Brazilian Edition. 2500-4999 Node 3 Year Gov	480-4 (1) 33904090 0830
02	01	UNIDADE	Kaspersky Manintenance Service Agreement, Business	336-0 (1) 33904090 0235

1. **Servidor de Administração e Console Administrativa**

1.1. Compatibilidade:

1.1.1. Microsoft Windows Server 2003 ou superior (Todas edições)
1.1.2. Microsoft Windows Server 2003 x64 ou superior (Todas edições)
1.1.3. Microsoft Windows Server 2008 (Todas edições)
1.1.4. Microsoft Windows Server 2008 Core (Todas edições)
1.1.5. Microsoft Windows Server 2008 x64 SP1 (Todas edições)
1.1.6. Microsoft Windows Server 2008 R2 (Todas edições)
1.1.7. Microsoft Windows Server 2008 R2 Core (Todas edições)
1.1.8. Microsoft Windows Server 2012 (Todas edições)
1.1.9. Microsoft Windows Server 2012 R2 (Todas edições)
1.1.10. Microsoft Windows XP Professional SP2 ou superior
1.1.11. Microsoft Windows XP Professional x64 e superior
1.1.12. Microsoft Windows Vista SP1
1.1.13. Microsoft Windows Vista x64 SP1
1.1.14. Microsoft Windows 7
1.1.15. Microsoft Windows 7 x64
1.1.16. Microsoft Windows 8
1.1.17. Microsoft Windows 8 x64

1.2.Suporta as seguintes plataformas virtuais:

1.2.1. VMware: Workstation 9.x, Workstation 10.x, ESX 4.x, ESXi 4.x, ESXi 5.5
1.2.2. Microsoft Hyper-V: 2008, 2008 R2, 2012, 2012 R2
1.2.3. KVM integrado com: RHEL 5.4 e 5.x acima, SLES 11 SPx, Ubuntu 10.10 LTS
1.2.4. Microsoft VirtualPC 6.0.156.0
1.2.5. Parallels Desktop 7 e superior
1.2.6. Oracle VM VirtualBox 4.0.4-70112 (Somente logon como convidado)
1.2.7. Citrix XenServer 6.1, 6.2

1.3.Características:

1.3.1. A console deve ser acessada via WEB (HTTPS) ou MMC;
1.3.2. Console deve ser baseada no modelo cliente/servidor
1.3.3. Compatibilidade com Windows Failover Clustering ou outra solução de alta disponibilidade
1.3.4. Deve permitir a atribuição de perfis para os administradores da Solução de Antivírus.
1.3.5. Console deve ser totalmente integrada com suas funções e módulos caso haja a necessidade no futuro de adicionar novas tecnologias tais como, criptografia, Patch management e MDM
1.3.6.As licenças deverão ser perpétuas, ou seja, expirado a validade da mesma o produto deverá permanecer funcional para a proteção contra códigos maliciosos;
1.3.7. Capacidade de remover remotamente e automaticamente qualquer solução de anti-virus (própria ou de terceiros) que estiver presente nas estações e servidores, sem a necessidade da senha de remoção do atual anti-virus;
1.3.8. Capacidade de instalar remotamente a solução de anti-virus nas estações e servidores Windows, através de compartilhamento administrativo, login script e/ou GPO de Active Directory;
1.3.9.Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria
1.3.10. A solução de gerencia deve permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas
1.3.11. Através da solução de gerência, deve ser possível verificar qual licença está aplicada para determinado computador
1.3.12. Capacidade de instalar remotamente a solução de segurança em smartphones e tablets de sistema iOS, Andoid e Windows
1.3.13. Capacidade de instalar remotamente qualquer "app" em smartphones e tablets de sistema iOS;
1.3.14. A solução de gerência centralizada deve permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle
1.3.15. Deverá ter a capacidade de criar regras para limitar o tráfego de comunicação cliente/servidor por subrede com os seguintes parâmetros: KB/s e horário.
1.3.16. Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux e Mac) protegidos pela solução anti-virus;
1.3.17. Capacidade de gerenciar smartphones e tablets (Windows Phone , Android e iOS) protegidos pela solução anti-virus;
1.3.18. Capacidade de gerar pacotes customizados (auto-executáveis) contendo a licença e configurações do produto;
1.3.19. Capacidade de atualizar os pacotes de instalação com as últimas vacinas;

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

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

1.3.22. Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes;

1.3.23. Deve permitir a realocação de máquinas novas na rede para um determinado grupo sem ter um agente ou endpoint instalado através dos seguintes parâmetros:
Nome do computador Nome
do domínio Range de IP
Sistema Operacional
Máquina virtual

1.3.24. Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas;

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

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

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

1.3.28. 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 antivirus instalado. Caso não possuir, deve instalar o anti-virus automaticamente;

1.3.29. Capacidade de agrupamento de máquina por características comuns entre as mesmas, por exemplo: agrupar todas as máquinas que não tenham o antivirus instalado, agrupar todas as máquinas que não receberam atualização nos últimos
2 dias, etc;

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

1.3.31. Deve fornecer as seguintes informações dos computadores:

1.3.31.1. Se o anti-virus está instalado;

1.3.31.2. Se o anti-virus está iniciado;

1.3.31.3. Se o anti-virus está atualizado;

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

1.3.31.5. Minutos/horas desde a última atualização de vacinas

1.3.31.6. Data e horário da última verificação executada na máquina;

1.3.31.7. Versão do anti-virus instalado na máquina;

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

1.3.31.9. Data e horário de quando a máquina foi ligada;

1.3.31.10. Quantidade de vírus encontrados (contador) na máquina;

1.3.31.11. Nome do computador;

1.3.31.12. Domínio ou grupo de trabalho do computador;
1.3.31.13. Data e horário da última atualização de vacinas;
1.3.31.14. Sistema operacional com Service Pack;
1.3.31.15. Quantidade de processadores;
1.3.31.16. Quantidade de memória RAM;
1.3.31.17. Usuário(s) logado(s) naquele momento, com informações de contato (caso disponíveis no Active Directory);
1.3.31.18. Endereço IP;
1.3.31.19. Aplicativos instalados, inclusive aplicativos de terceiros, com histórico de instalação, contendo data e hora que o software foi instalado ou removido.
1.3.31.20. Atualizações do Windows Updates instaladas
1.3.31.21. Informação completa de hardware contendo: processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de audio, adaptadores de rede, monitores, drives de CD/DVD
1.3.31.22. Vulnerabilidades de aplicativos instalados na máquina

1.3.32. Deve permitir bloquear as configurações do anti-virus instalado nas estações e servidores de maneira que o usuário não consiga alterará-las;

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

1.3.33.1. Mudança de gateway;
1.3.33.2. Mudança de subnet DNS;
1.3.33.3. Mudança de domínio;
1.3.33.4. Mudança de servidor DHCP;
1.3.33.5. Mudança de servidor DNS;
1.3.33.6. Mudança de servidor WINS;
1.3.33.7. Aparecimento de nova subnet;

1.3.34. Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet;

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

1.3.36. Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de anti-virus;

1.3.37. Capacidade de herança de tarefas e políticas na estrutura hierarquica de servidores administrativos;

1.3.38. Capacidade de eleger qualquer computador cliente como repositório de vacinas e de pacotes de instalação, sem que seja necessária a instalação de um servidor administrativo completo, onde outras máquinas clientes irão atualizar- se e receber pacotes de instalação, a fim de otimizar tráfego da rede;

1.3.39. Capacidade de fazer deste repositório de vacinas um gateway para conexão com o servidor de administração, para que outras máquinas que não consigam conectar-se diretamente ao servidor possam usar este gateway para receber e enviar informações ao servidor administrativo.

1.3.40. Capacidade de exportar relatórios para os seguintes tipos de arquivos: PDF, HTML e XML.

1.3.41. Capacidade de gerar traps SNMP para monitoramento de eventos;

1.3.42. Capacidade de enviar emails para contas específicas em caso de algum evento;

1.3.43. Deve possuir compatibilidade com Microsoft NAP, quando instalado em um

Windows 2008 Server;

1.3.44. Deve possuir compatibilidade com Cisco Network Admission Control (NAC);

1.3.45. Deve possuir documentação da estrutura do banco de dados para geração de relatórios a partir de ferramentas específicas de consulta (Crystal Reports, por exemplo).

1.3.46. Capacidade de ligar máquinas via Wake on Lan para realização de tarefas (varredura, atualização, instalação, etc), inclusive de máquinas que estejam em subnets diferentes do servidor;

1.3.47. Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado intervalo de tempo);

1.3.48. Capacidade de realizar atualização incremental de vacinas nos computadores clientes;

1.3.49. Deve armazenar localmente e enviar ao servidor de gerência a 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

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

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

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

1.3.53. Capacidade de diferenciar máquinas virtuais de máquinas físicas;

2. Estações Windows -

2.1.Compatibilidade:

2.1.1. Microsoft Windows XP Professional SP3 e superior
2.1.2. Microsoft Windows Vista Business/Enterprise/Ultimate SP2
2.1.3. Microsoft Windows Vista Business/Enterprise/Ultimate x64 SP2
2.1.4. Microsoft Windows 7 Professional/Enterprise/Ultimate
2.1.5. Microsoft Windows 7 Professional/Enterprise/Ultimate x64
2.1.6.Microsoft Windows 7 Professional/Enterprise/Ultimate SP1 e superior
2.1.7.Microsoft Windows 7 Professional/Enterprise/Ultimate x64 SP1 e superior
2.1.8. Microsoft Windows 8 Professional/Enterprise
2.1.9. Microsoft Windows 8 Professional/Enterprise x64
2.1.10. Microsoft Windows 8.1 Enterprise x86 / 64
2.1.11. Microsoft Windows 8.1 Pro x86 /64
2.1.12. Microsoft Windows 10 Enterprise x86 / 64
2.1.13. Microsoft Windows 10 Pro x86 / 64

2.2.Características:

2.2.1. Deve prover as seguintes proteções:

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

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

2.2.1.3. Antivírus de Email (módulo para verificação de emails recebidos e enviados, assim como seus anexos)

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

2.2.1.5. O Endpoint 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. Auto-proteção (contra ataques aos serviços/processos do antivírus)

2.2.1.8. Controle de dispositivos externos

2.2.1.9. Controle de acesso a sites por categoria

2.2.1.10. Controle de acesso a sites por horário

2.2.1.11. Controle de acesso a sites por usuários

2.2.1.12. Controle de execução de aplicativos

2.2.1.13. Controle de vulnerabilidades do Windows e dos aplicativos instalados

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

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

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

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

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

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

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

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

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

2.2.11. Capacidade de verificar somente arquivos novos e alterados;

2.2.12. Capacidade de verificar objetos usando heurística;

2.2.13. Capacidade de agendar uma pausa na verificação;

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

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

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

2.2.16.1. Perguntar o que fazer, ou;

2.2.16.2. Bloquear acesso ao objeto;

2.2.16.2.1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
2.2.16.2.2. Caso positivo de desinfecção:
2.2.16.2.2.1. Restaurar o objeto para uso;
2.2.16.2.3. Caso negativo de desinfecção:
2.2.16.2.3.1. Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);

2.2.17. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto.
2.2.18. Capacidade de verificar emails recebidos e enviados nos protocolos POP3, IMAP, NNTP, SMTP e MAPI, assim como conexões criptografadas (SSL) para POP3 e IMAP (SSL);
2.2.19. Capacidade de verificar tráfego de ICQ, MSN, AIM e IRC contra vírus e links phishings;
2.2.20. Capacidade de verificar links inseridos em emails contra phishings;
2.2.21. Capacidade de verificar tráfego SSL nos browsers: Internet Explorer, Firefox e Opera;
2.2.22. Capacidade de verificação de corpo e anexos de emails usando heurística;
2.2.23. O antivírus de email, ao encontrar um objeto potencialmente perigoso, deve:
2.2.23.1. Perguntar o que fazer, ou;
2.2.23.2. Bloquear o email;
2.2.23.2.1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
2.2.23.2.2. Caso positivo de desinfecção:
2.2.23.2.2.1. Restaurar o email para o usuário;
2.2.23.2.3. Caso negativo de desinfecção:
2.2.23.2.3.1. Mover para quarentena ou apagar o objeto (de acordo com a configuração pré-estabelecida pelo administrador);
2.2.24. Caso o email conter código que parece ser, mas não é definitivamente malicioso, o mesmo deve ser mantido em quarentena.
2.2.25. Possibilidade de verificar somente emails recebidos ou recebidos e enviados.
2.2.26. Capacidade de filtrar anexos de email, apagando-os ou renomeando-os de acordo com a configuração feita pelo administrador.
2.2.27. Capacidade de verificação de tráfego HTTP e qualquer script do Windows Script Host (JavaScript, Visual Basic Script, etc), usando heurísticas;
2.2.28. Deve ter suporte total ao protocolo IPv6;
2.2.29. Capacidade de alterar as portas monitoradas pelos módulos de Web e Email;
2.2.30. Na verificação de tráfego web, caso encontrado código malicioso o programa deve:
2.2.30.1. Perguntar o que fazer, ou;
2.2.30.2. Bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio, ou;
2.2.30.3. Permitir acesso ao objeto;
2.2.31. O antivírus de web deve realizar a verificação de, no mínimo, duas maneiras diferentes, sob escolha do administrador:
2.2.31.1. Verificação *on-the-fly*, onde os dados são verificados enquanto são recebidos em tempo-real, ou;
2.2.31.2. Verificação de *buffer*, onde os dados são recebidos e armazenados para posterior verificação.

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

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

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

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

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

2.2.37. Capacidade de distinguir diferentes sub-nets e conceder opção de ativar ou não o firewall para uma sub-net específica;

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

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

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

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

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

2.2.40.1. Discos de armazenamento locais
2.2.40.2. Armazenamento removível
2.2.40.3. Impressoras
2.2.40.4. CD/DVD
2.2.40.5. Drives de disquete
2.2.40.6. Modems
2.2.40.7. Dispositivos de fita
2.2.40.8. Dispositivos multifuncionais
2.2.40.9. Leitores de smart card
2.2.40.10. Dispositivos de sincronização via ActiveSync (Windows CE, Windows Mobile, etc)
2.2.40.11. Wi-Fi
2.2.40.12. Adaptadores de rede externos
2.2.40.13. Dispositivos MP3 ou smartphones
2.2.40.14. Dispositivos Bluetooth

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

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

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

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

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

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

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

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

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

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

3. Estações e Servidores Mac OS X -

3.1.Compatibilidade:

3.1.1.Mac OS X 10.4.11 ou superior
3.1.2. Mac OS X 10.5 (Leopard)
3.1.3. Mac OS X 10.6 (Snow Leopard)
3.1.4. Mac OS X 10.7 (Lion)
3.1.5. Mac OS X 10.8 (Mountain Lion)
3.1.6. Mac OS X 10.9 (Mavericks)
3.1.7. Mac OS X 10.10 (Yosemite)
3.1.8. Mac OS X Server 10.6 x86 e x64
3.1.9. Mac OS X Server 10.7 x86 e x64

3.2.Características:

3.2.1. Deve prover proteção residente para arquivos (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;

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

3.2.3.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;

3.2.4. Deve possuir suportes a notificações utilizando o Growl;

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

3.2.6. Capacidade de voltar para a base de dados de vacina anterior;

3.2.7. Capacidade de varrer a quarentena automaticamente após cada atualização de vacinas;

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

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

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

3.2.11. Capacidade de verificar somente arquivos novos e alterados;

3.2.12. Capacidade de verificar objetos usando heurística;

3.2.13. Capacidade de agendar uma pausa na verificação;

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

3.2.14.1. Perguntar o que fazer, ou;

3.2.14.2. Bloquear acesso ao objeto;

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

3.2.14.2.2. Caso positivo de desinfecção:

3.2.14.2.2.1. Restaurar o objeto para uso;

3.2.14.2.3. Caso negativo de desinfecção:

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

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

3.2.16. Capacidade de verificar arquivos de formato de email;

3.2.17. 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;

3.2.18. 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. Canaima 3

4.1.1.2. Red Flag Desktop 6.0 SP2

4.1.1.3. Red Hat Enterprise Linux 5.8 Desktop

4.1.1.4. Red Hat Enterprise Linux 6.2 Desktop

4.1.1.5. Fedora 16

4.1.1.6. CentOS-6.2

4.1.1.7. SUSE Linux Enterprise Desktop 10 SP4

4.1.1.8. SUSE Linux Enterprise Desktop 11 SP2
4.1.1.9. openSUSE Linux 12.1
4.1.1.10. openSUSE Linux 12.2
4.1.1.11. Debian GNU/Linux 6.0.5
4.1.1.12. Mandriva Linux 2011
4.1.1.13. Ubuntu 10.04 LTS
4.1.1.14. Ubuntu 12.04 LTS

4.1.2. Plataforma 64-bits:
4.1.2.1. Canaima 3
4.1.2.2. Red Flag Desktop 6.0 SP2
4.1.2.3. Red Hat Enterprise Linux 5.8
4.1.2.4. Red Hat Enterprise Linux 6.2 Desktop
4.1.2.5. Fedora 16
4.1.2.6. CentOS-6.2
4.1.2.7. SUSE Linux Enterprise Desktop 10 SP4
4.1.2.8. SUSE Linux Enterprise Desktop 11 SP2
4.1.2.9. openSUSE Linux 12.1
4.1.2.10. openSUSE Linux 12.2
4.1.2.11. Debian GNU/Linux 6.0.5
4.1.2.12. Ubuntu 10.04 LTS
4.1.2.13. 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 desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;
4.2.2.3. Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;
4.2.2.4. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados.

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

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

4.2.5. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomá-la a partir da extensão do arquivo;
4.2.6. Capacidade de verificar objetos usando heurística;
4.2.7. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena
4.2.8. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados
4.2.9. Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).

5. Servidores Windows -

5.1. Compatibilidade:

5.1.1. Microsoft Windows Small Business Server 2011 Essentials/Standard x64
5.1.2. Microsoft Windows Server 2003 Standard/Enterprise SP2 x86/x64
5.1.3. Microsoft Windows Server 2003 R2 Standard/Enterprise SP2 x86/x64
5.1.4. Microsoft Windows Server 2008 Standard/Enterprise/Datacenter SP1 x86/x64
5.1.5. Microsoft Windows Server 2008 Core Standard/Enterprise/Datacenter SP1 x86/x64
5.1.6. Microsoft Windows Server 2008 R2 Standard/Enterprise/Datacenter SP1
5.1.7. Microsoft Windows Server 2008 R2 Core Standard/Enterprise/Datacenter SP1
5.1.8. Microsoft Windows Server 2012 Foundation/Essentials/Standard x64
5.1.9. Microsoft Windows Hyper-V Server 2008 R2 SP1
5.1.10. Microsoft Terminal baseado em Windows Server 2003
5.1.11. Microsoft Terminal baseado em Windows Server 2008
5.1.12. Microsoft Terminal baseado em Windows Server 2008 R2
5.1.13. Citrix Presentation Server 4.0 e 4.5
5.1.14. Citrix XenApp 4.5, 5.0 e 6.0

5.2. Característica:

5.2.1. Deve prover as seguintes proteções:
5.2.1.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado
5.2.1.2. Auto-proteção contra ataques aos serviços/processos do antivírus
5.2.1.3. Firewall com IDS
5.2.1.4. Controle de vulnerabilidades do Windows e dos aplicativos instalados
5.2.2. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
5.2.3. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora.
5.2.4. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
5.2.4.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
5.2.4.2. Gerenciamento de tarefa (criar ou excluir tarefas de verificação)
5.2.4.3. Leitura de configurações
5.2.4.4. Modificação de configurações
5.2.4.5. Gerenciamento de Backup e Quarentena
5.2.4.6. Visualização de relatórios

5.2.4.7. Gerenciamento de relatórios
5.2.4.8. Gerenciamento de chaves de licença
5.2.4.9. Gerenciamento de permissões (adicionar/excluir permissões acima)

5.2.5. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:
5.2.5.1. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;
5.2.5.2. Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.

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

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

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

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

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

5.2.11. Capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado nos servidor.

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

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

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

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

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

5.2.17. Capacidade de verificar somente arquivos novos e alterados;

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

5.2.19. Capacidade de verificar objetos usando heurística;

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

5.2.21. Capacidade de agendar uma pausa na verificação;

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

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

5.2.23.1. Perguntar o que fazer, ou;

5.2.23.2. Bloquear acesso ao objeto;

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

5.2.23.2.2. Caso positivo de desinfecção:

5.2.23.2.2.1. Restaurar o objeto para uso;

5.2.23.2.3. Caso negativo de desinfecção:

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

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

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

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

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

6. Servidores Linux -

6.1.Compatibilidade:

6.1.1. Plataforma 32-bits:

6.1.1.1. Canaima 3

6.1.1.2. Asianux Server 3 SP4

6.1.1.3. Asianux Server 4 SP1

6.1.1.4. Red Hat Enterprise Linux 6.2 Server;

6.1.1.5. Red Hat Enterprise Linux 5.8 Server

6.1.1.6. Fedora 16;

6.1.1.7. CentOS-6.2;

6.1.1.8. SUSE Linux Enterprise Server 11 SP2;

6.1.1.9. Novell Open Enterprise Server 11;

6.1.1.10. openSUSE Linux 12.1;

6.1.1.11. openSUSE Linux 12.2;

6.1.1.12. Mandriva Enterprise Server 5.2;

6.1.1.13. Ubuntu Server 10.04.2 LTS;

6.1.1.14. Ubuntu Server 12.04 LTS;

6.1.1.15. Debian GNU/Linux 6.0.5;

6.1.1.16. FreeB.SD 8.3;

6.1.1.17. FreeBSD 9.

6.1.2.Plataforma 64-bits:

6.1.2.1. Canaima 3

6.1.2.2. Asianux Server 3 SP4

6.1.2.3. Asianux Server 4 SP1

6.1.2.4. Red Hat Enterprise Linux 6.2 Server;

6.1.2.5. Red Hat Enterprise Linux 5.8 Server

6.1.2.6. Fedora 16;
6.1.2.7. CentOS-6.2;
6.1.2.8. SUSE Linux Enterprise Server 11 SP2;
6.1.2.9. Novell Open Enterprise Server 11;
6.1.2.10. openSUSE Linux 12.1;
6.1.2.11. openSUSE Linux 12.2;
6.1.2.12. Mandriva Enterprise Server 5.2;
6.1.2.13. Ubuntu Server 10.04.2 LTS;
6.1.2.14. Ubuntu Server 12.04 LTS;
6.1.2.15. Debian GNU/Linux 6.0.5;
6.1.2.16. FreeBSD 8.3;
6.1.2.17. FreeBSD 9.

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:

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

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

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

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

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

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

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

6.2.6. Capacidade de verificar objetos usando heurística;

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

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

6.2.9.Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux)

7. **Servidores Novell Netware:**

7.1.Compatibilidade:

7.1.1. Novell Netware 5.x Support Pack 6 ou superior
7.1.2. Novell Netware 6.0 Support Pack 3 ou superior
7.1.3. Novell Netware 6.5 Support Pack 3 ou superior

7.2. Características:

7.2.1. Deve possuir proteção em tempo real para arquivos acessados, criados ou modificados;
7.2.2. Deve possuir verificação manual e agendada de acordo com a configuração do administrador;
7.2.3. Capacidade de realizar update de maneira automatica, via internet ou LAN;
7.2.4. Capacidade de fazer um rollback das vacinas;
7.2.5. Capacidade de mover arquivos suspeitos ou infectados para área de quarentena;
7.2.6. Capacidade de criar logs detalhados e salvar resultados das verificações agendadas;
7.2.7. Capacidade de salvar um backup de todos os objetos infectados e suspeitos tratados;
7.2.8. Capacidade de notificar o administrador de varreduras concluidas e sobre objetos maliciosos encontrados no servidor, utilizando a rede Novell ou email;

8. **Smartphones e tablets**

8.1.Compatibilidade:

8.1.1. Apple iOS 7.0 - 9.2
8.1.2. Windows Phone 8.1
8.1.3. Android OS 2.3 - 5.1

8.2.Características

8.2.1. Deve prover as seguintes proteções:
8.2.1.1. Proteção em tempo real do sistema de arquivos do dispositivo - interceptação e verificação de:
8.2.1.1.1. Todos os objetos transmitidos usando conexões wireless (porta de infra-vermelho, Bluetooth) e mensagens EMS, durante sincronismo com PC e ao realizar download usando o browser.
8.2.1.1.2. Arquivos abertos no smartphone
8.2.1.1.3. Programas instalados usando a interface do smartphone
8.2.1.2. Verificação dos objetos na memória interna do smartphone e nos cartões de expanção sob demanda do usuário e de acordo com um agendamento;
8.2.2. Deverá isolar em área de quarentena os arquivos infectados;
8.2.3. Deverá atualizar as bases de vacinas de modo agendado;
8.2.4. Deverá bloquear spams de SMS através de Black lists;
8.2.5. Deverá ter função de bloqueio do aparelho caso o SIM CARD for trocado para outro não autorizado;
8.2.6. Capacidade de desativar por política:
Wi-fi
Camera
Bluetooth

8.2.7. Deverá ter função de limpeza de dados pessoais a distância, em caso de roubo, por exemplo.
8.2.8. Capacidade de requerer uma senha para desbloquear o dispositivo e personalizar a quantidade de caracteres para esta senha
8.2.9. Deverá ter firewall pessoal;
8.2.10. Capacidade de tirar fotos quando a senha for inserida incorretamente (Mugshot)
8.2.11. Possibilidade de instalação remota utilizando o Microsoft System Center Mobile Device Manager 2008 SP1
8.2.12. Capacidade de enviar comandos remotamente de:
Localizar
Bloquear
8.2.13. Capacidade de detectar Jailbreak em dispositivos iOS
8.2.14. Capacidade de bloquear o acesso a site por categoria em dispositivos
8.2.15. Capacidade de bloquear o acesso a sites phishing ou malicioso
8.2.16. Capacidade de criar containers de aplicativos, separando dados corporativos de dados pessoais
8.2.17. Capacidade de bloquear o dispositivo quando o cartão "SIM" for substituído
8.2.18. Capacidade de configurar White e blacklist de aplicativos
8.2.19. Capacidade de localizar o dispositivo quando necessário
8.2.20. Permitir atualização das definições quando estiver em "roaming"
8.2.21. Capacidade de selecionar endereço do servidor para buscar a definição de vírus
8.2.22. Capacidade de enviar URL de instalação por e-mail
8.2.23. Capacidade de fazer a instalação através de um link QRCode
8.2.24. Capacidade de executar as seguintes ações caso a desinfecção falhe:
Deletar
Ignorar
Quarentenar
Perguntar ao usuário

9. Gerenciamento de dispositivos móveis (MDM):

9.1.Compatibilidade:

9.1.1. Dispositivos conectados através do Microsoft Exchange ActiveSync
9.1.1.1. Apple iOS
9.1.1.2. Windows Phone
9.1.1.3. Android
9.1.2. Dispositivos com suporte ao Apple Push Notification (APNs) servisse
9.1.2.1. Apple iOS 3.0 ou superior

9.2.Características:

9.2.1. Capacidade de aplicar políticas de ActiveSync através do servidor Microsoft Exchange
9.2.2. Capacidade de ajustar as configurações de:
9.2.2.1. Sincronização de e-mail
9.2.2.2. Uso de aplicativos
9.2.2.3. Senha do usuário
9.2.2.4. Criptografia de dados
9.2.2.5. Conexão de mídia removível
9.2.3. Capacidade de instalar certificados digitais em dispositivos móveis

9.2.4. Capacidade de, remotamente, resetar a senha de dispositivos iOS
9.2.5. Capacidade de, remotamente, apagar todos os dados de dispositivos iOS
9.2.6. Capacidade de, remotamente, bloquear um dispositivo iOS

10. Criptografia:

10.1. Compatibilidade:

10.1.1. Microsoft Windows XP Professional SP3 ou superior
10.1.2. Microsoft Windows Vista Business/Enterprise/Ultimate SP2
10.1.3. Microsoft Windows Vista Business/Enterprise/Ultimate x64 SP2
10.1.4. Microsoft Windows 7 Professional/Enterprise/Ultimate
10.1.5. Microsoft Windows 7 Professional/Enterprise/Ultimate x64
10.1.6. Microsoft Windows 8 Professional/Enterprise
10.1.7. Microsoft Windows 8 Professional/Enterprise x64
10.1.8. Microsoft Windows 8.1 Professional / Enterprise
10.1.9. Microsoft Windows 8.1 Professional / Enterprise x64
10.1.10. Microsoft Windows 10 Pro x86 / x64
10.1.11. Microsoft Windows 10 Enterprise x86 /x64

10.2. Características:

10.2.1. 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.
10.2.2. Utilizar, no mínimo, algoritmo AES com chave de 256 bits.
10.2.3. Capacidade de criptografar completamente o disco rígido da máquina, adicionando um ambiente de pré-boot para autenticação do usuário.
10.2.4. Capacidade de utilizar *Single Sign-On* para a autenticação de pré-boot.
10.2.5. Permitir criar vários usuários de autenticação pré-boot.
10.2.6. Capacidade de criar um usuário de autenticação pré-boot comum com uma senha igual para todas as máquinas a partir da console de gerenciamento.
10.2.7. Capacidade de criptografar drives removíveis de acordo com regra criada pelo administrador, com as opções:
10.2.7.1. Criptografar somente os arquivos novos que forem copiados para o disco removível, sem modificar os arquivos já existentes.
10.2.7.2. Criptografar todos os arquivos individualmente.
10.2.7.3. Criptografar o dispositivo inteiro, de maneira que não seja possível listar os arquivos e pastas armazenadas.
10.2.7.4. Criptografar o dispositivo em modo portátil, permitindo acessar os arquivos em máquinas de terceiros através de uma senha.
10.2.8. 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.
10.2.9. Capacidade de criar regras de exclusões para que certos arquivos ou pastas nunca sejam criptografados.
10.2.10. Capacidade de selecionar aplicações que podem ou não ter acesso aos arquivos criptografados.
10.2.11. Verifica compatibilidade de hardware antes de aplicar a criptografia
10.2.12. Possibilita estabelecer parâmetros para a senha de criptografia

10.2.13. Bloqueia o reuso de senhas
10.2.14. Bloqueia a senha após um número de tentativas pré estabelecidas
10.2.15. Capacidade de permitir o usuário solicitar permissão a determinado arquivo criptografado para o administrador mediante templates customizados
10.2.16. Permite criar exclusões para não criptografar determinados "discos rígidos" através de uma busca por nome do computador ou nome do dispositivo
10.2.17. Permite criptografar as seguintes pastas pré-definidas: "meus documentos", "Favoritos", "Desktop", "Arquivos temporários" e "Arquivos do outlook"
10.2.18. Permite utilizar variáveis de ambiente para criptografar pastas customizadas.
10.2.19. Capacidade de criptografar arquivos por grupos de extensão, tais como: Documentos do office, Document, arquivos de audio, etc
10.2.20. Permite criar um grupo de extensões de arquivos a serem criptografados
10.2.21. Capacidade de criar regra de criptografia para arquivos gerados por aplicações
10.2.22. Permite criptografia de dispositivos móveis mesmo quando o endpoint não possuir comunicação com a console de gerenciamento.

11. Gerenciamento de Sistemas:

11.1. Capacidade de criar imagens de sistema operacional remotamente e distribuir essas imagens para computadores gerenciados pela solução e para computadores *bare-metal*.
11.2. Capacidade de detectar softwares de terceiros vulneráveis, criando assim um relatório de softwares vulneráveis.
11.3. Capacidade de corrigir as vulnerabilidades de softwares, fazendo o download centralizado da correção ou atualização e aplicando essa correção ou atualização nas máquinas gerenciadas de maneira transparente para os usuários.
11.4. Possuir tecnologia de Controle de Admissão de Rede (NAC), com a possibilidade de criar regras de quais tipos de dispositivos podem ter acessos a recursos da rede.
11.5. Capacidade de gerenciar licenças de softwares de terceiros.
11.6. Capacidade de registrar mudanças de hardware nas máquinas gerenciadas.
11.7. Capacidade de gerenciar um inventário de hardware, com a possibilidade de cadastro de dispositivos (ex: router, switch, projetor, acessório, etc), informando data de compra, local onde se encontra, service tag, número de identificação e outros.
11.8. Possibilita fazer distribuição de software de forma manual e agendada
11.9. Suporta modo de instalação silenciosa
11.10. Suporte a pacotes MSI, exe, bat, cmd e outros padrões de arquivos executáveis
11.11. Possibilita fazer a distribuição através de agentes de atualização
11.12. Utiliza tecnolodia multicast para evitar tráfego na rede
11.13. Possibilita criar um inventário centralizado de imagens
11.14. Capacidade de atualizar o sistema operacional direto da imagem mantendo os dados do usuário
11.15. Suporte a WakeOnLan para deploy de imagens
11.16. Capacidade de atuar como servidor de atualização do Windows podendo fazer deploy de patches
11.17. Suporta modo de teste, podendo atribuir alguns computadores para receberem as atualizações de forma automatica para avaliação de alterações no comportamento

11.18. Capacidade de gerar relatórios de vulnerabilidades e patches

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

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

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

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

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

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

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

12. Serviços de Instalação:

12.1. Todos os serviços deverão ser executados por técnicos certificados pelo fabricante do software, que deverá ser comprovado através de certificações emitidas pelo próprio fabricante;

12.2. Documentação do Plano Técnico do Projeto e a Implementação do mesmo;

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

12.4. Validação das soluções implantadas;

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

12.4.2. Treinamento oficial pelo fabricante para 4 colaboradores;

12.4.3. Entrega dos ambientes em produção;

12.4.4. Políticas de segurança definidas;

12.4.5. Elaboração do documento técnico final do projeto;

12.5. Aceite por parte da CONTRATANTE.

13. Garantia e validade das licenças:

14.1. A validade das licenças será de 36 meses ininterruptos;

14.2. Suporte Premium de 36 meses.

FUNDAÇÃO CASA
CENTRO DE ATENDIMENTO
SOCIOEDUCATIVO AO ADOLESCENTE

ANEXO II

PLANILHA DE PROPOSTA DE PREÇOS

A

CENTRO DE ATENDIMENTO SOCIEDUCATIVO AO ADOLESCENTE - FUNDAÇÃO CASA

Referente: Pregão Eletrônico Nº 044/2019.

OBJETO: Contratação de empresa para renovação da Solução Antivirus Kasperssky EndPoint Security for Business Advanced.

Item	QTDE	Descrição / FABRICANTE	Valor Unitário (R$)	Preço total (R$)
1	4500	MARCA: Kaspersky Endpoint Security for Business – Advanced Brazilian Edition - 3 year Gov FABRICANTE: KASPERSKY Procedência: RUSSIA	R$68,14	R$306.630,00
2	1	MARCA: Kaspersky Manintenance Service Agreement, Business FABRICANTE: KASPERSKY Procedência : RUSSIA	R$231.370,00	R$ 231.370,00
			Valor Global	R$ 538.000,00

PRAZO DE ENTREGA:

De Acordo om edital.

PRAZO DE PAGAMENTO:

acordo com Edital.

VALIDADE DE PROPOSTA:

60 (sessenta) dias.

Poá, 14 de Junho de 2019

ARIANE ANDRADE DOS SANTOS
Fone: +55 11 3179-6756
Fax: +55 11 3179-6800
governo-saopaulo@brasoftware.com.br
www.brasoftware.com.br

57.142.978/0001-05
BRASOFTWARE INFORMÁTICA LTDA.
Rua Marina La Regina, 227
3º andar - Sala 11 à 16
Centro - Cep: 08550-210
Poá - SP