FUNDAÇÃO CASA
CENTRO DE ATENDIMENTO SOCIOEDUCATIVO AO ADOLESCENTE

PROCESSO SDE 9886/22 - FUNDCASASP-PRC-2022/09886
PREGÃO ELETRÔNICO SDE n.° 073/2022
CÓDIGO ÚNICO: 2022040367-1
CONTRATO SCO n.° 026/2022

TERMO DE CONTRATO CELEBRADO ENTRE A FUNDAÇÃO CASA E A EMPRESA DMK3 TECNOLOGIA LTDA, TENDO POR OBJETO A RENOVAÇÃO DE LICENCIAMENTO DE SOFTWARE END-POINT KASPERSKY

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 Fernando José da Costa, Secretário da Justiça e Cidadania, respondendo pelo expediente da Fundação CASA, nos termos do Decreto, publicado no DOE de 05-10-2020 e por seu Diretor Administrativo Aurélio Olímpio de Souza, nomeado nos termos da Portaria Administrativa n.º 831/2019, doravante denominada simplesmente **CONTRATANTE**.

II - CONTRATADA: **DMK3 TECNOLOGIA LTDA**, pessoa jurídica de direito privado, inscrita no Cadastro Nacional de Pessoa Jurídica do Ministério da Fazenda sob o n.º 23.247.377/0001-45, localizada à Avenida Iraí, n.º 79, CJ 134 e 135, Bloco B, Torres Aratas, Indianapolis – São Paulo - SP, CEP 04082-000, neste ato representada por sua sócia Mirella Saori Rocha Kurata, portadora da Cédula de Identidade n.º 27.610.095-5 SSP/SP e inscrita no CPF/MF sob o n.º 220.342.728-03, conforme consta 4ª Alteração do Contrato Social, 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 de licenciamento de Software End-Point Kaspersky, no qual se submetem as partes às cláusulas e condições adiante estipuladas, que reciprocamente se outorgam e aceitam e que darão integral cumprimento.

A lavratura do presente contrato decorre de licitação promovida na modalidade PREGÃO, em sua forma ELETRÔNICA, de SDE n.º 073/2022, advinda do Despacho DTI S/Nº, que deu origem ao Processo SDE n.º 9886/222 - **FUNDCASASP-PRC-2022/09886**, realizada

FUNDCASASPDCI202261966

Assinado com senha por SABRINA MIRANDA ARRAES DE CAMPOS - GERENTE ADMINISTRATIVO I / GCCCP - 21/07/2022 às 12:23:01, AURELIO OLIMPIO DE SOUZA - DIRETOR ADMINISTRATIVO / DGA - 21/07/2022 às 13:01:32, FERNANDO JOSÉ DA COSTA - PRESIDENTE / GP - 21/07/2022 às 13:03:16 e ROSANA MORENO PIRES - DIRETOR DE DIVISÃO I / DSUP - 21/07/2022 às 13:27:47.
Autenticado com senha por DANIELLA ALVES MAURICIO - ASSISTENTE TECNICO ADM I / SCO - 21/07/2022 às 11:39:04.
Documento Nº: 47591886-10 - consulta à autenticidade em
https://www.documentos.spsempapel.sp.gov.br/sigaex/public/app/autenticar?n=47591886-10

SIGA

FUNDAÇÃO CASA
CENTRO DE ATENDIMENTO SOCIOEDUCATIVO AO ADOLESCENTE

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 de licenciamento de Software End-Point Kaspersky** conforme detalhamento e especificações técnicas constantes do Memorial Descritivo, da proposta da CONTRATADA e demais documentos constantes do processo administrativo em epígrafe.

PARÁGRAFO ÚNICO

O presente contrato será regido pela Lei Federal nº 10.520/2002 e pelas normas mencionadas no preâmbulo durante toda a sua vigência, nos termos do parágrafo único do artigo 191 c/c o inciso II do artigo 193 da Lei Federal nº 14.133/2021.

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. art. 55, inciso 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. O prazo de execução (instalação/implementação) é de 45 (quarenta e cinco) dias úteis, juntamente com a transferência de conhecimento.

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 – 8º andar - Luz - São Paulo - SP – CEP 01030-001.

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 da entrega ou da própria aquisição

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.

FUNDCASASPDCI202261966

Assinado com senha por SABRINA MIRANDA ARRAES DE CAMPOS - GERENTE ADMINISTRATIVO I / GCCCP - 21/07/2022 às 12:23:01, AURELIO OLIMPIO DE SOUZA - DIRETOR ADMINISTRATIVO / DGA - 21/07/2022 às 13:01:32, FERNANDO JOSÉ DA COSTA - PRESIDENTE / GP - 21/07/2022 às 13:03:16 e ROSANA MORENO PIRES - DIRETOR DE DIVISÃO I / DSUP - 21/07/2022 às 13:27:47.
Autenticado com senha por DANIELLA ALVES MAURICIO - ASSISTENTE TECNICO ADM I / SCO - 21/07/2022 às 11:39:04.
Documento Nº: 47591886-10 - consulta à autenticidade em
https://www.documentos.spsempapel.sp.gov.br/sigaex/public/app/autenticar?n=47591886-10

FUNDAÇÃO CASA
CENTRO DE ATENDIMENTO SOCIOEDUCATIVO AO ADOLESCENTE

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 - obedecer às normas e rotinas do CONTRATANTE, em especial as que disserem respeito à proteção de dados pessoais, à segurança, à guarda, à manutenção e à integridade das informações coletadas, custodiadas, produzidas, recebidas, classificadas, utilizadas, acessadas, reproduzidas, transmitidas, distribuídas, processadas, arquivadas, eliminadas ou avaliadas durante a execução do objeto a que se refere a Cláusula Primeira deste Contrato, observando as normas legais e regulamentares aplicáveis.

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.

FUNDCASASPDCI202261966

Assinado com senha por SABRINA MIRANDA ARRAES DE CAMPOS - GERENTE ADMINISTRATIVO I / GCCCP - 21/07/2022 às 12:23:01, AURELIO OLIMPIO DE SOUZA - DIRETOR ADMINISTRATIVO / DGA - 21/07/2022 às 13:01:32, FERNANDO JOSÉ DA COSTA - PRESIDENTE / GP - 21/07/2022 às 13:03:16 e ROSANA MORENO PIRES - DIRETOR DE DIVISÃO I / DSUP - 21/07/2022 às 13:27:47.
Autenticado com senha por DANIELLA ALVES MAURICIO - ASSISTENTE TECNICO ADM I / SCO - 21/07/2022 às 11:39:04.
Documento Nº: 47591886-10 - consulta à autenticidade em
https://www.documentos.spsempapel.sp.gov.br/sigaex/public/app/autenticar?n=47591886-10

FUNDAÇÃO CASA
CENTRO DE ATENDIMENTO SOCIOEDUCATIVO AO ADOLESCENTE

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:

FUNDCASASPDCI202261966

Assinado com senha por SABRINA MIRANDA ARRAES DE CAMPOS - GERENTE ADMINISTRATIVO I / GCCCP - 21/07/2022 às 12:23:01, AURELIO OLIMPIO DE SOUZA - DIRETOR ADMINISTRATIVO / DGA - 21/07/2022 às 13:01:32, FERNANDO JOSÉ DA COSTA - PRESIDENTE / GP - 21/07/2022 às 13:03:16 e ROSANA MORENO PIRES - DIRETOR DE DIVISÃO I / DSUP - 21/07/2022 às 13:27:47.
Autenticado com senha por DANIELLA ALVES MAURICIO - ASSISTENTE TECNICO ADM I / SCO - 21/07/2022 às 11:39:04.
Documento Nº: 47591886-10 - consulta à autenticidade em
https://www.documentos.spsempapel.sp.gov.br/sigaex/public/app/autenticar?n=47591886-10

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;

V - observar, no tratamento de dados pessoais de profissionais, empregados, prepostos, administradores e/ou sócios da CONTRATADA, a que tenha acesso durante a execução do objeto a que se refere a Cláusula Primeira deste Contrato, as normas legais e regulamentares aplicáveis, em especial, a Lei Federal nº 13.709, de 14 de agosto de 2018, com suas alterações subsequentes.

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

FUNDCASASPDCI202261966

Assinado com senha por SABRINA MIRANDA ARRAES DE CAMPOS - GERENTE ADMINISTRATIVO I / GCCCP - 21/07/2022 às 12:23:01, AURELIO OLIMPIO DE SOUZA - DIRETOR ADMINISTRATIVO / DGA - 21/07/2022 às 13:01:32, FERNANDO JOSÉ DA COSTA - PRESIDENTE / GP - 21/07/2022 às 13:03:16 e ROSANA MORENO PIRES - DIRETOR DE DIVISÃO I / DSUP - 21/07/2022 às 13:27:47.
Autenticado com senha por DANIELLA ALVES MAURICIO - ASSISTENTE TECNICO ADM I / SCO - 21/07/2022 às 11:39:04.
Documento Nº: 47591886-10 - consulta à autenticidade em
https://www.documentos.spsempapel.sp.gov.br/sigaex/public/app/autenticar?n=47591886-10

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** 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$ 230,00 (duzentos e trinta reais) para o item 01, R$ 144.137,00 (centro e quarenta e quatro mil e centro e trinta e sete reais) para o item 02 e R$ 3.727,00 (três mil, setecentos e vinte e sete reais) para o item 03, perfazendo o total de R$ 1.201.499,00 (um milhão, duzentos e um mil, quatrocentos e noventa e nove 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
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 as Cláusulas deste instrumento.

I - A CONTRATADA deverá emitir nota fiscal eletrônica (Modelo 55), e/ou nota fiscal conjugada, nos termos das legislações vigentes. Tratando-se 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

FUNDCASASPDCI202261966

Assinado com senha por SABRINA MIRANDA ARRAES DE CAMPOS - GERENTE ADMINISTRATIVO I / GCCCP - 21/07/2022 às 12:23:01, AURELIO OLIMPIO DE SOUZA - DIRETOR ADMINISTRATIVO / DGA - 21/07/2022 às 13:01:32, FERNANDO JOSÉ DA COSTA - PRESIDENTE / GP - 21/07/2022 às 13:03:16 e ROSANA MORENO PIRES - DIRETOR DE DIVISÃO I / DSUP - 21/07/2022 às 13:27:47.
Autenticado com senha por DANIELLA ALVES MAURICIO - ASSISTENTE TECNICO ADM I / SCO - 21/07/2022 às 11:39:04.
Documento Nº: 47591886-10 - consulta à autenticidade em
https://www.documentos.spsempapel.sp.gov.br/sigaex/public/app/autenticar?n=47591886-10

eletrônica de prestação de serviço, em cumprimento ao que dispuser a legislação onde a Empresa estiver domiciliada/estabelecida, em nome da CONTRATANTE.

II - FUNDAÇÃO CASA/SP - inscrita no Cadastro Nacional de Pessoa Jurídica do Ministério da Fazenda sob nº 44.480.283/0001-91, situada na Rua Florêncio de Abreu, nº 848 – Bairro Luz – São Paulo/SP – CEP 01030-001.

PARÁGRAFO PRIMEIRO
A(s) nota(s) fiscal(is)/fatura(s) 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 SEGUNDO
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.

d) 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 nos pagamentos, incidirá correção monetária sobre o valor devido na forma da legislação aplicável, utilizando-se a “Tabela Prática do Tribunal de Justiça do Estado de São Paulo” ou outra ferramenta que lhe venha a substituir, 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 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 CONTRATADA, de que os registros estão suspensos, nos termos do artigo 8º da Lei Estadual nº 12.799/2008.

PARÁGRAFO QUINTO
Os pagamentos serão efetuados mediante crédito aberto em conta corrente em nome da CONTRATADA no Banco do Brasil S/A.

PARÁGRAFO SEXTO

FUNDCASASPDCI202261966

Assinado com senha por SABRINA MIRANDA ARRAES DE CAMPOS - GERENTE ADMINISTRATIVO I / GCCCP - 21/07/2022 às 12:23:01, AURELIO OLIMPIO DE SOUZA - DIRETOR ADMINISTRATIVO / DGA - 21/07/2022 às 13:01:32, FERNANDO JOSÉ DA COSTA - PRESIDENTE / GP - 21/07/2022 às 13:03:16 e ROSANA MORENO PIRES - DIRETOR DE DIVISÃO I / DSUP - 21/07/2022 às 13:27:47.
Autenticado com senha por DANIELLA ALVES MAURICIO - ASSISTENTE TECNICO ADM I / SCO - 21/07/2022 às 11:39:04.
Documento Nº: 47591886-10 - consulta à autenticidade em
https://www.documentos.spsempapel.sp.gov.br/sigaex/public/app/autenticar?n=47591886-10

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.

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.

FUNDCASASPDCI202261966

Assinado com senha por SABRINA MIRANDA ARRAES DE CAMPOS - GERENTE ADMINISTRATIVO I / GCCCP - 21/07/2022 às 12:23:01, AURELIO OLIMPIO DE SOUZA - DIRETOR ADMINISTRATIVO / DGA - 21/07/2022 às 13:01:32, FERNANDO JOSÉ DA COSTA - PRESIDENTE / GP - 21/07/2022 às 13:03:16 e ROSANA MORENO PIRES - DIRETOR DE DIVISÃO I / DSUP - 21/07/2022 às 13:27:47.
Autenticado com senha por DANIELLA ALVES MAURICIO - ASSISTENTE TECNICO ADM I / SCO - 21/07/2022 às 11:39:04.
Documento Nº: 47591886-10 - consulta à autenticidade em
https://www.documentos.spsempapel.sp.gov.br/sigaex/public/app/autenticar?n=47591886-10

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 ADMINISTRATIVAS
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/sancoes/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 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, de acordo com o previsto no Memorial Descritivo – Anexo I do edital e deste Termo de Contrato.

CLÁUSULA DÉCIMA QUINTA – DISPOSIÇÕES FINAIS
Fica ajustado, ainda, que:

FUNDCASASPDCI202261966

Assinado com senha por SABRINA MIRANDA ARRAES DE CAMPOS - GERENTE ADMINISTRATIVO I / GCCCP - 21/07/2022 às 12:23:01, AURELIO OLIMPIO DE SOUZA - DIRETOR ADMINISTRATIVO / DGA - 21/07/2022 às 13:01:32, FERNANDO JOSÉ DA COSTA - PRESIDENTE / GP - 21/07/2022 às 13:03:16 e ROSANA MORENO PIRES - DIRETOR DE DIVISÃO I / DSUP - 21/07/2022 às 13:27:47.
Autenticado com senha por DANIELLA ALVES MAURICIO - ASSISTENTE TECNICO ADM I / SCO - 21/07/2022 às 11:39:04.
Documento Nº: 47591886-10 - consulta à autenticidade em
https://www.documentos.spsempapel.sp.gov.br/sigaex/public/app/autenticar?n=47591886-10

FUNDAÇÃO CASA
CENTRO DE ATENDIMENTO SOCIOEDUCATIVO AO ADOLESCENTE

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 da Lei Federal nº 10.520/2002 e disposições regulamentares pertinentes, e, subsidiariamente, as disposições da Lei Federal nº 8.666/1993, da Lei Federal nº 8.078/1990 – Código de Defesa do Consumidor – e princípios gerais dos contratos.

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 01 (uma) via, que, lido e achado conforme pela CONTRATADA e pela CONTRATANTE, vai por elas assinado para que produza todos os efeitos de Direito, sendo assinado também pelas testemunhas abaixo identificadas.

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

Fernando José da Costa
Secretário da Justiça e Cidadania
Respondendo pelo Expediente da Fundação CASA

Aurélio Olímpio de Souza
Diretor Administrativo

CONTRATADA: DMK3 TECNOLOGIA LTDA

MIRELLA SAORI ROCHA KURATA:22034272803
Assinado de forma digital por MIRELLA SAORI ROCHA KURATA:22034272803
Dados: 2022.07.21 09:24:03 -03'00'

Mirella Saori Rocha Kurata
Sócia

TESTEMUNHAS:

Sabrina Miranda Cabral Arraes
Gerente Administrativo

Rosana Moreno Pires
Diretora de Divisão

FUNDCASASPDCI202261966

Assinado com senha por SABRINA MIRANDA ARRAES DE CAMPOS - GERENTE ADMINISTRATIVO I / GCCCP - 21/07/2022 às 12:23:01, AURELIO OLIMPIO DE SOUZA - DIRETOR ADMINISTRATIVO / DGA - 21/07/2022 às 13:01:32, FERNANDO JOSÉ DA COSTA - PRESIDENTE / GP - 21/07/2022 às 13:03:16 e ROSANA MORENO PIRES - DIRETOR DE DIVISÃO I / DSUP - 21/07/2022 às 13:27:47.
Autenticado com senha por DANIELLA ALVES MAURICIO - ASSISTENTE TECNICO ADM I / SCO - 21/07/2022 às 11:39:04.
Documento Nº: 47591886-10 - consulta à autenticidade em
https://www.documentos.spsempapel.sp.gov.br/sigaex/public/app/autenticar?n=47591886-10

FUNDAÇÃO CASA
CENTRO DE ATENDIMENTO SOCIOEDUCATIVO AO ADOLESCENTE

ANEXO I

MEMORIAL DESCRITIVO

Item	Descrição	Partnumber	Código BEC	Quantidade
1	Kaspersky Optimum Security Brazilian Edition. 2500-4999 Node 3 year Renewal Plus License	KL4709KAYT9	21600-3	4.500
2	Kaspersky Enhanced Support Brazilian Edition. 3 year Certificate	KL7122KLZTZ	336-0	1
3	Kaspersky Professional Services - 8 Hours, Remote Brazilian Edition. 5-9 Day 1 year Certificate.	KL7222K1EFZ	3055-4	6

1. Servidor de Administração e Console Administrativa

1.1. Compatibilidade:

1.1.1. Microsoft Windows Server 2012 Standard / Core / Foundation / Essentials / Datacenter x64;
1.1.2. Microsoft Storage Server 2012 e 2012 R2 x64;
1.1.3. Microsoft Windows Server 2012 R2 Standard / Core / Foundation / Essentials / Datacenter x64;
1.1.4. Microsoft Windows Server 2016 Standard / Core / Datacenter x64;
1.1.5. Microsoft Windows Server 2019 Standard / Core / Datacenter x64;
1.1.6. Microsoft Windows 7 SP1 Professional / Enterprise / Ultimate x32/x64;
1.1.7. Microsoft Windows 8 SP1 Professional / Enterprise x32/x64;
1.1.8. Microsoft Windows 8 Professional / Enterprise x64;
1.1.9. Microsoft Windows 8.1 Professional / Enterprise x32;
1.1.10. Microsoft Windows 8.1 Professional / Enterprise x64;
1.1.11. Microsoft Windows 10 x32;
1.1.12. Microsoft Windows 10 x64;
1.1.13. Windows 10 21H1 31-bit/64-bit;

1.2. Suporta as seguintes plataformas virtuais:

1.2.1. Vmware: Workstation 15.x Pro, vSphere 6.5, vSphere 6.7;
1.2.2. Microsoft Hyper-V: 2012, 2012 R2, 2016, 2019 x64;
1.2.5. Parallels Desktop 16;
1.2.7. Citrix XenServer 7.1;

1.3. Características:

1.3.1. A console deve ser acessada via WEB (HTTPS) ou MMC;
1.3.2. A console deve suportar arquitetura on-premise e arquitetura cloud-based;
1.3.3. Console deve ser baseada no modelo cliente/servidor;
1.3.4. A console deve suportar autenticação de dois fatores;
1.3.5. Compatibilidade com Windows Failover Clustering ou outra solução de alta disponibilidade;
1.3.6. Deve permitir a atribuição de perfis para os administradores da Solução de Antivírus;
1.3.7. Deve permitir incluir usuários do AD para logarem na console de administração
1.3.8. 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;

FUNDCASASPDCI202261966

Assinado com senha por SABRINA MIRANDA ARRAES DE CAMPOS - GERENTE ADMINISTRATIVO I / GCCCP - 21/07/2022 às 12:23:01, AURELIO OLIMPIO DE SOUZA - DIRETOR ADMINISTRATIVO / DGA - 21/07/2022 às 13:01:32, FERNANDO JOSÉ DA COSTA - PRESIDENTE / GP - 21/07/2022 às 13:03:16 e ROSANA MORENO PIRES - DIRETOR DE DIVISÃO I / DSUP - 21/07/2022 às 13:27:47.
Autenticado com senha por DANIELLA ALVES MAURICIO - ASSISTENTE TECNICO ADM I / SCO - 21/07/2022 às 11:39:04.
Documento Nº: 47591886-10 - consulta à autenticidade em
https://www.documentos.spsempapel.sp.gov.br/sigaex/public/app/autenticar?n=47591886-10

1.3.9. 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 da licença;
1.3.10. Capacidade de remover remotamente e automaticamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores;
1.3.11. Capacidade de instalar remotamente a solução de antivírus nas estações e servidores Windows, através de compartilhamento administrativo, através da console de gerenciamento e GPO de AD.
1.3.12. Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria;
1.3.13. Deve armazenar histórico das alterações feitas em políticas;
1.3.14. Deve permitir voltar para uma configuração antiga da política de acordo com o histórico de alterações efetuadas pelo administrador apenas selecionando a data em que a política foi alterada;
1.3.15. Deve ter a capacidade de comparar a política atual com a anterior, informando quais configurações foram alteradas;
1.3.16. A solução de gerencia deve permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas;
1.3.17. Através da solução de gerência, deve ser possível verificar qual licença está aplicada para determinado computador;
1.3.19. A solução de gerência centralizada deve permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle;
1.3.20. 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;
1.3.21. Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux e Mac) protegidos pela solução antivírus;
1.3.22. Capacidade de gerenciar smartphones e tablets (Android e iOS) protegidos pela solução de segurança;
1.3.23. Capacidade de instalar atualizações em computadores de teste antes de instalar nos demais computadores da rede;
1.3.24. Capacidade de gerar pacotes customizados (auto executáveis) contendo a licença e configurações do produto;
1.3.25. Capacidade de atualizar os pacotes de instalação com as últimas vacinas;
1.3.26. Capacidade de fazer distribuição remota de qualquer software, ou seja, deve ser capaz de remotamente enviar qualquer software pela estrutura de gerenciamento de antivírus para que seja instalado nas máquinas clientes;
1.3.27. A comunicação entre o cliente e o servidor de administração deve ser criptografada;
1.3.28. Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes;
1.3.29. Deve permitir a realocação de máquinas novas na rede para um determinado grupo sem ter um agente ou endpoint instalado utilizando os seguintes parâmetros:

- Nome do computador;
- Nome do domínio;
- Range de IP;
- Sistema Operacional;
- Máquina virtual.

1.3.30. Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas;
1.3.31. 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;

FUNDCASASPDCI202261966

Assinado com senha por SABRINA MIRANDA ARRAES DE CAMPOS - GERENTE ADMINISTRATIVO I / GCCCP - 21/07/2022 às 12:23:01, AURELIO OLIMPIO DE SOUZA - DIRETOR ADMINISTRATIVO / DGA - 21/07/2022 às 13:01:32, FERNANDO JOSÉ DA COSTA - PRESIDENTE / GP - 21/07/2022 às 13:03:16 e ROSANA MORENO PIRES - DIRETOR DE DIVISÃO I / DSUP - 21/07/2022 às 13:27:47.
Autenticado com senha por DANIELLA ALVES MAURICIO - ASSISTENTE TECNICO ADM I / SCO - 21/07/2022 às 11:39:04.
Documento Nº: 47591886-10 - consulta à autenticidade em
https://www.documentos.spsempapel.sp.gov.br/sigaex/public/app/autenticar?n=47591886-10

1.3.32. Capacidade de monitorar diferentes subnets de rede a fim de encontrar máquinas novas para serem adicionadas à proteção;
1.3.33. 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;
1.3.34. 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;
1.3.35. Capacidade de agrupamento de máquina por características comuns entre as mesmas, por exemplo: agrupar todas as máquinas que não tenham o antivírus instalado, agrupar todas as máquinas que não receberam atualização nos últimos 2 dias, etc;
1.3.36. 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;
1.3.37. Deve fornecer as seguintes informações dos computadores:
1.3.37.1. Se o antivírus está instalado;
1.3.37.2. Se o antivírus está iniciado;
1.3.37.3. Se o antivírus está atualizado;
1.3.37.4. Minutos/horas desde a última conexão da máquina com o servidor administrativo;
1.3.37.5. Minutos/horas desde a última atualização de vacinas;
1.3.37.6. Data e horário da última verificação executada na máquina;
1.3.37.7. Versão do antivírus instalado na máquina;
1.3.37.8. Se é necessário reiniciar o computador para aplicar mudanças;
1.3.37.9. Data e horário de quando a máquina foi ligada;
1.3.37.10. Quantidade de vírus encontrados (contador) na máquina;
1.3.37.11. Nome do computador;
1.3.37.12. Domínio ou grupo de trabalho do computador;
1.3.37.13. Data e horário da última atualização de vacinas;
1.3.37.14. Sistema operacional com Service Pack;
1.3.37.15. Quantidade de processadores;
1.3.37.16. Quantidade de memória RAM;
1.3.37.17. Sessões de usuários, com informações de contato (caso disponíveis no Active Directory);
1.3.37.18. Endereço IP;
1.3.37.21. Aplicativos instalados, inclusive aplicativos de terceiros, com histórico de instalação, contendo data e hora que o software foi instalado ou removido;
1.3.37.22. Informação completa de hardware contendo: processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de áudio, adaptadores de rede, monitores, drives de CD/DVD;
1.3.37.23. Vulnerabilidades de aplicativos instalados na máquina;
1.3.38. Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterá-las;
1.3.39. Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como:
1.3.39.1. Alteração de Gateway Padrão;
1.3.39.2. Alteração de subrede;
1.3.39.3. Alteração de domínio;
1.3.39.4. Alteração de servidor DHCP;
1.3.39.5. Alteração de servidor DNS;

FUNDCASASPDCI202261966

Assinado com senha por SABRINA MIRANDA ARRAES DE CAMPOS - GERENTE ADMINISTRATIVO I / GCCCP - 21/07/2022 às 12:23:01, AURELIO OLIMPIO DE SOUZA - DIRETOR ADMINISTRATIVO / DGA - 21/07/2022 às 13:01:32, FERNANDO JOSÉ DA COSTA - PRESIDENTE / GP - 21/07/2022 às 13:03:16 e ROSANA MORENO PIRES - DIRETOR DE DIVISÃO I / DSUP - 21/07/2022 às 13:27:47.
Autenticado com senha por DANIELLA ALVES MAURICIO - ASSISTENTE TECNICO ADM I / SCO - 21/07/2022 às 11:39:04.
Documento Nº: 47591886-10 - consulta à autenticidade em
https://www.documentos.spsempapel.sp.gov.br/sigaex/public/app/autenticar?n=47591886-10

1.3.39.6. Alteração de servidor WINS;
1.3.39.7. Alteração de subrede;
1.3.39.8. Resolução de Nome;
1.3.39.9. Disponibilidade de endereço de conexão SSL;
1.3.40. Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet;
1.3.41. Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes;
1.3.42. Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus;
1.3.43. A console de gerenciamento deve suportar funções de controle de acesso com base na função (RBAC) para a hierarquia de servidores. ;
1.3.44. Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos;
1.3.45. 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;
1.3.46. 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;
1.3.47. Capacidade de exportar relatórios para os seguintes tipos de arquivos: PDF, HTML e XML;
1.3.48. Capacidade de monitoramento do sistema através de um SNMP client;
1.3.49. Capacidade de enviar e-mails para contas específicas em caso de algum evento;
1.3.50. Listar em um único local, todos os computadores não gerenciados na rede;
1.3.51. Deve encontrar computadores na rede através de no mínimo três formas: Domínio, Active Directory e subredes;
1.3.52. Deve possuir compatibilidade com Microsoft NAP, quando instalado em um Windows 2008 Server;
1.3.53. Capacidade de baixar novas versões do antivírus direto pela console de gerenciamento, sem a necessidade de importá-los manualmente
1.3.54. 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;
1.3.55. Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado intervalo de tempo);
1.3.56. Deve através de opções de optimizações fazer com que o computador gerenciado conceda recursos à outras aplicações, mantendo o antivírus ativo porém sem comprometer o desempenho do computador;
1.3.57. Deve permitir a configuração de senha no endpoint e configurar quando que será necessário a utilizá-la, (ex: Solicitar senha quando alguma tarefa de scan for criada localmente no endpoint);
1.3.59. Deve ser capaz de configurar quais eventos serão armazenados localmente, nos eventos do windows ou ainda se serão mostrados na tela para o colaborador, sejam estes eventos informativos, de alertas ou de erros;
1.3.60. Capacidade de realizar atualização incremental de vacinas nos computadores clientes;
1.3.61. Deve armazenar localmente e enviar ao servidor de gerência a ocorrência de vírus com os seguintes dados, no mínimo:

FUNDCASASPDCI202261966

Assinado com senha por SABRINA MIRANDA ARRAES DE CAMPOS - GERENTE ADMINISTRATIVO I / GCCCP - 21/07/2022 às 12:23:01, AURELIO OLIMPIO DE SOUZA - DIRETOR ADMINISTRATIVO / DGA - 21/07/2022 às 13:01:32, FERNANDO JOSÉ DA COSTA - PRESIDENTE / GP - 21/07/2022 às 13:03:16 e ROSANA MORENO PIRES - DIRETOR DE DIVISÃO I / DSUP - 21/07/2022 às 13:27:47.
Autenticado com senha por DANIELLA ALVES MAURICIO - ASSISTENTE TECNICO ADM I / SCO - 21/07/2022 às 11:39:04.
Documento Nº: 47591886-10 - consulta à autenticidade em
https://www.documentos.spsempapel.sp.gov.br/sigaex/public/app/autenticar?n=47591886-10

- Nome do vírus;
- Nome do arquivo infectado;
- Data e hora da detecção;
- Nome da máquina ou endereço IP;
- Ação realizada.

1.3.62. Capacidade de reportar vulnerabilidades de softwares presentes nos computadores;
1.3.63. Capacidade de listar updates nas máquinas com o respectivo link para download
1.3.64. Deve criar um backup de todos arquivos deletados em computadores durante a desinfecção para que possam ser restaurados;
1.3.65. Deve ter uma quarentena na própria console de gerenciamento, permitindo baixar um artefato ou enviar direto para análise do fabricante;
1.3.66. Capacidade de realizar resumo de hardware de cada máquina cliente;
1.3.67. Capacidade de realizar resumo de hardware de cada máquina cliente;
1.3.68. Capacidade de diferenciar máquinas virtuais de máquinas físicas.

2. Estações Windows

2.1. Compatibilidade:

2.1.1. Microsoft Windows 7 Professional/Enterprise/Home SP1 x86 / x64;
2.1.2. Microsoft Windows 8 Professional/Enterprise x86 / x64;
2.1.3. Microsoft Windows 8.1 Professional / Enterprise x86 / x64;
2.1.4. Microsoft Windows 10 Pro / Enterprise / Home / Education x86 / x64;
2.1.5. Microsoft Windows Server 2019 Essentials / Standard / Datacenter;
2.1.6. Microsoft Windows Server 2016 Essentials / Standard / Datacenter;
2.1.7. Microsoft Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter;
2.1.8. Microsoft Windows Server 2012 Foundation / Essentials / Standard / Datacenter;
2.1.9. Microsoft Windows Server 2008 R2 Foundation / Essentials / Standard / Datacenter SP1;
2.1.10. Microsoft Windows Small Business Server 2011 Standard / Standard x64;
2.1.11. Microsoft Windows MultiPoint Server 2011 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. O Endpoint deve possuir opção para rastreamento por linha de comando, parametrizável, com opção de limpeza;
2.2.1.5. Firewall com IDS;
2.2.1.6. Autoproteção (contra-ataques aos serviços/processos do antivírus);
2.2.1.7. Controle de dispositivos externos;
2.2.1.8. Controle de acesso a sites por categoria, ex: Bloquear conteúdo adulto, sites de jogos, etc;
2.2.1.9. Controle de acesso a sites por horário;
2.2.1.10. Controle de acesso a sites por usuários;
2.2.1.11. Controle de acesso a websites por dados, ex: Bloquear websites com conteúdos de vídeo e áudio;
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;

FUNDCASASPDCI202261966

Assinado com senha por SABRINA MIRANDA ARRAES DE CAMPOS - GERENTE ADMINISTRATIVO I / GCCCP - 21/07/2022 às 12:23:01, AURELIO OLIMPIO DE SOUZA - DIRETOR ADMINISTRATIVO / DGA - 21/07/2022 às 13:01:32, FERNANDO JOSÉ DA COSTA - PRESIDENTE / GP - 21/07/2022 às 13:03:16 e ROSANA MORENO PIRES - DIRETOR DE DIVISÃO I / DSUP - 21/07/2022 às 13:27:47.
Autenticado com senha por DANIELLA ALVES MAURICIO - ASSISTENTE TECNICO ADM I / SCO - 21/07/2022 às 11:39:04.
Documento Nº: 47591886-10 - consulta à autenticidade em
https://www.documentos.spsempapel.sp.gov.br/sigaex/public/app/autenticar?n=47591886-10

2.2.3. As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa);
2.2.4. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;
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. Deverá possuir módulo dedicado para proteção contra port scanning;
2.2.8. Deverá possuir módulo dedicado para proteção contra network flooding;
2.2.9. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);
2.2.10. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
2.2.11. 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;
2.2.12. Ter a capacidade de fazer detecções por comportamento, identificando ameaças avançadas sem a necessidade de assinaturas;
2.2.13. Ao detectar uma ameaça, a solução deve exibir informações:
2.2.13.1. Do objeto SHA256;
2.2.13.2. Do objeto MD5.
2.2.14. Capacidade de verificar somente arquivos novos e alterados;
2.2.15. Capacidade de verificar objetos usando heurística;
2.2.16. Capacidade de agendar uma pausa na verificação;
2.2.17. Deve permitir a filtragem de conteúdo de URL avançada efetuando a classificação dos sites em categorias;
2.2.18. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;
2.2.19. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
2.2.19.1. Perguntar o que fazer, ou;
2.2.19.2. Bloquear acesso ao objeto;
2.2.19.2.1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
2.2.19.2.2. Caso positivo de desinfecção:
2.2.19.2.2.1. Restaurar o objeto para uso;
2.2.19.2.3. Caso negativo de desinfecção:
2.2.19.2.3.1. Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);
2.2.20. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
2.2.21. Capacidade de verificar e-mails recebidos e enviados nos protocolos POP3, POP3S, IMAP, NNTP, SMTP e MAPI;
2.2.22. Capacidade de verificar links inseridos em e-mails contra phishings;
2.2.23. Capacidade de verificar tráfego nos browsers: Internet Explorer, Firefox, Google Chrome e Opera;
2.2.24. Capacidade de verificação de corpo e anexos de e-mails usando heurística;

FUNDCASASPDCI202261966

Assinado com senha por SABRINA MIRANDA ARRAES DE CAMPOS - GERENTE ADMINISTRATIVO I / GCCCP - 21/07/2022 às 12:23:01, AURELIO OLIMPIO DE SOUZA - DIRETOR ADMINISTRATIVO / DGA - 21/07/2022 às 13:01:32, FERNANDO JOSÉ DA COSTA - PRESIDENTE / GP - 21/07/2022 às 13:03:16 e ROSANA MORENO PIRES - DIRETOR DE DIVISÃO I / DSUP - 21/07/2022 às 13:27:47.
Autenticado com senha por DANIELLA ALVES MAURICIO - ASSISTENTE TECNICO ADM I / SCO - 21/07/2022 às 11:39:04.
Documento Nº: 47591886-10 - consulta à autenticidade em
https://www.documentos.spsempapel.sp.gov.br/sigaex/public/app/autenticar?n=47591886-10

2.2.25. O antivírus de e-mail, ao encontrar um objeto potencialmente perigoso, deve:
2.2.25.1. Perguntar o que fazer, ou;
2.2.25.2. Bloquear o e-mail;
2.2.25.2.1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
2.2.25.2.2. Caso positivo de desinfecção:
2.2.25.2.2.1. Restaurar o e-mail para o usuário;
2.2.25.2.3. Caso negativo de desinfecção:
2.2.25.2.3.1. Mover para quarentena ou apagar o objeto (de acordo com a configuração pré-estabelecida pelo administrador);
2.2.27. Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados;
2.2.28. Capacidade de filtrar anexos de e-mail, apagando-os ou renomeando-os de acordo com a configuração feita pelo administrador;
2.2.29. Capacidade de verificação de tráfego HTTP/HTTPS e qualquer script do Windows Script Host (JavaScript, Visual Basic Script, etc), usando heurísticas;
2.2.31. Capacidade de alterar as portas monitoradas pelos módulos de Web e E-mail;
2.2.32. Na verificação de tráfego web, caso encontrado código malicioso o programa deve:
2.2.32.1. Perguntar o que fazer, ou;
2.2.32.2. Bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio, ou;
2.2.32.3. Permitir acesso ao objeto;
2.2.33. O antivírus de web deve realizar a verificação de, no mínimo, duas maneiras diferentes, sob escolha do administrador:
2.2.33.1. Verificação *on-the-fly*, onde os dados são verificados enquanto são recebidos em tempo-real, ou;
2.2.33.2. Verificação de *buffer*, onde os dados são recebidos e armazenados para posterior verificação;
2.2.34. Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus de web;
2.2.35. Deve possuir módulo que analise as ações de cada aplicação em execução no computador, gravando as ações executadas e comparando-as com sequências características de atividades perigosas. Tais registros de sequências devem ser atualizados juntamente com as vacinas;
2.2.37. 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;
2.2.38. Deve possuir módulo de bloqueio de *Phishing*, com atualizações incluídas nas vacinas, obtidas pelo *Anti-Phishing Working Group* (http://www.antiphishing.org/);
2.2.39. Capacidade de distinguir diferentes subnets e conceder opção de ativar ou não o firewall para uma subnet específica;
2.2.40. 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;
2.2.41. Deve permitir a importação e exportação de listas de regras e exclusões para as aplicações no formato XML;
2.2.42. Deve permitir a criação de zonas confiáveis locais independentes por parte do usuário.
2.2.43. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:
2.2.43.1. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;
2.2.43.2. Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá

FUNDCASASPDCI202261966

Assinado com senha por SABRINA MIRANDA ARRAES DE CAMPOS - GERENTE ADMINISTRATIVO I / GCCCP - 21/07/2022 às 12:23:01, AURELIO OLIMPIO DE SOUZA - DIRETOR ADMINISTRATIVO / DGA - 21/07/2022 às 13:01:32, FERNANDO JOSÉ DA COSTA - PRESIDENTE / GP - 21/07/2022 às 13:03:16 e ROSANA MORENO PIRES - DIRETOR DE DIVISÃO I / DSUP - 21/07/2022 às 13:27:47.
Autenticado com senha por DANIELLA ALVES MAURICIO - ASSISTENTE TECNICO ADM I / SCO - 21/07/2022 às 11:39:04.
Documento Nº: 47591886-10 - consulta à autenticidade em
https://www.documentos.spsempapel.sp.gov.br/sigaex/public/app/autenticar?n=47591886-10

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

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

2.2.44.1. Discos de armazenamento locais;
2.2.44.2. Armazenamento removível;
2.2.44.3. Impressoras;
2.2.44.4. CD/DVD;
2.2.44.5. Drives de disquete;
2.2.44.6. Modems;
2.2.44.7. Dispositivos de fita;
2.2.44.8. Dispositivos multifuncionais;
2.2.44.9. Leitores de smart card;
2.2.44.10. Dispositivos de sincronização via ActiveSync (Windows CE, Windows Mobile, etc);
2.2.44.11. Wi-Fi;
2.2.44.12. Adaptadores de rede externos;
2.2.44.13. Dispositivos MP3 ou smartphones;
2.2.44.14. Dispositivos Bluetooth;
2.2.44.15. Câmeras e Scanners.

2.2.45. 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;

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

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

2.2.48. Deve permitir controlar o acesso a dispositivos externos com base em prioridade de regras.

2.2.49. Capacidade de habilitar “logging” em dispositivos removíveis tais como Pendrive, Discos externos, etc.

2.2.50. Capacidade de configurar novos dispositivos por Class ID/Hardware ID;

2.2.51. 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);

2.2.52. O controle de aplicações deve ter a capacidade de criar regras seguindo os seguintes modos de operação:

2.2.52.1. Black list: Permite a execução de qualquer aplicação, exceto pelas especificadas por regras.
2.2.52.2. White list: Impede a execução de qualquer aplicação, exceto pelas especificadas por regras.

2.2.53. Capacidade de bloquear execução de aplicativo que está em armazenamento externo;

2.2.54. 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;

2.2.55. 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;

FUNDCASASPDCI202261966

Assinado com senha por SABRINA MIRANDA ARRAES DE CAMPOS - GERENTE ADMINISTRATIVO I / GCCCP - 21/07/2022 às 12:23:01, AURELIO OLIMPIO DE SOUZA - DIRETOR ADMINISTRATIVO / DGA - 21/07/2022 às 13:01:32, FERNANDO JOSÉ DA COSTA - PRESIDENTE / GP - 21/07/2022 às 13:03:16 e ROSANA MORENO PIRES - DIRETOR DE DIVISÃO I / DSUP - 21/07/2022 às 13:27:47.
Autenticado com senha por DANIELLA ALVES MAURICIO - ASSISTENTE TECNICO ADM I / SCO - 21/07/2022 às 11:39:04.
Documento Nº: 47591886-10 - consulta à autenticidade em
https://www.documentos.spsempapel.sp.gov.br/sigaex/public/app/autenticar?n=47591886-10

2.2.56. 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.
2.2.57. Capacidade de voltar ao estado anterior do sistema operacional após um ataque de malware.
2.2.58. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros.
2.2.59. Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning).
2.2.60. Capacidade de integração com o Windows Defender Security Center.
2.2.61. Capacidade de integração com a Antimalware Scan Interface (AMSI).
2.2.63. Deve permitir sincronização com soluções de terceiros por meio de API.
2.2.64. Deve permitir o gerenciamento remoto da solução por meio de aplicativos de administração remota.

3. Estações Mac OS X
3.1. Compatibilidade:
3.1.1. macOS Catalina 10.15
3.1.2. macOS Mojave 10.14
3.1.3. masOS High Sierra 10.13
3.1.4. macOS Sierra 10.12
3.1.5. macOS 11.0 Big Sur
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. Possuir módulo de web-antivírus para proteger contra ameaças durante navegação na internet com possíbilidade de analisar endereços https;
3.2.3. Possuir módulo de bloqueio á ataques na rede;
3.2.4. Possibilidade de bloquear a comunicação entre a máquina atacante e os demais computadores por tempo definido pelo administrador;
3.2.5. Capacidade de criar exclusões para computadores que não devem ser monitorados pelo módulo de bloqueio à ataques na rede;
3.2.6. Possibilidade de importar uma chave no pacote de instalação;
3.2.7. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
3.2.8. As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa);
3.2.9. Capacidade de voltar para a base de dados de vacina anterior;
3.2.11. 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;
3.2.12. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);
3.2.13. 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;
3.2.14. Capacidade de verificar somente arquivos novos e alterados;
3.2.15. Capacidade de verificar objetos usando heurística;
3.2.16. Capacidade de agendar uma pausa na verificação;

FUNDCASASPDCI202261966

Assinado com senha por SABRINA MIRANDA ARRAES DE CAMPOS - GERENTE ADMINISTRATIVO I / GCCCP - 21/07/2022 às 12:23:01, AURELIO OLIMPIO DE SOUZA - DIRETOR ADMINISTRATIVO / DGA - 21/07/2022 às 13:01:32, FERNANDO JOSÉ DA COSTA - PRESIDENTE / GP - 21/07/2022 às 13:03:16 e ROSANA MORENO PIRES - DIRETOR DE DIVISÃO I / DSUP - 21/07/2022 às 13:27:47.
Autenticado com senha por DANIELLA ALVES MAURICIO - ASSISTENTE TECNICO ADM I / SCO - 21/07/2022 às 11:39:04.
Documento Nº: 47591886-10 - consulta à autenticidade em
https://www.documentos.spsempapel.sp.gov.br/sigaex/public/app/autenticar?n=47591886-10

3.2.17. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
3.2.17.1. Perguntar o que fazer, ou;
3.2.17.2. Bloquear acesso ao objeto;
3.2.17.2.1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
3.2.17.2.2. Caso positivo de desinfecção:
3.2.17.2.2.1. Restaurar o objeto para uso;
3.2.17.2.3. Caso negativo de desinfecção:
3.2.17.2.3.1. Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);
3.2.18. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
3.2.19. Capacidade de verificar arquivos de formato de email;
3.2.20. 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;
3.2.21. Capacidade de, através da mesma console central de gerenciamento:
3.2.21.1. Ser instalado;
3.2.21.2. Ser removido;
3.2.21.3. Ser gerenciado;

4. Estações de trabalho Linux
4.1. Compatibilidade:
4.1.1. Plataforma 32-bits:
4.1.1.1. Ubuntu 16.04 LTS;
4.1.1.2. Red Hat® Enterprise Linux® 6.7 Server;
4.1.1.3. CentOS 6.7;
4.1.1.4. Debian GNU / Linux 9.4 ;
4.1.1.5. Debian GNU / Linux 10;
4.1.1.6. Linux Mint 18.2;
4.1.1.7. Linux Mint 19;
4.1.1.8. GosLinux 6.6;
4.1.1.9. Mageia 4;
4.1.1.10. OS Lotos ;
4.1.2. Plataforma 64-bits:
4.1.2.1. Ubuntu 16.04 LTS;
4.1.2.2. Ubuntu 18.04 LTS;
4.1.2.3. Red Hat Enterprise Linux 6.7;
4.1.2.4. Red Hat Enterprise Linux 7.2;
4.1.2.5. Red Hat Enterprise Linux 8.0;
4.1.2.6. CentOS 6.7;
4.1.2.7. CentOS 7.2;
4.1.2.8. CentOS 8.0;
4.1.2.9. Debian GNU / Linux 9.4
4.1.2.10. Debian GNU / Linux 10.1;
4.1.2.11. OracleLinux 7.3;
4.1.2.12. OracleLinux 8;
4.1.2.13. SUSE® Linux Enterprise Server 15;
4.1.2.14. openSUSE® Leap 15;
4.1.2.15. Amazon Linux AMI
4.1.2.16. Linux Mint 18.2;

FUNDCASASPDCI202261966

Assinado com senha por SABRINA MIRANDA ARRAES DE CAMPOS - GERENTE ADMINISTRATIVO I / GCCCP - 21/07/2022 às 12:23:01, AURELIO OLIMPIO DE SOUZA - DIRETOR ADMINISTRATIVO / DGA - 21/07/2022 às 13:01:32, FERNANDO JOSÉ DA COSTA - PRESIDENTE / GP - 21/07/2022 às 13:03:16 e ROSANA MORENO PIRES - DIRETOR DE DIVISÃO I / DSUP - 21/07/2022 às 13:27:47.
Autenticado com senha por DANIELLA ALVES MAURICIO - ASSISTENTE TECNICO ADM I / SCO - 21/07/2022 às 11:39:04.
Documento Nº: 47591886-10 - consulta à autenticidade em
https://www.documentos.spsempapel.sp.gov.br/sigaex/public/app/autenticar?n=47591886-10

4.1.2.17. Linux Mint 19;
4.1.2.18. GosLinux 6.6
4.1.2.19. GosLinux 7.2
4.1.2.20. Oracle Linux 6.7;
4.1.2.21. SUSE Linux Enterprise Server 12 SP3;
4.1.2.22. Pardus OS 19.1;
4.1.2.23. RED OS 7.2;

4.2. Características:

4.2.1. Deve prover as seguintes proteções:
4.2.2. Antivírus de arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
4.2.3. Deve permitir gerenciamento, no mínimo, das seguintes formas:
4.2.3.1. Via linha de comando;
4.2.3.2. Via console administrativa;
4.2.3.3. Via GUI;
4.2.3.4. Via web (remotamente);
4.2.4. Deve possuir funcionalidade de scan de drives removíveis, tais como:
4.2.4.1. CDs;
4.2.4.2. DVDs;
4.2.4.3. Discos blu-ray;
4.2.4.4. Flash drives (pen drives);
4.2.4.5. HDs externos;
4.2.4.6. Disquetes;
4.2.5. Deve fornecer os seguintes controles para dispositivos externos conectados ao computador:
4.2.5.1. Por tipo de dispositivo;
4.2.5.2. Por barramento de conexão.
4.2.6. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;
4.2.7. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
4.2.8. Capacidade de criar exclusões por local, máscara e nome da ameaça;
4.2.9. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
4.2.10. 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;
4.2.11. Dectectar aplicações que possam ser utilizadas como vetor de ataque por hackers;
4.2.12. Fazer detecções através de heurística utilizando no mínimo as seguintes opções de nível:
4.2.12.1. Alta;
4.2.12.2. Média;
4.2.12.3. Baixa;
4.2.12.4. Recomendado;
4.2.13. Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;
4.2.14. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados.
4.2.15. Em caso erros, deve ter capacidade de criar *logs* automaticamente, sem necessidade de outros softwares;
4.2.16. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;

FUNDCASASPDCI202261966

Assinado com senha por SABRINA MIRANDA ARRAES DE CAMPOS - GERENTE ADMINISTRATIVO I / GCCCP - 21/07/2022 às 12:23:01, AURELIO OLIMPIO DE SOUZA - DIRETOR ADMINISTRATIVO / DGA - 21/07/2022 às 13:01:32, FERNANDO JOSÉ DA COSTA - PRESIDENTE / GP - 21/07/2022 às 13:03:16 e ROSANA MORENO PIRES - DIRETOR DE DIVISÃO I / DSUP - 21/07/2022 às 13:27:47.
Autenticado com senha por DANIELLA ALVES MAURICIO - ASSISTENTE TECNICO ADM I / SCO - 21/07/2022 às 11:39:04.
Documento Nº: 47591886-10 - consulta à autenticidade em
https://www.documentos.spsempapel.sp.gov.br/sigaex/public/app/autenticar?n=47591886-10

4.2.18. Capacidade de verificar objetos usando heurística;
4.2.19. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;
4.2.20. Deve fornecer análise de todo o tráfego HTTP/HTTPS/FTP que chegar no computador do usuário.
4.2.21. O módulo de análise de tráfego deve fornecer os seguintes componentes de proteção:
4.2.21.1. Detecção de phishing e sites maliciosos;
4.2.21.2. Bloqueio de download de arquivos maliciosos;
4.2.21.3. Bloqueio de adware;
4.2.22. Deve possuir módulo escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;
4.2.23. Deve fornecer a possibilidade de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).
4.2.24. Deve possuir módulo de proteção contra criptografia maliciosa.

5. Servidores Windows
5.1. Compatibilidade:
5.2. Plataforma 32-bits:
5.2.1. Windows Server 2003 Standard/Enterprise/Datacenter SP2 e posterior;
5.2.2. Windows Server 2003 R2 Standard/Enterprise/Datacenter SP2 e posterior;
5.2.3. Windows Server 2008 Standard/Enterprise/Datacenter SP1 e posterior;
5.2.4. Windows Server 2008 Core Standard/Enterprise/Datacenter SP1 e posterior;
5.3. Plataforma 64-bits
5.3.1. Windows Server 2003 Standard/Enterprise/Datacenter SP2 e posterior;
5.3.2. Windows Server 2003 R2 Standard/Enterprise/Datacenter SP2 e posterior;
5.3.3. Microsoft Windows Server 2008 Standard / Enterprise / DataCenter SP1 ou posterior;
5.3.4. Microsoft Windows Server 2008 Core Standard / Enterprise / DataCenter SP1 ou posterior.
5.3.5. Microsoft Windows Server 2008 R2 Foundation / Standard / Enterprise / DataCenter SP1 ou posterior;
5.3.6. Microsoft Windows Server 2008 R2 Core Standard / Enterprise / DataCenter SP1 ou posterior;
5.3.7. Microsoft Small Business Server 2008 Standard / Premium
5.3.8. Microsoft Windows Hyper-V Server 2008 R2 SP1 e posterior;
5.3.9. Microsoft Microsoft Small Business Server 2011 Essentials / Standard
5.3.10. Microsoft Windows MultiPoint Server 2011;
5.3.11. Microsoft MultiPoint Server 2012 Standard / Premium;
5.3.12. Microsoft Windows MultiPoint Server 2016
5.3.13. Windows 10 Enterprise multi-session;
5.3.14. Microsoft Windows Server 2012 Essentials / Standard / Foundation / Datacenter;
5.3.15. Microsoft Windows Server 2012 R2 Essentials / Standard / Foundation / Datacenter;
5.3.16. Microsoft Windows Server 2012 Core Standard / Datacenter;
5.3.17. Microsoft Windows Server 2012 R2 Core Standard / Datacenter;
5.3.18. Microsoft Windows Storage Server 2012;
5.3.19. Microsoft Windows Storage Server 2012 R2;
5.3.20. Microsoft Windows Hyper-V Server 2012;
5.3.21. Microsoft Windows Hyper-V Server 2012 R2;
5.3.22. Windows Server 2016 Essentials /Standard / Datacenter;
5.3.23. Windows Server 2016 Core Standard / Datacenter;
5.3.24. Windows Storage Server 2016;

FUNDCASASPDCI202261966

Assinado com senha por SABRINA MIRANDA ARRAES DE CAMPOS - GERENTE ADMINISTRATIVO I / GCCCP - 21/07/2022 às 12:23:01, AURELIO OLIMPIO DE SOUZA - DIRETOR ADMINISTRATIVO / DGA - 21/07/2022 às 13:01:32, FERNANDO JOSÉ DA COSTA - PRESIDENTE / GP - 21/07/2022 às 13:03:16 e ROSANA MORENO PIRES - DIRETOR DE DIVISÃO I / DSUP - 21/07/2022 às 13:27:47.
Autenticado com senha por DANIELLA ALVES MAURICIO - ASSISTENTE TECNICO ADM I / SCO - 21/07/2022 às 11:39:04.
Documento Nº: 47591886-10 - consulta à autenticidade em
https://www.documentos.spsempapel.sp.gov.br/sigaex/public/app/autenticar?n=47591886-10

5.3.25. Windows Storage Server 2019;
5.3.26. Windows Hyper-V Server 2016;
5.3.27. Windows Hyper-V Server 2019;
5.3.28. Windows Server 2019 Essentials / Standard / Datacenter / Core / Terminal;

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;
5.4.1.3. Firewall com IDS;
5.4.1.4. Controle de vulnerabilidades do Windows e dos aplicativos instalados;
5.4.2. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
5.4.3. Deve permitir gerenciamento, no mínimo, das seguintes formas:
5.4.3.1. Via console administrativa;
5.4.3.2. Via web (remotamente);
5.4.4. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;
5.4.5. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
5.4.5.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
5.4.5.2. Gerenciamento de tarefa (criar ou excluir tarefas de verificação);
5.4.5.3. Leitura de configurações;
5.4.5.4. Modificação de configurações;
5.4.5.5. Gerenciamento de Backup e Quarentena;
5.4.5.6. Visualização de logs;
5.4.5.7. Gerenciamento de logs;
5.4.5.8. Gerenciamento de ativação da aplicação;
5.4.5.9. Gerenciamento de permissões (adicionar/excluir permissões acima);
5.4.5.10. Deve possuir bloqueio de inicialização de aplicativos baseado em whitelists.
5.4.6. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:
5.4.6.1. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;
5.4.6.2. 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.
5.4.7. 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;
5.4.8. Bloquear malwares tais como Cryptlockers mesmo quando o ataque vier de um computador sem antivírus na rede
5.4.9. Capacidade de resumir automaticamente tarefas de verificação que tenham sido paradas por anormalidades (queda de energia, erros, etc);
5.4.10. Em caso de erros, deve ter capacidade de criar *logs* e *traces* automaticamente, sem necessidade de outros softwares;
5.4.11. Deve possuir funcionalidade de análise personalizada de logs do Windows.
5.4.12. Capacidade de configurar níveis de verificação diferentes para cada pasta, grupo de pastas ou arquivos do servidor;
5.4.13. Capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado no servidor;

FUNDCASASPDCI202261966

Assinado com senha por SABRINA MIRANDA ARRAES DE CAMPOS - GERENTE ADMINISTRATIVO I / GCCCP - 21/07/2022 às 12:23:01, AURELIO OLIMPIO DE SOUZA - DIRETOR ADMINISTRATIVO / DGA - 21/07/2022 às 13:01:32, FERNANDO JOSÉ DA COSTA - PRESIDENTE / GP - 21/07/2022 às 13:03:16 e ROSANA MORENO PIRES - DIRETOR DE DIVISÃO I / DSUP - 21/07/2022 às 13:27:47.
Autenticado com senha por DANIELLA ALVES MAURICIO - ASSISTENTE TECNICO ADM I / SCO - 21/07/2022 às 11:39:04.
Documento Nº: 47591886-10 - consulta à autenticidade em
https://www.documentos.spsempapel.sp.gov.br/sigaex/public/app/autenticar?n=47591886-10

5.4.14. Capacidade de criar uma lista de máquina que nunca serão bloqueadas mesmo quando infectadas;
5.4.15. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;
5.4.16. 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;
5.4.18. 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;
5.4.19. Capacidade de verificar somente arquivos novos e alterados;
5.4.20. Capacidade de escolher qual tipo de objeto composto será verificado (ex: arquivos comprimidos, arquivos auto descompressores, .PST, arquivos compactados por compactadores binários, etc.);
5.4.21. Capacidade de verificar objetos usando heurística;
5.4.22. Capacidade de configurar diferentes ações para diferentes tipos de ameaças;
5.4.23. Capacidade de agendar uma pausa na verificação;
5.4.25. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
5.4.25.1. Perguntar o que fazer, ou;
5.4.25.2. Bloquear acesso ao objeto;
5.4.25.2.1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
5.4.25.2.2. Caso positivo de desinfecção:
5.4.25.2.2.1. Restaurar o objeto para uso;
5.4.25.2.3. Caso negativo de desinfecção:
5.4.25.2.3.1. Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);
5.4.26. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
5.4.27. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;
5.4.28. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;
5.4.29. Em caso de detecção de sinais de de uma infecção ativa, deve possuir capacidade de, automaticamente:
5.4.29.1. Executar os procedimentos pré-configurados pelo administrador;
5.4.29.2. Em caso de ausência de procedimentos pré-configurados, criar tais procedimentos e executá-los.
5.4.30. Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa.
5.4.31. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros
5.4.32. Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning).
5.4.33. Capacidade de bloquear a criptografia de arquivos em pastas compartilhadas, após a execução de um malware em um dispositivo que possua o mapeamento da pasta.
5.4.34. Deve possuir controle de dispositivos externos.

6. Servidores Linux
6.1. Compatibilidade:

FUNDCASASPDCI202261966

Assinado com senha por SABRINA MIRANDA ARRAES DE CAMPOS - GERENTE ADMINISTRATIVO I / GCCCP - 21/07/2022 às 12:23:01, AURELIO OLIMPIO DE SOUZA - DIRETOR ADMINISTRATIVO / DGA - 21/07/2022 às 13:01:32, FERNANDO JOSÉ DA COSTA - PRESIDENTE / GP - 21/07/2022 às 13:03:16 e ROSANA MORENO PIRES - DIRETOR DE DIVISÃO I / DSUP - 21/07/2022 às 13:27:47.
Autenticado com senha por DANIELLA ALVES MAURICIO - ASSISTENTE TECNICO ADM I / SCO - 21/07/2022 às 11:39:04.
Documento Nº: 47591886-10 - consulta à autenticidade em
https://www.documentos.spsempapel.sp.gov.br/sigaex/public/app/autenticar?n=47591886-10

6.1.1. Plataforma 32-bits:
6.1.1.1. Ubuntu 16.04 LTS;
6.1.1.2. Red Hat® Enterprise Linux® 6.7 Server;
6.1.1.3. CentOS 6.7;
6.1.1.4. Debian GNU / Linux 9.4 ;
6.1.1.5. Debian GNU / Linux 10;
6.1.1.6. Linux Mint 18.2;
6.1.1.7. Linux Mint 19;
6.1.1.8. GosLinux 6.6;
6.1.1.9. Mageia 4;
6.1.1.10. OS Lotos ;
6.1.2. Plataforma 64-bits:
6.1.2.1. Ubuntu 16.04 LTS;
6.1.2.2. Ubuntu 18.04 LTS;
6.1.2.3. Red Hat Enterprise Linux 6.7;
6.1.2.4. Red Hat Enterprise Linux 7.2;
6.1.2.5. Red Hat Enterprise Linux 8.0;
6.1.2.6. CentOS 6.7;
6.1.2.7. CentOS 7.2;
6.1.2.8. CentOS 8.0;
6.1.2.9. Debian GNU / Linux 9.4
6.1.2.10. Debian GNU / Linux 10.1;
6.1.2.11. OracleLinux 7.3;
6.1.2.12. OracleLinux 8;
6.1.2.13. SUSE® Linux Enterprise Server 15;
6.1.2.14. openSUSE® Leap 15;
6.1.2.15. Amazon Linux AMI
6.1.2.16. Linux Mint 18.2;
6.1.2.17. Linux Mint 19;
6.1.2.18. GosLinux 6.6
6.1.2.19. GosLinux 7.2
6.2. Características:
6.2.1. Deve prover as seguintes proteções:
6.2.2. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
6.2.3. Deve permitir gerenciamento, no mínimo, das seguintes formas:
6.2.3.1. Via linha de comando;
6.2.3.2. Via console administrativa;
6.2.3.3. Via GUI;
6.2.3.4. Via web;
6.2.4. Deve possuir funcionalidade de scan de drives removíveis, tais como:
6.2.4.1. CDs;
6.2.4.2. DVDs;
6.2.4.3. Discos Blu-ray;
6.2.4.4. Flash drives;
6.2.4.5. HDs externos;
6.2.4.6. Disquetes;
6.2.5. Deve fornecer os seguintes controles para dispositivos externos conectados ao computador:
6.2.5.1. Por tipo de dispositivo;
6.2.5.2. Por barramento de conexão.

FUNDCASASPDCI202261966

Assinado com senha por SABRINA MIRANDA ARRAES DE CAMPOS - GERENTE ADMINISTRATIVO I / GCCCP - 21/07/2022 às 12:23:01, AURELIO OLIMPIO DE SOUZA - DIRETOR ADMINISTRATIVO / DGA - 21/07/2022 às 13:01:32, FERNANDO JOSÉ DA COSTA - PRESIDENTE / GP - 21/07/2022 às 13:03:16 e ROSANA MORENO PIRES - DIRETOR DE DIVISÃO I / DSUP - 21/07/2022 às 13:27:47.
Autenticado com senha por DANIELLA ALVES MAURICIO - ASSISTENTE TECNICO ADM I / SCO - 21/07/2022 às 11:39:04.
Documento Nº: 47591886-10 - consulta à autenticidade em
https://www.documentos.spsempapel.sp.gov.br/sigaex/public/app/autenticar?n=47591886-10

6.2.6. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;
6.2.7. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
6.2.8. 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;
6.2.9. Gerenciamento de Quarentena: Deve bloquear objetos suspeitos;
6.2.10. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados);
6.2.11. Em caso erros, deve ter capacidade de criar *logs* automaticamente, sem necessidade de outros softwares;
6.2.12. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
6.2.13. Capacidade de verificar objetos usando heurística;
6.2.14. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;
6.2.15. Fazer detecções através de heurística utilizando no mínimo as seguintes opções de nível:
6.2.15.1. Alta;
6.2.15.2. Média;
6.2.15.3. Baixa;
6.2.15.4. Recomendado;
6.2.16. Deve fornecer análise de todo o tráfego HTTP/HTTPS/FTP que chegar no computador do usuário.
6.2.17. O módulo de análise de tráfego deve fornecer os seguintes componentes de proteção:
6.2.17.1. Detecção de phishing e sites maliciosos;
6.2.17.2. Bloqueio de download de arquivos maliciosos;
6.2.17.3. Bloqueio de adware;
6.2.18. Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).
6.2.19. Deve possuir módulo de proteção contra criptografia maliciosa.

7. Smartphones e tablets
7.1. Compatibilidade:
7.1.1. Dispositivos com os sistemas operacionais:
7.1.1.1. Android 5.0 – 5.1.1
7.1.1.2. Android 6.0 – 6.0.1
7.1.1.3. Android 7.0 – 7.12
7.1.1.4. Android 8.0 – 8.1
7.1.1.5. Android 9.0
7.1.1.6. Android 10.0
7.2. Características:
7.2.1. Deve prover as seguintes proteções:
7.2.1.1. Proteção em tempo real do sistema de arquivos do dispositivo – interceptação e verificação de:
7.2.1.2. Proteção contra adware e autodialers;
7.2.1.3. Todos os objetos transmitidos usando conexões wireless (porta de infravermelho, Bluetooth) e mensagens EMS, durante sincronismo com PC e ao realizar download usando o browser;
7.2.1.4. Arquivos abertos no smartphone;
7.2.1.5. Programas instalados usando a interface do smartphone

FUNDCASASPDCI202261966

Assinado com senha por SABRINA MIRANDA ARRAES DE CAMPOS - GERENTE ADMINISTRATIVO I / GCCCP - 21/07/2022 às 12:23:01, AURELIO OLIMPIO DE SOUZA - DIRETOR ADMINISTRATIVO / DGA - 21/07/2022 às 13:01:32, FERNANDO JOSÉ DA COSTA - PRESIDENTE / GP - 21/07/2022 às 13:03:16 e ROSANA MORENO PIRES - DIRETOR DE DIVISÃO I / DSUP - 21/07/2022 às 13:27:47.
Autenticado com senha por DANIELLA ALVES MAURICIO - ASSISTENTE TECNICO ADM I / SCO - 21/07/2022 às 11:39:04.
Documento Nº: 47591886-10 - consulta à autenticidade em
https://www.documentos.spsempapel.sp.gov.br/sigaex/public/app/autenticar?n=47591886-10

7.2.1.6. Verificação dos objetos na memória interna do smartphone e nos cartões de expansão sob demanda do usuário e de acordo com um agendamento;
7.2.2. Deverá isolar em área de quarentena os arquivos infectados;
7.2.3. Deverá atualizar as bases de vacinas de modo agendado;
7.2.4. Capacidade de desativar por política:
7.4.2.1. Wi-fi;
7.4.2.2. Câmera;
7.4.2.3. Bluetooth.
7.2.5. Deverá ter função de limpeza de dados pessoais a distância, em caso de roubo, por exemplo;
7.2.6. Capacidade de requerer uma senha para desbloquear o dispositivo e personalizar a quantidade de caracteres para esta senha;
7.2.7. Deverá ter firewall pessoal (Android);
7.2.8. Capacidade de tirar fotos quando a senha for inserida incorretamente;
7.2.9. Capacidade de enviar comandos remotamente de:
7.2.9.1. Localizar;
7.2.9.2. Bloquear.
7.2.10. Capacidade de detectar Root em dispositivos Android;
7.2.11. Capacidade de bloquear o acesso a site por categoria em dispositivos;
7.2.12. Capacidade de bloquear o acesso a sites phishing ou maliciosos;
7.2.13. Capacidade de configurar White e blacklist de aplicativos;
7.2.14. Capacidade de localizar o dispositivo quando necessário;
7.2.15. Permitir atualização das definições quando estiver em “roaming”;
7.2.16. Capacidade de selecionar endereço do servidor para buscar a definição de vírus;
7.2.17. Capacidade de agendar uma verificação (Android);
7.2.18. Capacidade de enviar URL de instalação por e-mail;
7.2.19. Capacidade de fazer a instalação através de um link QRCode;
7.2.20. Capacidade de executar as seguintes ações caso a desinfecção falhe (Android):

- Deletar;
- Ignorar;
- Quarentenar;
- Perguntar ao usuário.

8. Gerenciamento de dispositivos móveis (MDM) - Android

8.1. Compatibilidade:

8.1.1. Dispositivos com os sistemas operacionais:
8.1.1.1. Android 5.0 – 5.1.1
8.1.1.2. Android 6.0 – 6.0.1
8.1.1.3. Android 7.0 – 7.12
8.1.1.4. Android 8.0 – 8.1
8.1.1.5. Android 9.0
8.1.1.6. Android 10.0
8.1.2. Softwares de gerência de dispositivos:
8.1.2.1. VMWare AirWatch 9.3;
8.1.2.2. MobileIron 10.0;
8.1.2.3. IBM Maas360 10.68;
8.1.2.4. Microsoft Intune 1908;
8.1.2.5. SOTI MobiControl 14.1.4 (1693);

8.2. Características:

8.2.1. Capacidade de aplicar políticas de ActiveSync através do servidor Microsoft Exchange;

FUNDCASASPDCI202261966

Assinado com senha por SABRINA MIRANDA ARRAES DE CAMPOS - GERENTE ADMINISTRATIVO I / GCCCP - 21/07/2022 às 12:23:01, AURELIO OLIMPIO DE SOUZA - DIRETOR ADMINISTRATIVO / DGA - 21/07/2022 às 13:01:32, FERNANDO JOSÉ DA COSTA - PRESIDENTE / GP - 21/07/2022 às 13:03:16 e ROSANA MORENO PIRES - DIRETOR DE DIVISÃO I / DSUP - 21/07/2022 às 13:27:47.
Autenticado com senha por DANIELLA ALVES MAURICIO - ASSISTENTE TECNICO ADM I / SCO - 21/07/2022 às 11:39:04.
Documento Nº: 47591886-10 - consulta à autenticidade em
https://www.documentos.spsempapel.sp.gov.br/sigaex/public/app/autenticar?n=47591886-10

8.2.2. Capacidade de ajustar as configurações de:
8.2.2.1. Sincronização de e-mail;
8.2.2.2. Uso de aplicativos;
8.2.2.3. Senha do usuário;
8.2.2.4. Criptografia de dados;
8.2.2.5. Conexão de mídia removível.
8.2.3. Capacidade de instalar certificados digitais em dispositivos móveis;
8.2.4. Deve permitir configurar horário para sincronização do dispositivo com a console de gerenciamento;
8.2.5. Capacidade de desinstalar remotamente o antivírus do dispositivo;
8.2.6. Deve permitir fazer o upgrade do antivírus de forma remota sem a necessidade de desinstalar a versão atual;
8.2.7. Capacidade de sincronizar com Samsung Knox;

9. Gerenciamento de dispositivos móveis (MDM) – iOS
9.1. Compatibilidade:
9.1.1. Dispositivos com os sistemas operacionais:
9.1.1.1. iOS 10.0 – 10.3.3
9.1.1.2. iOS 11.0 – 11.3
9.1.1.3. iOS 12.0
9.1.1.4. iOS 13.0
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. Senha do usuário;
9.2.2.3. Criptografia de dados;
9.2.3. Capacidade de instalar certificados digitais em dispositivos móveis;
9.2.4. Capacidade de instalar as ferramentas necessárias para o gerenciamento dos dispositivos clientes através de:
9.2.4.1. Link por e-mail;
9.2.4.2. Link por mensagem de texto;
9.2.4.3. QR Code
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 7 Ultimate SP1 ou superior x86/x64;
10.1.2. Microsoft Windows 7 Enterprise SP1 ou superior x86/x64;
10.1.3. Microsoft Windows 7 Professional SP1 ou superior x86/x64;
10.1.4. Microsoft Windows 8 Enterprise x86/x64;
10.1.5. Microsoft Windows 8 Pro x86/x64;
10.1.6. Microsoft Windows 8.1 Pro x86/x64;
10.1.7. Microsoft Windows 8.1 Enterprise x86/x64;
10.1.8. Microsoft Windows 10 Enterprise x86/x64;
10.1.9. Microsoft Windows 10 Pro x86/x64;
10.2. Características

FUNDCASASPDCI202261966

Assinado com senha por SABRINA MIRANDA ARRAES DE CAMPOS - GERENTE ADMINISTRATIVO I / GCCCP - 21/07/2022 às 12:23:01, AURELIO OLIMPIO DE SOUZA - DIRETOR ADMINISTRATIVO / DGA - 21/07/2022 às 13:01:32, FERNANDO JOSÉ DA COSTA - PRESIDENTE / GP - 21/07/2022 às 13:03:16 e ROSANA MORENO PIRES - DIRETOR DE DIVISÃO I / DSUP - 21/07/2022 às 13:27:47.
Autenticado com senha por DANIELLA ALVES MAURICIO - ASSISTENTE TECNICO ADM I / SCO - 21/07/2022 às 11:39:04.
Documento Nº: 47591886-10 - consulta à autenticidade em
https://www.documentos.spsempapel.sp.gov.br/sigaex/public/app/autenticar?n=47591886-10

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. Deve permitir que o usuário monitore a criptografia do disco ou o processo de descriptografia em tempo real;
10.2.7. Capacidade de criar um usuário de autenticação pré-boot comum com uma senha igual para todas as máquinas a partir da console de gerenciamento;
10.2.8. Capacidade de criptografar drives removíveis de acordo com regra criada pelo administrador, com as opções:
10.2.8.1. Criptografar somente os arquivos novos que forem copiados para o disco removível, sem modificar os arquivos já existentes;
10.2.8.2. Criptografar todos os arquivos individualmente;
10.2.8.3. Criptografar o dispositivo inteiro, de maneira que não seja possível listar os arquivos e pastas armazenadas;
10.2.8.4. Criptografar o dispositivo em modo portátil, permitindo acessar os arquivos em máquinas de terceiros através de uma senha;
10.2.9. Capacidade de selecionar pastas e arquivos (por tipo, ou extensão) para serem criptografados automaticamente;
10.2.10. Capacidade de criar regras de exclusões para que certos arquivos ou pastas nunca sejam criptografados;
10.3. Capacidade de selecionar aplicações que podem ou não ter acesso aos arquivos criptografados;
10.4. Verifica compatibilidade de hardware antes de aplicar a criptografia;
10.5. Possibilita estabelecer parâmetros para a senha de criptografia;
10.6. Capacidade de permitir o usuário solicitar permissão a determinado arquivo criptografado para o administrador mediante templates customizados;
10.7. Permite criar exclusões para não criptografar determinados “discos rígidos” através de uma busca por nome do computador ou nome do dispositivo
10.8. Permite criptografar as seguintes pastas pré-definidas: “meus documentos”, “Favoritos”, “Desktop”, “Arquivos temporários” e “Arquivos do outlook”;
10.9. Permite utilizar variáveis de ambiente para criptografar pastas customizadas;
10.10. Capacidade de criptografar arquivos por grupos de extensão, tais como: Documentos do office, Document, arquivos de audio, etc;
10.11. Permite criar um grupo de extensões de arquivos a serem criptografados;
10.12. Capacidade de criar regra de criptografia para arquivos gerados por aplicações;
10.13. Permite criptografia de dispositivos móveis mesmo quando o endpoint não possuir comunicação com a console de gerenciamento.
10.14. Capacidade de deletar arquivos de forma segura após a criptografia;
10.15. Capacidade de criptografar somente o espaço em disco utilizado;
10.16. Deve ter a opção de criptografar arquivos criados a partir de aplicações selecionadas pelo administrador;
10.17. Capacidade de bloquear aplicações selecionadas pelo administrador de acessarem arquivos criptografados;
10.18. Deve permitir criptografar somente o espaço utilizado em dispositivos removíveis tais como pendrives, HD externo, etc;
10.19. Capacidade de criptografar discos utilizando a criptografia BitLocker da Microsoft;

FUNDCASASPDCI202261966

Assinado com senha por SABRINA MIRANDA ARRAES DE CAMPOS - GERENTE ADMINISTRATIVO I / GCCCP - 21/07/2022 às 12:23:01, AURELIO OLIMPIO DE SOUZA - DIRETOR ADMINISTRATIVO / DGA - 21/07/2022 às 13:01:32, FERNANDO JOSÉ DA COSTA - PRESIDENTE / GP - 21/07/2022 às 13:03:16 e ROSANA MORENO PIRES - DIRETOR DE DIVISÃO I / DSUP - 21/07/2022 às 13:27:47.
Autenticado com senha por DANIELLA ALVES MAURICIO - ASSISTENTE TECNICO ADM I / SCO - 21/07/2022 às 11:39:04.
Documento Nº: 47591886-10 - consulta à autenticidade em
https://www.documentos.spsempapel.sp.gov.br/sigaex/public/app/autenticar?n=47591886-10

10.20. Deve ter a opção de utilização de TPM para criptografia através do BitLocker;
10.21. Capacidade de fazer “Hardware encryption”;

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. Deve possibilitar a utilização de servidores PXE na rede para deploy de imagens;
11.3. Capacidade de detectar softwares de terceiros vulneráveis, criando assim um relatório de softwares vulneráveis;
11.4. 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;
11.5. Capacidade de gerenciar licenças de softwares de terceiros;
11.6. Capacidade de atualizar informações sobre hardware presentes nos relatórios após 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);
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 tecnologia 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 automática 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;
11.26. Capacidade de adicionar caminhos específicos para procura de vulnerabilidades e updates em arquivos;
11.27. Capacidade de instalar atualizações ou correções somente em computadores definidos, em grupos definidos ou em uma porcentagem de computadores conforme selecionado pelo administrador;
11.28. Capacidade de configurar o reinicio do computador após a aplicação das atualizações e correções de vulnerabilidades;
11.29. Deve permitir selecionar o idioma das aplicações que serão atualizadas;

FUNDCASASPDCI202261966

Assinado com senha por SABRINA MIRANDA ARRAES DE CAMPOS - GERENTE ADMINISTRATIVO I / GCCCP - 21/07/2022 às 12:23:01, AURELIO OLIMPIO DE SOUZA - DIRETOR ADMINISTRATIVO / DGA - 21/07/2022 às 13:01:32, FERNANDO JOSÉ DA COSTA - PRESIDENTE / GP - 21/07/2022 às 13:03:16 e ROSANA MORENO PIRES - DIRETOR DE DIVISÃO I / DSUP - 21/07/2022 às 13:27:47.
Autenticado com senha por DANIELLA ALVES MAURICIO - ASSISTENTE TECNICO ADM I / SCO - 21/07/2022 às 11:39:04.
Documento Nº: 47591886-10 - consulta à autenticidade em
https://www.documentos.spsempapel.sp.gov.br/sigaex/public/app/autenticar?n=47591886-10

11.30. Permitir agendar o sincronismo entre a console de gerenciamento e os sites da Microsoft para baixar atualizações recentes;

12. Detecção e Resposta Gerenciada

12.1. Do monitoramento, identificação e investigação dos eventos de segurança cibernética

12.1.1. O serviço de monitoramento deverá utilizar informações extraídas de registros gerados pelos sistemas monitorados.

12.1.2. Deverá ser instalado agentes específicos nos servidores e desktops, objetivando coletar informações mais detalhadas para o serviço de monitoramento, desde que seja plenamente compatível com o sistema onde será instalado e não afete o desempenho dos serviços.

12.1.3. A análise das informações correlacionadas deve ser realizada com auxílio de bases globais de inteligência cibernética em conjunto com a expertise dos profissionais do fabricante, com vistas a reduzir ao máximo os falsos positivos.

12.1.4. É obrigatório que a comunicação entre equipamentos e soluções do fabricante instalados nos dispositivos e qualquer infraestrutura onde esses dados sejam processados ocorra de forma segura, utilizando algoritmos criptográficos para preservar o sigilo das informações.

12.1.5. Deverá ser feita a investigação e a classificação dos eventos monitorados, aplicando os principais frameworks de gestão de incidentes de segurança cibernética bem como boas práticas de mercado na detecção e triagem dos eventos de segurança, objetivando minimizar a presença de falsos positivos na abertura de incidentes de segurança.

12.1.6. O serviço de monitoramento deverá ser capaz de coletar e realizar a correlação de eventos dos sistemas e ativos monitorados, permitindo uma visão mais abrangente do alcance das ações maliciosas, bem como de possível movimentação lateral do atacante dentro da rede.

12.1.7. O monitoramento deverá ser capaz de identificar as principais ameaças, bem como táticas, técnicas e procedimentos de ataque descritos na base de conhecimento MITRE ATT&CK, sem prejuízo do uso de outras bases de conhecimento ou serviços de inteligência de ameaças, para complementação da capacidade de identificação de atividades maliciosas.

12.1.8. Deverá monitorar e avaliar criticamente os serviços, traçando curvas de comportamento, definindo a volumetria média e identificando comportamentos anômalos, visando antecipar a identificação de incidentes de segurança.

12.1.9. A solução deverá prover inteligência de proteção contra ataques cibernéticos a nível global, sendo responsável por pesquisar novos tipos de ataques, vírus, malwares, botnets, vulnerabilidades e afins com intuito de melhoria contínua de detecção e mitigação destes males dentro dos serviços e ativos de segurança monitorados.

12.1.10. O fabricante deverá utilizar solução para registro de incidente de segurança, acessível pela equipe técnica da Contratante, para indicar ações de contenção, comunicar à equipe da Contratante sobre o andamento do tratamento dos incidentes.

12.2. Compatibilidade:

12.2.1. É suportada por qualquer um dos seguintes navegadores:

12.2.1.1. Apple Safari versões mais recentes

12.2.1.2. Google Chrome versões mais recentes

12.2.1.3. Microsoft Edge

12.2.1.4. Mozilla Firefox versões mais recentes

12.2.2. Requisitos de rede:

12.2.2.1. Em condições médias de carga: um canal full-duplex com largura de banda de pelo menos 1,7 Kbps para cada ativo.

FUNDCASASPDCI202261966

Assinado com senha por SABRINA MIRANDA ARRAES DE CAMPOS - GERENTE ADMINISTRATIVO I / GCCCP - 21/07/2022 às 12:23:01, AURELIO OLIMPIO DE SOUZA - DIRETOR ADMINISTRATIVO / DGA - 21/07/2022 às 13:01:32, FERNANDO JOSÉ DA COSTA - PRESIDENTE / GP - 21/07/2022 às 13:03:16 e ROSANA MORENO PIRES - DIRETOR DE DIVISÃO I / DSUP - 21/07/2022 às 13:27:47.
Autenticado com senha por DANIELLA ALVES MAURICIO - ASSISTENTE TECNICO ADM I / SCO - 21/07/2022 às 11:39:04.
Documento Nº: 47591886-10 - consulta à autenticidade em
https://www.documentos.spsempapel.sp.gov.br/sigaex/public/app/autenticar?n=47591886-10

12.2.2.2. Em condições de carga máxima: um canal full-duplex com largura de banda de pelo menos 2,7 Kbps para cada ativo.
12.2.3. Compatibilidade de sensor de endpoint
12.2.3.1. O agente de endpoint deve ser compatível com os seguintes sistemas operacionais, para no mínimo a coleta e envio dos dados/telemetria ao SOC do fabricante:
12.2.3.1.1. Microsoft Windows 7 e superiores;
12.2.3.1.2. macOS 10.14-11;
12.2.3.1.3. CentOS 6.7 ou superior;
12.2.3.1.4. Debian GNU / Linux 9.4 ou superior;
12.2.3.1.5. Linux Mint 19 ou superior;
12.2.3.1.6. Oracle Linux 7.3 ou superior;
12.2.3.1.7. Red Hat Enterprise Linux 6.7 ou superior;
12.2.3.1.8. SUSE Linux Enterprise Server 12 SP5 ou superior;
12.2.3.1.9. Ubuntu 18.04 LTS ou superior.

12.3. Capacidades Técnicas

12.3.1. Deve possuir console web própria do serviço, além de integração nativa com a console do “software de segurança e antivírus para servidores físicos, microcomputadores e smartphones/tablets”
12.3.2. A console deve possuir dashboards com as informações principais, apresentando no mínimo:
12.3.2.1. Número de incidentes e status
12.3.2.2. Quantidade de dispositivos monitorados
12.3.3. Deve possuir mecanismo de notificações, com no mínimo as seguintes opções:
12.3.3.1. E-mail
12.3.3.2. Telegram
12.3.4. Deve permitir o envio de relatórios.
12.3.5. O agente deve enviar a telemetria em tempo real para o SoC do fabricante;
12.3.6. O serviço deve compreender monitoramento dos dados enviados e alertas gerados em um regime 24x7x265.
12.3.7. O envio e armazenamento da telemetria, devem respeitar as principais legislações de proteção de dados, como GDPR e LGPD.
12.3.8. O SoC do fabricante deve possuir datacenters em pelo menos duas localidades em diferentes países.
12.3.9. O SoC do fabricante deve possuir equipes de analistas em pelo menos 3 regiões (países) incluindo Brasil.
12.3.10. Os dados coletados devem passar por no mínimo:
12.3.10.1. Modelos de Machine Learning/Inteligência Artificial;
12.3.10.2. Análise humana;
12.3.10.3. Correlação com IoA’s (indicadore de ataque);
12.3.10.4. Emulação em sandbox (quando necessário);
12.3.11. Após análise, informações sobre atividades potencialmente maliciosas, devem ser apresentadas no portal como “Incidentes”
12.3.12. O Incidente deve possuir no mínimo as seguintes informações:
12.3.12.1. Resumo
12.3.12.2. Prioridade (Baixa, Média e Alta)
12.3.12.3. Recomendação
12.3.12.4. Data de criação e data de atualização
12.3.12.5. Correlacionamento com táticas/técnicas do Framewok MITRE ATT&CK
12.3.12.6. Dispositivos afetados
12.3.12.7. IoC’s de host e de rede
12.3.12.8. Descrição completa em linha do tempo

FUNDCASASPDCI202261966

Assinado com senha por SABRINA MIRANDA ARRAES DE CAMPOS - GERENTE ADMINISTRATIVO I / GCCCP - 21/07/2022 às 12:23:01, AURELIO OLIMPIO DE SOUZA - DIRETOR ADMINISTRATIVO / DGA - 21/07/2022 às 13:01:32, FERNANDO JOSÉ DA COSTA - PRESIDENTE / GP - 21/07/2022 às 13:03:16 e ROSANA MORENO PIRES - DIRETOR DE DIVISÃO I / DSUP - 21/07/2022 às 13:27:47.
Autenticado com senha por DANIELLA ALVES MAURICIO - ASSISTENTE TECNICO ADM I / SCO - 21/07/2022 às 11:39:04.
Documento Nº: 47591886-10 - consulta à autenticidade em
https://www.documentos.spsempapel.sp.gov.br/sigaex/public/app/autenticar?n=47591886-10

12.3.13. O incidente pode receber ações de resposta recomendada disparadas pela equipe de SoC, compreendendo no mínimo as seguintes ações:
12.3.13.1. Transferir arquivo para o SoC;
12.3.13.2. Isolar um dispositivo;
12.3.13.3. Desabilitar isolamento de dispositivo;
12.3.13.4. Deletar chave de registro;
12.3.13.5. Dump de memória;
12.3.14. As ações devem ser aprovadas no portal por profissional da contratante, com a opção de habilitar aprovação automática.

12.4. Agente de Endpoint

12.4.1. As funcionalidades relacionadas a detecção e resposta solicitadas nesse item, devem ser operadas na mesma console de gerenciamento da solução de endpoint;
12.4.2. A solução deve oferecer módulo focado em capacidades de EDR "Endpoint Detection and Response", incluindo no mínimo as seguintes capacidades:
12.4.2.1. O agente deve ter capacidade de coletar e processar dados relacionadas ao veredito e ao contexto da ameaça;
12.4.2.2. Deve fornecer graficamente a visualização da cadeia do ataque;
12.4.2.3. Deve possuir a capacidade de varredura, para identificar a presença de um artefato detectado em outros dispositivos na rede, através de indicadores de comprometimento (IoC).
12.4.2.4. A varredura deve oferecer opções de resposta automatizada (sem intervenção do administrador), para serem executadas caso o IoC seja encontrado em outro dispositivo, com no mínimo as seguintes opções:
12.4.2.4.1. Isolar o host;
12.4.2.4.2. Iniciar uma varredura nas áreas críticas;
12.4.2.4.3. Quarentenar o objeto;
12.4.2.5. A solução deve criar um report detalhado sobre o incidente, tendo a capacidade de incluir no mínimo os seguintes dados:
12.4.2.5.1. Detecções provenientes da solução de endpoint;
12.4.2.5.2. Processos;
12.4.2.5.3. Alterações de registro;
12.4.2.5.4. Conexões remotas;
12.4.2.5.5. Criação de arquivos;
12.4.2.6. Varredura por todos os dispositivos executada a partir de indicador de comprometimento (IoC) gerado através da solução e importado pelo administrador.
12.4.2.7. Possibilidade de exportar os indicadores de comprometimento (IoC) gerados a partir da solução.
12.4.2.8. A solução deve oferecer no mínimo as seguintes opções de resposta:
12.4.2.8.1. Prevenir a execução de um arquivo;
12.4.2.8.2. Quarentenar um arquivo;
12.4.2.8.3. Iniciar uma varredura por IoC;
12.4.2.8.4. Parar um processo;
12.4.2.8.5. Executar um processo;
12.4.2.9. Ferramenta que possibilite o isolamento do host infectado com no mínimo as características abaixo:
12.4.2.9.1. A opção de isolamento deve estar disponível junto a visualização do incidente;
12.4.2.9.2. Na configuração padrão, o isolamento deve ser feito de forma granular, permitindo o controle do dispositivo pela console administrativa mesmo após ativação da regra;
13. Suporte Técnico
13.1. O Suporte Técnico do fabricante:

FUNDCASASPDCI202261966

Assinado com senha por SABRINA MIRANDA ARRAES DE CAMPOS - GERENTE ADMINISTRATIVO I / GCCCP - 21/07/2022 às 12:23:01, AURELIO OLIMPIO DE SOUZA - DIRETOR ADMINISTRATIVO / DGA - 21/07/2022 às 13:01:32, FERNANDO JOSÉ DA COSTA - PRESIDENTE / GP - 21/07/2022 às 13:03:16 e ROSANA MORENO PIRES - DIRETOR DE DIVISÃO I / DSUP - 21/07/2022 às 13:27:47.
Autenticado com senha por DANIELLA ALVES MAURICIO - ASSISTENTE TECNICO ADM I / SCO - 21/07/2022 às 11:39:04.
Documento Nº: 47591886-10 - consulta à autenticidade em
https://www.documentos.spsempapel.sp.gov.br/sigaex/public/app/autenticar?n=47591886-10

13.2. Deverá oferecer serviço relacionado as operações do produto e suas funcionalidades, tão como orientação no caso de infecção.
13.3. Deve possibilitar a abertura de chamados de suporte, para no mínimo, os seguintes métodos: via telefone, e-mail e/ou "website";
13.4. Deverá disponibilizar portal da web do suporte técnico do fabricante com aceitação de solicitações 24 horas por dia, 365 dias por ano;
13.5. Deverá disponibilizar suporte técnico por telefone em horário comercial e em português;
13.6. Deverá disponibilizar suporte técnico por telefone 24x7, podendo este ser em inglês fora do horário comercial (9h as 18h);
13.7. Deverá ser permitido autorizar até 4 pessoas a abrir chamados diretamente nas centrais de suporte técnico do fabricante;
13.8. O tratamento de incidentes, deve ser realizado por um time dedicado de engenheiros sênior, que atuarão como ponto principal de contato, para fornecer assistência avançada em horário comercial.
13.9. O tratamento de incidentes, deve ser realizado por um time dedicado de engenheiros sênior, que atuarão como ponto principal de contato, para fornecer assistência avançada 24x7 para casos de severidade nível 1.
13.10. O atendimento do incidente deve incluir acesso remoto a infraestrutura da contratada, caso necessário.
13.11. Do SLA de atendimento:
13.11.1. O tempo máximo para início do atendimento a chamados de nível 1 é de 2 horas contados do recebimento da notificação.
13.11.2. O tempo máximo para início do atendimento a chamados de nível 2 é de 6 horas, contados do recebimento da notificação.
13.11.3. O tempo máximo para início do atendimento a chamados de nível 3 é de 8 horas, contados do recebimento da notificação.
13.11.4. O tempo máximo para início do atendimento a chamados de nível 4 é de 10 horas, contados do recebimento da notificação.
13.11.5. Níveis de severidade do incidente
13.11.6. "Nível de Severidade 1" (crítico) deve significar um problema crítico do Produto, que afeta a continuidade dos negócios do Cliente por interrupções no funcionamento normal do Produto e que faz com que o (s) Produto (s) ou Sistema Operacional falhe, ou que causa perda de dados, alteração das configurações padrão para valores inseguros ou problemas de segurança, desde que não haja solução alternativa disponível.
13.11.7. A lista de incidentes relacionados ao produto, que se referem ao nível de gravidade 1, inclui, mas não está limitada a:
13.11.8. Toda a rede local (ou sua parte crítica) está inoperante, o que dificulta ou suspende os principais processos de negócios.
13.11.9. "Nível de Severidade 2" (alto) significa um problema moderado que afeta a funcionalidade do produto, mas não causa
13.11.10. Corrupção / perda de dados ou falha de software. O nível de gravidade 1 é reclassificado para o nível de gravidade 2 quando uma solução alternativa é acessível.
13.11.11. A lista de incidentes relacionados ao produto, que se referem ao nível de gravidade 2, inclui, mas não está limitada a:
13.11.12. O produto apresenta mau funcionamento ou não funciona, mas a continuidade dos principais processos de negócios não é interrompida.
13.11.13. "Nível de Severidade 3" (médio) significa um problema não crítico ou solicitação de serviço, que não afeta a funcionalidade do produto.

FUNDCASASPDCI202261966

Assinado com senha por SABRINA MIRANDA ARRAES DE CAMPOS - GERENTE ADMINISTRATIVO I / GCCCP - 21/07/2022 às 12:23:01, AURELIO OLIMPIO DE SOUZA - DIRETOR ADMINISTRATIVO / DGA - 21/07/2022 às 13:01:32, FERNANDO JOSÉ DA COSTA - PRESIDENTE / GP - 21/07/2022 às 13:03:16 e ROSANA MORENO PIRES - DIRETOR DE DIVISÃO I / DSUP - 21/07/2022 às 13:27:47.
Autenticado com senha por DANIELLA ALVES MAURICIO - ASSISTENTE TECNICO ADM I / SCO - 21/07/2022 às 11:39:04.
Documento Nº: 47591886-10 - consulta à autenticidade em
https://www.documentos.spsempapel.sp.gov.br/sigaex/public/app/autenticar?n=47591886-10

FUNDAÇÃO CASA
CENTRO DE ATENDIMENTO SOCIOEDUCATIVO AO ADOLESCENTE

A lista de incidentes, que se refere ao nível de gravidade 3, inclui, mas não se limita aos seguintes problemas: o produto está parcialmente fora de serviço (mau funcionamento), mas outros aplicativos utilizados pelo Cliente não estão envolvidos.

13.11.14. "Nível de Severidade 4" (baixo) significa outros problemas não críticos ou solicitações de serviço. Todos os incidentes que não satisfazem qualquer um dos critérios listados acima, referem-se a este nível de gravidade.

FUNDCASASPDCI202261966

Assinado com senha por SABRINA MIRANDA ARRAES DE CAMPOS - GERENTE ADMINISTRATIVO I / GCCCP - 21/07/2022 às 12:23:01, AURELIO OLIMPIO DE SOUZA - DIRETOR ADMINISTRATIVO / DGA - 21/07/2022 às 13:01:32, FERNANDO JOSÉ DA COSTA - PRESIDENTE / GP - 21/07/2022 às 13:03:16 e ROSANA MORENO PIRES - DIRETOR DE DIVISÃO I / DSUP - 21/07/2022 às 13:27:47.
Autenticado com senha por DANIELLA ALVES MAURICIO - ASSISTENTE TECNICO ADM I / SCO - 21/07/2022 às 11:39:04.
Documento Nº: 47591886-10 - consulta à autenticidade em
https://www.documentos.spsempapel.sp.gov.br/sigaex/public/app/autenticar?n=47591886-10

FUNDAÇÃO CASA
CENTRO DE ATENDIMENTO
SOCIOEDUCATIVO AO ADOLESCENTE

ANEXO II

PLANILHA DE PROPOSTA

PREGÃO ELETRÔNICO SDE n.º 073/2022
PROCESSO FUNDCASASP-PRC-2022/09886

São Paulo, 14 de Julho de 2022

PLANILHA DE PROPOSTA

LOTE						
ITEM	QUANT	UNIDADE	DESCRIÇÃO	PARTNUMBER	R$ UNIT.	R$ TOTAL
01	4.500	Unidade	Kaspersky Optimum Security Brazilian Edition. 2500-4999 Node 3 year Renewal Plus License.	KL4709KAYT9	R$ 230,00	R$ 1.035.000,00
02	01	Unidade	Kaspersky Enhanced Support Brazilian Edition. 3 year Certificate.	KL7122KLZTZ	R$ 144.137,00	R$ 144.137,00
03	06	Unidade	Kaspersky Professional Services - 8 Hours, Remote Brazilian Edition. 5-9 Day 1 year Certificate.	KL7222K1EFZ	R$ 3.727,00	R$ 22.362,00
					VALOR TOTAL DO LOTE:	**R$ 1.201.499,00**

***O valor total da proposta é de* R$ 1.201.499,00 (Hum milhão, duzentos e um mil, quatrocentos e noventa e nove reais)**

- Validade da proposta: 60 (sessenta) dias

FUNDCASASPDCI202261966

Assinado com senha por SABRINA MIRANDA ARRAES DE CAMPOS - GERENTE ADMINISTRATIVO I / GCCCP - 21/07/2022 às 12:23:01, AURELIO OLIMPIO DE SOUZA - DIRETOR ADMINISTRATIVO / DGA - 21/07/2022 às 13:01:32, FERNANDO JOSÉ DA COSTA - PRESIDENTE / GP - 21/07/2022 às 13:03:16 e ROSANA MORENO PIRES - DIRETOR DE DIVISÃO I / DSUP - 21/07/2022 às 13:27:47.
Autenticado com senha por DANIELLA ALVES MAURICIO - ASSISTENTE TECNICO ADM I / SCO - 21/07/2022 às 11:39:04.
Documento Nº: 47591886-10 - consulta à autenticidade em
https://www.documentos.spsempapel.sp.gov.br/sigaex/public/app/autenticar?n=47591886-10

FUNDAÇÃO CASA
CENTRO DE ATENDIMENTO SOCIOEDUCATIVO AO ADOLESCENTE

ANEXO III

REGULAMENTO PARA OS PROCEDIMENTOS DE SANÇÕES ADMINISTRATIVAS NO ÂMBITO DA FUNDAÇÃO CASA-SP

Artigo 1º - Os processos administrativos que objetivem apurar a prática de infração e registrar sanções administrativas previstas na Lei federal nº 8.666, de 21 de junho de 1993, na Lei federal nº 10.520, de 17 de julho de 2002, ou na Lei nº 6.544, de 22 de novembro de 1989, serão disciplinados por este Regulamento.

Parágrafo único: O disposto neste Regulamento aplica-se, também, às contratações celebradas com dispensa ou inexigibilidade de licitação, com fundamento nos artigos 24 e 25 da Lei federal nº 8.666, de 21 de junho de 1993.

Artigo 2º – Caberá ao Diretor da Divisão Regional, nos ajustes a ela vinculados, e ao Diretor Administrativo, nos ajustes vinculados à Sede, pela inexecução total ou parcial ou por descumprimento injustificado de prazos ou de outras obrigações, aplicar ao contratado as penalidades de advertência, multa, suspensão temporária de participação em licitação e impedimento de licitar e contratar com a Administração.

Artigo 3º - Caberá ao Presidente desta Fundação rescindir unilateralmente o termo de contrato ou instrumento equivalente, sem prejuízo da aplicação das demais penalidades previstas no artigo 2º.

Artigo 4º - As penalidades de multa serão calculadas na forma prevista nos artigos 5º ao 9º.

Artigo 5º - Pela recusa injustificada em assinar, aceitar ou retirar o contrato ou instrumento equivalente, dentro do prazo estabelecido pela Fundação, será aplicada ao adjudicatário ou vencedor da licitação, multa de 40% (quarenta por cento) sobre o valor total da compra, serviço ou obra, reajustado até a data da aplicação da penalidade, ou multa correspondente à diferença de preço resultante da nova licitação realizada para o mesmo objeto.

Artigo 6º - Pela inexecução total do ajuste, será aplicada ao contratado multa compensatória de 50% (cinquenta por cento) calculada sobre o valor total do contrato ou instrumento equivalente, reajustado até a data da aplicação da penalidade, ou multa compensatória no valor correspondente à diferença de preço resultante de nova licitação realizada para o mesmo objeto.

Artigo 7º - Pela inexecução parcial do ajuste, será aplicada ao contratado multa compensatória de 30% (trinta por cento) calculada sobre o valor dos materiais não entregues, dos serviços ou obras não executadas, ou multa compensatória no valor correspondente à diferença de preço resultante de nova licitação realizada para o mesmo objeto.

Parágrafo único: Considera-se inexecução parcial o inadimplemento de cláusulas essenciais do contrato, que comprometa a obtenção do objeto contratual.

Artigo 8º - Pelo descumprimento injustificado de prazos fixados no contrato ou instrumento equivalente para entrega de materiais, execução de etapas ou conclusão de obras e de serviços com prazos determinados, serão aplicadas as seguintes multas moratórias, que

FUNDCASASPDCI202261966

Assinado com senha por SABRINA MIRANDA ARRAES DE CAMPOS - GERENTE ADMINISTRATIVO I / GCCCP - 21/07/2022 às 12:23:01, AURELIO OLIMPIO DE SOUZA - DIRETOR ADMINISTRATIVO / DGA - 21/07/2022 às 13:01:32, FERNANDO JOSÉ DA COSTA - PRESIDENTE / GP - 21/07/2022 às 13:03:16 e ROSANA MORENO PIRES - DIRETOR DE DIVISÃO I / DSUP - 21/07/2022 às 13:27:47.
Autenticado com senha por DANIELLA ALVES MAURICIO - ASSISTENTE TECNICO ADM I / SCO - 21/07/2022 às 11:39:04.
Documento Nº: 47591886-10 - consulta à autenticidade em
https://www.documentos.spsempapel.sp.gov.br/sigaex/public/app/autenticar?n=47591886-10

incidirão sobre o valor das obrigações não cumpridas:

I – Atraso de 30 dias: multa de 0,2% (dois décimos por cento) por dia de atraso;

II – Atraso de 31 a 60 dias: multa de 0,3% (três décimos por cento) por dia, desde o primeiro dia de atraso;

III – Atraso superior a 60 dias: multa de 30% calculada sobre o valor correspondente ao material entregue ou serviço finalizado com atraso.

§1º - Se o material ou serviço entregue não for aceito pela Fundação, caberá ao contratado substituí-lo ou refazê-lo nas seguintes condições:

I – Quando a entrega ocorrer dentro do prazo estipulado na contratação, o contratado deverá substituir o material ou refazer o serviço, sem prejuízo ao prazo inicialmente previsto no instrumento contratual para a entrega / conclusão do serviço, sob pena de aplicação da penalidade cabível caso a nova entrega / conclusão ocorra após o prazo inicialmente fixado;

II – Quando a entrega ocorrer após o final do prazo estipulado na contratação, o contratado deverá substituir o material ou refazer o serviço em até 5 (cinco) dias úteis a contar da data da recusa do material ou serviço, sem prejuízo das penalidades previstas para o atraso, que será contado a partir do prazo inicialmente previsto no instrumento contratual.

Artigo 9º - Pelo descumprimento injustificado de outras obrigações que não configurem inexecução total ou parcial do contrato ou mora no adimplemento, será aplicada multa de 0,1% a 2% (um décimo por cento a dois por cento) sobre o valor faturado mensalmente pelo contratado, correspondente ao mês da ocorrência do ato ou fato irregular.

§1º - No caso de obras e serviços os percentuais previstos neste artigo serão aplicados sobre o último valor faturado pela empresa contratada, que corresponde ao mês da ocorrência do ato ou fato irregular.

§2º - As obrigações do ‘caput’ deste artigo são aquelas que não comprometem diretamente o objeto principal do contrato, mas que ferem critérios e condições nele explicitamente previstos.

§3º - A aplicação da penalidade a que se refere o presente artigo será procedida mediante a avaliação e justificativa, por parte do gestor do contrato, quanto à gravidade da infração contratual e o percentual aplicável, na forma do caput.

Artigo 10 - As multas previstas neste Regulamento serão calculadas pela aplicação das seguintes fórmulas:

I – Inexecução Parcial – multa de 30%

M = [TX1 x SD]

II – Atraso até 30 dias – multa de 0,2%

FUNDCASASPDCI202261966

Assinado com senha por SABRINA MIRANDA ARRAES DE CAMPOS - GERENTE ADMINISTRATIVO I / GCCCP - 21/07/2022 às 12:23:01, AURELIO OLIMPIO DE SOUZA - DIRETOR ADMINISTRATIVO / DGA - 21/07/2022 às 13:01:32, FERNANDO JOSÉ DA COSTA - PRESIDENTE / GP - 21/07/2022 às 13:03:16 e ROSANA MORENO PIRES - DIRETOR DE DIVISÃO I / DSUP - 21/07/2022 às 13:27:47.
Autenticado com senha por DANIELLA ALVES MAURICIO - ASSISTENTE TECNICO ADM I / SCO - 21/07/2022 às 11:39:04.
Documento Nº: 47591886-10 - consulta à autenticidade em
https://www.documentos.spsempapel.sp.gov.br/sigaex/public/app/autenticar?n=47591886-10

M = [TX2 x (DA x VA)]

III – Atraso de 31 a 60 dias – multa de 0,3%

M = [TX3 x (DA x VA)]

IV – Atraso superior a 60 dias – multa de 30%

M = [TX1 x VA]

V - Descumprimento de condições de execução contratual – multa de 0,1% a 2% (conforme proposto pelo gestor).

M = [TX4 x VM]

Sendo:

M = multa
TX1 = 30%
TX2 = 0,2%
TX3 = 0,3%
TX4 = 0,1% a 2% (conforme proposto pelo gestor)
DA = dias de atraso
SD = saldo devedor
VA = valor do produto / serviço entregue com atraso
VM = valor mensal do contrato

Artigo 11 - Instruído na forma prevista no Capítulo XIII da Portaria Administrativa nº 339/2020, o procedimento será encaminhado:

I – Ao Diretor Administrativo, quando a aplicação da penalidade decorrer de contrato iniciado na Sede desta Fundação, ou;

II – Ao respectivo Diretor da Divisão Regional, quando o processo for iniciado em uma das Regionais da Fundação CASA-SP.

Parágrafo único: As autoridades referidas neste artigo deverão analisar o ato ou fato irregular, e, mediante ato fundamentado, classificá-lo como inexecução total ou inexecução parcial, ou mero descumprimento de outras obrigações, e, sendo o caso, rescisão contratual.

Artigo 12 - A contagem dos prazos de entrega ou de execução será feita em dias corridos, iniciando-se no primeiro dia útil subsequente à data estabelecida no contrato ou instrumento equivalente, configurando-se o atraso a partir do primeiro dia útil subsequente ao do encerramento deste prazo.

Parágrafo único: Somente se iniciam e vencem os prazos referidos neste artigo em dia útil.

Artigo 13 - As multas previstas nos artigos 7°, 8º e 9º serão descontadas do primeiro pagamento eventualmente devido pela Fundação, ou da garantia do respectivo contrato ou instrumento equivalente, após a publicação da sanção no Diário Oficial.

FUNDCASASPDCI202261966

Assinado com senha por SABRINA MIRANDA ARRAES DE CAMPOS - GERENTE ADMINISTRATIVO I / GCCCP - 21/07/2022 às 12:23:01, AURELIO OLIMPIO DE SOUZA - DIRETOR ADMINISTRATIVO / DGA - 21/07/2022 às 13:01:32, FERNANDO JOSÉ DA COSTA - PRESIDENTE / GP - 21/07/2022 às 13:03:16 e ROSANA MORENO PIRES - DIRETOR DE DIVISÃO I / DSUP - 21/07/2022 às 13:27:47.
Autenticado com senha por DANIELLA ALVES MAURICIO - ASSISTENTE TECNICO ADM I / SCO - 21/07/2022 às 11:39:04.
Documento Nº: 47591886-10 - consulta à autenticidade em
https://www.documentos.spsempapel.sp.gov.br/sigaex/public/app/autenticar?n=47591886-10

Parágrafo único: Se a multa aplicada for superior ao valor do primeiro pagamento, o excesso será descontado do pagamento seguinte e assim sucessivamente.

Artigo 14 – O Diretor Administrativo ou o Diretor da Divisão Regional, constatado o descumprimento das obrigações previstas nos artigos 5º, 6º, 7º, 8º e 9º e, após procederem na forma estabelecida no artigo 11, intimarão o licitante, a adjudicatária ou a contratada para apresentação de defesa prévia, obedecendo os seguintes prazos:

I - 5 (cinco) dias úteis, quando a sanção proposta for de advertência ou multa, conforme previsto neste Regulamento, ou suspensão temporária, prevista no inciso III, do artigo 87 da Lei federal nº 8.666, de 21 de junho de 1993;

II - 10 (dez) dias, quando a sanção proposta for a de declaração de inidoneidade, prevista no inciso IV, do artigo 87 da Lei federal nº 8.666, de 21 de junho de 1993;

III - 10 (dez) dias, quando a sanção proposta for a de impedimento de licitar e contratar com a Administração, prevista no artigo 7º da Lei federal nº 10.520, de 17 de julho de 2002.

§1º - se, no prazo de defesa prévia, o licitante, a adjudicatária ou a contratada manifestar-se expressamente pela concordância com a aplicação da penalidade ou manter-se inerte, o Diretor Administrativo ou o Diretor da Divisão Regional, conforme o caso, decidirá sobre a aplicação da sanção;

§2º - se, no prazo previsto neste Regulamento, o licitante, a adjudicatária ou a contratada apresentar defesa prévia, o feito deverá ser remetido ao GTAJ.

§3° - As defesas apresentadas serão analisadas pelo GTAJ desta Fundação, que poderá solicitar diligência, encaminhando o procedimento ao Diretor Administrativo ou Diretor da Divisão Regional para esclarecimentos.

Artigo 15 – O licitante, a adjudicatária ou a contratada deverá efetuar o recolhimento do valor da multa no prazo de 05 dias úteis, contados do primeiro dia útil subsequente à data da notificação quanto à decisão pela sua aplicação, através de publicação na imprensa oficial.

§1º - após a publicação e, sendo aplicada a penalidade de multa, as autoridades procederão aos encaminhamentos necessários para o desconto de tal valor de eventuais créditos que sejam devidos à empresa;

Artigo 16 - Havendo atraso no pagamento da multa, 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.

Artigo 17 – Se o pagamento da multa imposta ao contratado não for efetuado extrajudicialmente, dentro do prazo estabelecido no artigo 15, sua cobrança será efetuada judicialmente, nos termos da legislação em vigor.

Artigo 18 – As penalidades estabelecidas neste Regulamento são autônomas e a aplicação de uma não exclui a aplicação da outra e não impede a rescisão unilateral do ajuste.

Parágrafo único: A aplicação da multa prevista no artigo 8º, de natureza moratória, não

FUNDCASASPDCI202261966

Assinado com senha por SABRINA MIRANDA ARRAES DE CAMPOS - GERENTE ADMINISTRATIVO I / GCCCP - 21/07/2022 às 12:23:01, AURELIO OLIMPIO DE SOUZA - DIRETOR ADMINISTRATIVO / DGA - 21/07/2022 às 13:01:32, FERNANDO JOSÉ DA COSTA - PRESIDENTE / GP - 21/07/2022 às 13:03:16 e ROSANA MORENO PIRES - DIRETOR DE DIVISÃO I / DSUP - 21/07/2022 às 13:27:47.
Autenticado com senha por DANIELLA ALVES MAURICIO - ASSISTENTE TECNICO ADM I / SCO - 21/07/2022 às 11:39:04.
Documento Nº: 47591886-10 - consulta à autenticidade em
https://www.documentos.spsempapel.sp.gov.br/sigaex/public/app/autenticar?n=47591886-10

impede a aplicação superveniente das multas, de natureza compensatória, prevista nos artigos 6º e 7º, cumulando-se os respectivos valores.

Artigo 19 – As disposições estabelecidas neste Regulamento deverão constar em todos os instrumentos convocatórios das licitações e em todos os contratos de fornecimento, serviços ou obras inclusive os de fornecimento de materiais, execução de serviços e de obras a serem realizadas com dispensa ou inexigibilidade de licitação.

Artigo 20 - Da aplicação das penalidades previstas neste Regulamento caberá recurso à Presidência da Fundação, no prazo de 5 (cinco) dias úteis, nos termos do artigo 109 da Lei Federal 8.666, de 21 de junho de 1993.

Parágrafo único: Os recursos interpostos serão analisados pelo GTAJ desta Fundação, instruídos, quando necessário, da manifestação dos gestores, do Diretor Administrativo ou do Diretor da Divisão Regional.

Artigo 21 – Os casos não previstos neste Regulamento serão decididos pelo Diretor Administrativo que poderá, a depender da complexidade da decisão, alçar ao Presidente da Fundação.

FUNDCASASPDCI202261966

Assinado com senha por SABRINA MIRANDA ARRAES DE CAMPOS - GERENTE ADMINISTRATIVO I / GCCCP - 21/07/2022 às 12:23:01, AURELIO OLIMPIO DE SOUZA - DIRETOR ADMINISTRATIVO / DGA - 21/07/2022 às 13:01:32, FERNANDO JOSÉ DA COSTA - PRESIDENTE / GP - 21/07/2022 às 13:03:16 e ROSANA MORENO PIRES - DIRETOR DE DIVISÃO I / DSUP - 21/07/2022 às 13:27:47.
Autenticado com senha por DANIELLA ALVES MAURICIO - ASSISTENTE TECNICO ADM I / SCO - 21/07/2022 às 11:39:04.
Documento Nº: 47591886-10 - consulta à autenticidade em
https://www.documentos.spsempapel.sp.gov.br/sigaex/public/app/autenticar?n=47591886-10