Ministério do Desenvolvimento Regional – MDR
Companhia de Desenvolvimento dos Vales do São Francisco e do Parnaíba
Área de Gestão Estratégica

TERMO DE REFERÊNCIA

CONTRATAÇÃO DE ATUALIZAÇÃO DE LICENÇAS DE SOFTWARES DA SOLUÇÃO CENTRALIZADA DE SEGURANÇA DO TIPO *ENDPOINT PROTECTION* - CEB (ANTIVÍRUS/*ANTIMALWARE*) *E MVISION THREAT INTELLIGENCE EXCHANGE* – TIE.

Outubro/2020

Ministério do Desenvolvimento Regional – MDR
Companhia de Desenvolvimento dos Vales do São Francisco e do Parnaíba
Área de Gestão Estratégica

ÍNDICE

Ministério do Desenvolvimento Regional – MDR
Companhia de Desenvolvimento dos Vales do São Francisco e do Parnaíba
Área de Gestão Estratégica

TERMO DE REFERÊNCIA

1. OBJETO DA CONTRATAÇÃO

1.1. O objeto da presente licitação é: a CONTRATAÇÃO de atualização de licenças de uso perpétuo dos softwares da solução de segurança centralizada, já instalados na Codevasf, do tipo endpoint protection (Antvírus/Antmalware) CEB e Threat Intelligence Exchange – TIE com repasse de conhecimento, garantias e atualizações, distribuídos em 3 itens conforme descrito abaixo:

Grupo 1

Item	Tipo	Descrição	CATMAT CATSER	Unid.	Qtd.	Valor Unitário (R$)	Valor Total (R$)
1	**Atualização**	Fornecimento **de Atualização de Licenciamento da solução:** • McAfee Complete EndPoint Protection – Business - CEB de caráter perpétuo, para os ambientes Físicos e virtualizado *Vmware*;	27456	Licença	1750	R$ 125,153	R$ 219.018,33
2	**Atualização**	Fornecimento **de Atualização de Licenciamento da solução:** • McAfee MVISION Threat Intelligence Exchange – TIE de caráter perpétuo, para os ambientes Físicos e virtualizado *Vmware*;	27456	Licença	1750	R$ 57,50	R$ 100.625,00
		Total					R$ 319.643,33

Item	Tipo	Descrição	CATMAT CATSER	Unid.	Qtd.	Valor Unitário (R$)	Valor Total (R$)
3	**SERVIÇO**	Repasse de conhecimento das funcionalidades / operação da ferramenta (Treinamento)	3840	Aluno	4	R$ 3.200,00	R$ 12.800,00
		Total					R$ 12.800,00

1.2. O valor total dos itens, informados na tabela acima, foi apurado em R$ 332.443,33 (trezentos e trinta e dois mil quatrocentos e quarenta e três reais e trinta e três centavos) com base nos valores obtidos por meio da realização de pesquisa de preços, na Instrução Normativa Nº 73 de 5 de agosto de 2020.

1.3. Os recursos orçamentários correrão à conta do Programa de Trabalho 04.122.0032.2000.0001 - ADMINISTRAÇÃO DA UNIDADE - NACIONAL, Categorias Econômica 3 sob a gestão da Área de Gestão Estratégica da Codevasf – AE.

1.4. Os quantitativos foram estimados e estão demonstrados nos autos do processo desta contratação.

1.5. O valor corresponde à média dos preços pesquisados e praticados no mercado por item da tabela acima diz respeito ao período de agosto/2021 e janeiro/2022.

1.6. Os elementos técnicos descritos neste instrumento e em seus anexos são os mínimos necessários para assegurar que a contratação se dê de forma satisfatória com as mínimas condições técnicas e de qualidade exigidas, e ainda, assegurar o gasto racional dos recursos públicos.

1.7. No interesse da CONTRATANTE, e em comum acordo com a CONTRATADA, o objeto do Contrato poderá ser suprimido ou aumentado até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado da contratação, facultada a supressão além desse limite, por acordo entre as partes, conforme disposto no art. 81, inciso VI, § 1º, da Lei nº 13.303/16.

2. TERMINOLOGIAS E DEFINIÇÕES

Neste Termo de Referência (TR) ou em quaisquer outros documentos relacionados com os serviços acima solicitados, os termos ou expressões têm o seguinte significado e/ou interpretação:

TERMO DE REFERÊNCIA – Conjunto de elementos necessários e suficientes, com nível de precisão adequado, para caracterizar os bens a serem fornecidos, capazes de propiciar avaliação do custo pela administração diante de orçamento detalhado, definição dos métodos, estratégia de suprimento, valor estimado em planilhas de acordo com o preço de mercado, cronograma físico-financeiro, se for o caso, critério de aceitação do objeto, deveres da CONTRATADA e do CONTRATANTE, procedimentos de fiscalização e gerenciamento do contrato, prazo de execução e sanções, de forma clara, concisa e objetiva.

CODEVASF – Companhia de Desenvolvimento dos Vales do São Francisco e do Parnaíba – Empresa pública vinculada ao Ministério da Integração Nacional, com sede no Setor de Grandes Áreas Norte, Quadra 601 – Lote 1 – Brasília-DF.

AE/GTI ou GTI – Gerência de Tecnologia da Informação da Área de Gestão Estratégica da CODEVASF.

AE/GTI/UIT ou UIT – Unidade de Infraestrutura de TI, subordinada a Gerência de Tecnologia da Informação.

Ministério do Desenvolvimento Regional – MDR
Companhia de Desenvolvimento dos Vales do São Francisco e do Parnaíba
Área de Gestão Estratégica

LICITANTE – Empresa habilitada para apresentar proposta.

CATMAT – É um módulo do SIASG denominado Sistema de Catalogação de materiais, onde é realizada a inclusão de itens, bem como a sua consulta. Todos os procedimentos para a sua utilização constam dos Manuais disponíveis no site do Compras Governamentais: www.comprasgovernamentais.gov.br.

CONTRATO – Documento, subscrito pela CODEVASF e a CONTRATADA vencedora do certame, que define as obrigações e direitos de ambas com relação à execução dos fornecimentos.

CONTRATADA – Empresa licitante selecionada e contratada pela CODEVASF para a execução dos serviços.

ESPECIFICAÇÃO TÉCNICA – Tipo de norma destinada a fixar as características dos serviços, condições ou requisitos exigíveis para matérias primas, produtos semifabricados, elementos de construção, materiais ou produtos industriais semifabricados. Conterá a definição do serviço, descrição do método construtivo, controle tecnológico e geométrico e norma de medição e pagamento.

FISCALIZAÇÃO – Equipe da CODEVASF atuando sob a autoridade de um Coordenador, indicada para exercer em sua representação a fiscalização do contrato.

DOCUMENTOS DE CONTRATO – Conjunto de todos os documentos que integram o contrato e regulam a execução dos serviços, compreendendo o Edital, Termo de Referência, especificações técnicas, desenhos e proposta financeira da executante, cronogramas e demais documentos complementares que se façam necessários à execução dos serviços.

DOCUMENTOS COMPLEMENTARES ou SUPLEMENTARES – Documentos que, por força de condições técnicas imprevisíveis, se fizerem necessários para a complementação ou suplementação dos documentos emitidos nos Termo de Referência.

SIASG - é um conjunto informatizado de ferramentas para operacionalizar internamente o funcionamento sistêmico das atividades de gestão de materiais, edificações públicas, veículos oficiais, comunicações administrativas, licitações e contratos. É utilizado por várias entidades da Administração Pública Federal (Ministérios, Secretarias, etc.). Pode ser acessado pelo site do Compras Governamentais: www.comprasgovernamentais.gov.br.

PDTI: Plano Diretor de Tecnologia da Informação é resultado do detalhamento das ações decorrentes do Planejamento Estratégico da Tecnologia da Informação - PETI, de forma a consolidar todas as iniciativas, metas e os indicadores da área de Tecnologia da Informação, dando visibilidade às ações, prazos e custos necessários para alcance dos objetivos estratégicos definidos e, ainda, assegurando que estas ações agreguem valor ao negócio da CODEVASF.

PETI: Plano Estratégico de Tecnologia da Informação é o instrumento que tem por objetivo assegurar que as metas e objetivos da TI estejam fortemente alinhados com o Planejamento Estratégico da CODEVASF.

Ministério do Desenvolvimento Regional – MDR
Companhia de Desenvolvimento dos Vales do São Francisco e do Parnaíba
Área de Gestão Estratégica

PROPOSTA FINANCEIRA – Documento gerado pelo licitante que estabelece os valores unitário e global dos serviços e fornecimentos, apresentando todo o detalhamento dos custos e preços unitários propostos.

3. CRITÉRIO DE JULGAMENTO

3.1. **Critério de Julgamento:** Menor preço por grupo e item

3.2. **MODO DE DISPUTA: ABERTO,** com intervalo mínimo de diferença entre os lances de 0,5 % (meio por cento), do valor do item pertinente, que incidirá tanto em relação aos lances intermediários quanto e relação ao lance que cobrir a melhor oferta**.**

3.3. **Valor estimado:** Público.

4. OBJETIVO DA CONTRATAÇÃO

4.1. Garantir a proteção da infraestrutura de rede e seus ativos (desktops e servidores) contra os ataques de vírus, anti-ransomware e spam. Bem como proteger os trabalhos desenvolvidos pelos funcionários em seus computadores (estações de trabalho).

O presente objeto é de natureza comum - bens cujos padrões de desempenho e qualidade possam ser objetivamente definidos pelo edital, por meio de especificações reconhecidas e usuais do mercado.

5. DESCRIÇÃO DOS FORNECIMENTOS

5.1. O objeto da presente licitação é: a CONTRATAÇÂO de atualização de licenças de uso perpétuo dos softwares da solução de segurança centralizada, já instalados na Codevasf, do tipo endpoint protection (Antvírus/Antmalware) CEB e Threat Intelligence Exchange – TIE com repasse de conhecimento, garantias e atualizações;

5.2. As licenças devem ser disponibilizadas em meio digital, conforme distribuídos no item 1.1, grupo 1, itens 1 e 2 deste Termo de Referência.

5.3. A descrição dos fornecimentos consta nas Especificações Técnicas – Anexo A e das Planilhas de Quantidades e Preços Orçados e Escopo de Fornecimento – Anexo C deste Termo de Referência, que deverão ser observadas criteriosamente pelas licitantes.

5.4. **LOCAL DE EXECUÇÃO DOS SERVIÇOS**

5.4.1. Os serviços serão executados preferencialmente remotamente, e só em casos de não solução do problema, serão executados presencialmente.

5.4.2. Os serviços presenciais serão executados nas dependências da CONTRATANTE, por decisão unilateral da CONTRATANTE. O endereço para execução dos serviços indicado é:

UNIDADE	Endereço
Sede (Brasília – DF)	SGAN 601, Conj. I – Ed. Manoel Novaes.

5.4.3. No caso dos serviços prestados nas dependências da Codevasf e durante sua execução, o prestador de serviço da CONTRATADA deverá estar identificado por crachá da CONTRATADA e acompanhado por empregado da Unidade de Infraestrutura e Tecnologia da CONTRATANTE.

5.4.4. Os custos relacionados aos deslocamentos, ocorridos em função de entendimento, validação e/ou aceite dos serviços, serão por conta da CONTRATADA.

6. CONDIÇÕES DE PARTICIPAÇÃO

6.1. Poderão participar da presente licitação empresas do ramo, pertinente e compatível com o objeto desta licitação, nacionais ou estrangeiras, que atendam às exigências do TR e seus anexos.

6.2. As Empresas estrangeiras poderão participar nas mesmas condições das empresas nacionais.

6.3. As licitantes poderão apresentar propostas para um ou mais itens, devendo apresentar proposta para a integralidade de cada item a que concorrer, discriminados nas Especificações Técnicas – Anexo A deste Termo de Referência. Não serão aceitas propostas para parte do item, implicando na desclassificação da proposta.

6.4. CONSÓRCIO

6.4.1. Não será permitida a participação de consórcio.

6.5. SUBCONTRATAÇÃO

6.5.1. Não será permitida a subcontratação total ou parcial do objeto desta licitação.

7. PROPOSTA FINANCEIRA

7.1. As propostas financeiras deverão conter no mínimo o seguinte:

a) Planilha de preços unitários (Proposta) e totais ofertados para as licenças de software, devidamente preenchida, com clareza e sem rasuras, conforme modelo constante do Anexo c, que é parte integrante deste termo de Referência.

7.2. O prazo de validade da proposta será de 60 (sessenta) dias contados a partir da data estabelecida para entrega das mesmas, sujeita a revalidação por idêntico período.

7.3. Nos preços unitários propostos, deverão estar incluídos todos os custos que venham a incidir, direta ou indiretamente, nos fornecimentos objeto deste Termo de Referência.

7.4. Será considerada a melhor proposta, a que apresentar o menor preço para o item avaliado, conforme critérios acima estabelecidos.

8. ALTERAÇÃO SUBJETIVA

8.1. É admissível a fusão, cisão ou incorporação da CONTRATADA com/em outra pessoa jurídica, desde que sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na licitação original; sejam mantidas as demais cláusulas e condições do contrato; não haja prejuízo à execução do objeto pactuado e haja a anuência expressa da Administração à continuidade do contrato.

9. DOCUMENTAÇÃO DE HABILITAÇÃO

9.1. QUALIFICAÇÃO TÉCNICA

9.1.1. Serão aceitas propostas que atendam aos termos e condições das especificações técnicas sem desvio ou exceções aos requisitos técnicos, na forma solicitada no Anexo A deste Termo de Referência.

9.1.2. A Empresa deverá comprovar que já forneceu itens equivalentes de mesmas características com quantidades de (pelo menos 850 licenças) e compatíveis com o objeto desta licitação, itens 01 e 02, por meio da apresentação de atestados fornecidos por pessoas jurídicas, com não mais 3 anos de emissão, de direito público ou privado.

10. PRAZO DE EXECUÇÃO DOS FORNECIMENTOS

10.1. O prazo para vigência será de 30 (trinta) dias, contado a partir da data de emissão da Ordem de Fornecimento.

10.2. O prazo para execução do serviço e do fornecimento, objetos desta licitação, terá duração de 24 meses contados a partir da assinatura do contrato, podendo ser prorrogado o primeiro termo aditivo, por 24 meses, e o segundo por 12 meses.

10.3. Após avaliação da qualidade dos serviços prestados e preços praticados no mercado de forma a manter a condição mais vantajosa para a Administração Pública, no interesse de ambas as partes nos termos da Lei nº 13.303/2016, Art. 71, limitando-se a 60 meses, e em comum acordo com a CONTRATADA far-se-á a renovação do contrato.

11. FORMAS E CONDIÇÕES DE PAGAMENTO

11.1. Os pagamentos, objeto desta licitação, serão efetuados em reais, com base nos preços das licenças, efetivamente entregue, contra a apresentação das Notas Fiscais/Faturas devidamente atestadas pela Fiscalização da CODEVASF, conforme legislação vigente:

11.2. Será observado o prazo de até 30 (trinta) dias para pagamento, contado da data final do período de adimplemento de cada parcela estipulada.

11.3. A fatura só será liberada para pagamento depois de aprovada pelo fiscal do contrato e deverá estar isenta de erros ou omissões, sem o que será, de forma imediata, devolvida à CONTRATADA para correções.

11.4. Na hipótese de irregularidade no cadastro ou habilitação no SICAF, a CONTRATADA deverá regularizar a sua situação perante o cadastro no prazo de até 30 (trinta) dias, sob pena de aplicação das penalidades previstas no edital, anexo (s) e rescisão do contrato.

11.5. Qualquer atraso acarretado por parte da CONTRATADA na apresentação da fatura ou nota fiscal, ou dos documentos exigidos como condição para pagamento, importará na interrupção da contagem do prazo de vencimento do pagamento, iniciando novo prazo após a regularização da situação

11.6. A fatura emitida pela CONTRATADA deverá conter a descrição dos serviços a que se destina e seu valor em moeda corrente (Reais) sem indexação ao valor do dólar.

11.7. O pagamento será procedido de consulta ao SICAF, para comprovação de cumprimento das obrigações trabalhistas, previdenciárias e as relativas ao FGTS, correspondentes à última nota fiscal ou fatura que tenha sido paga pela CONTRATANTE.

11.8. O pagamento será creditado em nome da CONTRATADA, mediante Ordem Bancária em conta-corrente por ela indicada ou meio de Ordem Bancária para pagamento de fatura com código de barras, uma vez satisfeitas as condições estabelecidas neste Termo de Referência.

11.9. A Nota Fiscal/Fatura deverá destacar o valor do IRPJ e demais contribuições incidentes, para fins de retenção na fonte, de acordo com o art. 2º, § 6º da IN/SRF n.º 1234/2012, ou informar a isenção, não incidência ou alíquota zero, e respectivo enquadramento legal, sob pena de retenção do imposto de renda e das contribuições sobre o valor total do documento fiscal, no percentual correspondente à natureza do bem.

11.10. É de inteira responsabilidade da CONTRATADA a entrega à CONTRATANTE dos documentos de cobrança, acompanhados dos seus respectivos anexos, de forma clara, objetiva e ordenada, que se não for atendido, implica desconsideração pela CONTRATANTE dos prazos estabelecidos para conferência e pagamento.

11.11. Caso a CONTRATADA seja optante pelo Sistema Integrado de Pagamento de Impostos e Contribuições das Microempresas e Empresas de Pequeno Porte – SIMPLES, deverá apresentar, juntamente com a Nota Fiscal, a devida comprovação, a fim de evitar a retenção na fonte dos tributos e contribuições, conforme legislação em vigor.

11.12. Os valores referentes às licenças serão pagos em parcela única, após a sua ativação, atesto dos produtos, se for o caso, e da fatura pelo representante da CONTRATANTE, em moeda corrente nacional, em até 30 dias após o recebimento da fatura.

11.13. Os valores referentes ao GRUPO 1: ITENS 01, 02 serão pagos, em parcela única, mediante a entrega, instalação ou atualização e aceite do fiscal da CONTRATANTE;

11.14. Os valores referentes aos GRUPO 1- ITEM 03 será, em pagamento único, à CONTRATADA mediante execução do curso e aceite do fiscal da CONTRATANTE.

11.15. É vedado ao contratado transferir a terceiros os direitos ou créditos decorrentes do contrato.

11.16. Será considerado em atraso o pagamento efetuado após o prazo estabelecido no subitem 10.2, caso em que a CONTRATANTE pagará atualização financeira, aplicando-se a seguinte fórmula:

AM = P x I, onde:

AM = Atualização Monetária

P = Valor da Parcela a ser paga; e

I = Percentual de atualização monetária, assim apurado:

$$I = (1+im1/100)dx^{1/30} \times (1+im2/100)dx^{2/30} \times \ldots \times (1+imn/100)dx^{n/30} - 1$$, onde:

i = Variação do Índice de Custos de Tecnologia da Informação - ICTI no mês “m”;

d = Número de dias em atraso no mês “m”;

m = Meses considerados para o cálculo da atualização monetária.

12. REAJUSTAMENTO DOS PREÇOS

12.1. O preço é fixo e irreajustável pelo período de 12 meses, após a assinatura do instrumento contratual. Após esse prazo, poderá ser reajustado a contar da data de apresentação da proposta, mediante manifestação expressa da CONTRATADA, tendo como limite máximo a variação do Índice de Custos de Tecnologia da Informação - ICTI, mantido pela Fundação Instituto de Pesquisa Econômica Aplicada - IPEA, conforme fórmula abaixo. O reajuste calculado deverá ser encaminhado a CONTRATANTE para análise e posterior aprovação.

$$IR = \frac{I_{1\ mês\ renovação} - I_{0\ mês\ base}}{I_{0\ mês\ base}} \times 100$$, onde:

IR corresponde ao índice de reajustamento;

$I_{1\ mês\ renovação}$ corresponde ao valor do ICTI referente ao mês de renovação;

$I_{0\ mês\ base}$ corresponde ao valor do ICTI referente a data de apresentação da proposta.

13. RECEBIMENTO DEFINITIVO DOS FORNECIMENTOS

13.1. Após a entrega e disponibilização das licenças nos servidores da CONTRATANTE, a CONTRATADA requererá à Codevasf, através da Fiscalização, o seu recebimento provisório, que deverá ocorrer no prazo de 15 (quinze) dias da data da solicitação dos mesmos.

13.2. O recebimento definitivo do objeto, após a sua conclusão, obedecerá ao disposto no descrito abaixo:

a) Provisoriamente, pelo responsável por seu acompanhamento e fiscalização, mediante termo circunstanciado, assinado pelas partes em até 15 (quinze) dias da comunicação escrita da CONTRATADA;
b) Definitivamente, por servidor ou comissão designada pela autoridade competente, mediante termo circunstanciado, assinado pelas partes, após o decurso do prazo de observação, ou vistoria que comprove a adequação do objeto aos termos contratuais.

b1) A CONTRATADA é obrigada a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, o objeto do contrato em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou de materiais empregados.

13.3. Na hipótese de o termo circunstanciado ou a verificação a que se refere este item não serem, respectivamente, lavrado ou procedida dentro dos prazos fixados, reputar-se-ão como realizados, desde que comunicados à Administração nos 15 (quinze) dias anteriores à exaustão dos mesmos.

13.4. Os ensaios, testes e demais provas exigidas por normas técnicas oficiais para a boa execução do objeto do contrato correm por conta do contratado.

13.5. A CODEVASF rejeitará, no todo ou em parte fornecimento executado em desacordo com o contrato.

13.6. Na hipótese da necessidade de correção, será estabelecido um prazo para que a CONTRATADA, às suas expensas, complemente, refaça ou substitua as licenças rejeitadas.

13.7. A CONTRATADA entende e aceita que o pleno cumprimento do estipulado neste item é condicionante para:

a) Emissão, pela CODEVASF, do Atestado de Capacidade Técnica;
b) Emissão do Termo de Encerramento Físico (TEF); e

14. VISTORIA

14.1. As empresas interessadas na consecução dos serviços constantes no objeto deste Termo de referência poderão realizar visita técnica na cidade de Brasília/DF, no Edifício Sede da

CODEVASF localizado no endereço: SGAN Quadra 601, Conjunto I, Lote 01, Edifício CODEVASF, CEP: 70.830-901, em Brasília-DF.

14.2. A visita técnica deverá ser programada com antecedência mínima de 2 (dois) dias úteis junto à Unidade de Infraestrutura e Tecnologia por meio do e-mail ae.gti.uit@codevasf.gov.br e poderão ocorrer no máximo em até 24 horas antes do início da licitação.

14.3. A visita técnica tem a finalidade de prover ao licitante conhecimento das instalações, metodologias, arquiteturas e recursos do ambiente da CONTRATANTE para que o mesmo tenha condições de avaliar o grau de dificuldade existentes na execução dos serviços, constantes no objeto do termo de referência que possam influenciar nos custos envolvidos no fornecimento do serviço.

14.4. Os custos da vistoria são de responsabilidade da licitante, incluindo seu deslocamento ao local vistoriado.

14.5. As licitantes se obrigam a não divulgar, publicar ou fazer uso das informações recebidas durante a vistoria. A simples participação na vistoria caracteriza o compromisso irretratável de guarda do sigilo dos dados colhidos.

14.6. Não tendo realizada a vistoria, a licitante não poderá arguir desconhecimento dos processos, procedimentos, ambientes e das ferramentas utilizadas pela CONTRATANTE para se opor à manutenção dos termos e das condições de sua proposta.

14.7. Nenhuma visita será realizada sem a confirmação de seu agendamento, por e-mail, por parte da CONTRATANTE.

14.8. A vistoria é FACULTATIVA, podendo a licitante realizá-la por intermédio de representante legal.

14.9. Para a vistoria, o licitante, ou o seu representante, deverá estar devidamente identificado, e assinará a declaração de vistoria.

15. QUALIDADE TÉCNICA

15.1. Atestado(s) de qualificação técnica emitido em nome da licitante, expedido por pessoa(s) jurídica(s) de direito público ou privado, que comprove que a CONTRATADA presta ou prestou serviços de atividade pertinente e compatível em características com o objeto do Termo de Referência, conforme inciso II do art. 58 da Lei nº 13.303/16.

16. FISCALIZAÇÃO

16.1. A gestão do contrato, bem como a fiscalização da execução dos fornecimentos será realizada pela CODEVASF, por técnicos designados, a quem compete verificar se a CONTRATADA vencedora está executando os trabalhos, observando o contrato e os documentos que o integram.

16.2. A Fiscalização deverá verificar, periodicamente, no decorrer da execução do contrato, se a CONTRATADA vencedora mantém, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação, comprovada mediante consulta ao SICAF, CADIN ou certidões comprobatórias.

16.3. A Fiscalização terá poderes para agir e decidir perante a CONTRATADA, inclusive rejeitando serviços que estiverem em desacordo com o Contrato, com as Normas Técnicas vigentes relacionadas ao objeto deste Termo de Referência e com a melhor técnica consagrada pelo uso, obrigando-se desde já a CONTRATADA a assegurar e facilitar o acesso da Fiscalização, aos serviços, e a todos os elementos que forem necessários ao desempenho de sua missão.

16.4. A Fiscalização terá plenos poderes para sustar qualquer serviço que não esteja sendo executado dentro dos termos do contrato, dando conhecimento do fato à Gerência de Tecnologia da Informação, responsável pela execução do contrato.

16.5. Cabe à Fiscalização verificar a ocorrência de fatos para os quais haja sido estipulada qualquer penalidade contratual. A Fiscalização informará ao setor competente quanto ao fato, instruindo o seu relatório com os documentos necessários, e em caso de multa, a indicação do seu valor.

16.6. Das decisões da Fiscalização poderá a CONTRATADA recorrer à Gerência de Tecnologia da Informação da CODEVASF, responsável pelo acompanhamento do contrato, no prazo de 10 (dez) dias úteis da respectiva comunicação. Os recursos relativos a multas serão feitos na forma prevista na respectiva cláusula.

16.7. A ação e/ou omissão, total ou parcial, da Fiscalização não eximirá a CONTRATADA da integral responsabilidade pela execução do objeto deste contrato.

16.8. Fica assegurado aos técnicos da CODEVASF o direito de, a seu exclusivo critério, acompanhar, fiscalizar e participar, total ou parcialmente, diretamente ou através de terceiros, da execução dos serviços prestados pela licitante vencedora, com livre acesso ao local de trabalho para obtenção de quaisquer esclarecimentos julgados necessários à execução dos serviços.

17. CRITÉRIOS DE SUSTENTABILIDADE AMBIENTAL

17.1. A licitante vencedora deverá observar os seguintes critérios de sustentabilidade ambiental, no que couber, conforme a instrução normativa SLTI/MP nº 01/2010:

a) Que os bens sejam constituídos, no todo ou em parte, por material reciclado, atóxico, biodegradável, conforme ABNT NBR – 15448-1 e 15448-2;

b) Que sejam observados os requisitos ambientais para a obtenção de certificação do Instituto Nacional de Metrologia, Normalização e Qualidade Industrial – INMETRO como produtos sustentáveis ou de menor impacto ambiental em relação aos seus similares;

c) Que os bens devam ser, preferencialmente, acondicionados em embalagem adequada, com o menor volume possível, que utilize materiais recicláveis, de forma a garantir a máxima proteção durante o transporte e o armazenamento;

d) Que os bens não contenham substâncias perigosas em concentração acima da recomendada na diretiva RoHS (*Restriction of Certain Hazardous Substances*), tais

como mercúrio (Hg), chumbo (Pb), cromo hexavalente (Cr(VI)), cádmio (Cd), bifenil-polibromados (PBBs), éteres difenil-polibromados (PBDEs).

A licitante vencedora deverá apresentar certificação emitida por instituição pública oficial ou instituição credenciada, ou por qualquer outro meio de prova que ateste que o bem fornecido cumpre com as exigências supracitadas.

Em caso de inexistência de certificação que ateste a adequação, a CODEVASF poderá realizar diligências para verificar a adequação do produto às exigências deste TR, antes da assinatura do contrato, correndo as despesas por conta da licitante vencedora. Caso não se confirme a adequação do produto, a proposta vencedora será desclassificada.

17.2. Caso a CONTRATADA deverá comprovar a adoção de práticas de desfazimento sustentável ou reciclagem dos bens que forem inservíveis para o processo de reutilização.

18. OBRIGAÇÕES DA CONTRATADA

18.1. Alocar todos os recursos necessários para obter uma perfeita execução dos serviços previstos no objeto deste TERMO DE REFERÊNCIA, de forma plena e satisfatória, sem ônus adicionais de qualquer natureza para a CODEVASF, além dos valores estipulados na Proposta Comercial.

18.2. Realizar a entrega das licenças, bem como todas as senhas e chaves, conforme estabelecido no termo de contrato e/ou ordem de fornecimento dentro de elevados padrões éticos e profissionais.

18.3. Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação.

18.4. A CONTRATADA deverá indicar um preposto para representá-la durante o período de vigência do contrato, o qual deverá ser indicado mediante declaração em que deverá constar o nome completo, nº CPF, nº do documento de identidade.

18.5. Atender prontamente quaisquer orientações e exigências do fiscal do contrato, inerentes à execução do objeto contratual.

18.6. Reparar quaisquer danos diretamente causados à CONTRATANTE ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução dos serviços pela CONTRATANTE.

18.7. Em caso de insucesso de contato direto com o fabricante, a CONTRATADA deverá intermediá-lo, a fim de obter as licenças e atualizações.

18.8. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato.

18.9. A CONTRATADA deverá investir em medidas de promoção da ética e de prevenção da corrupção que contribuam para um ambiente mais íntegro, ético e transparente no setor privado e em suas relações como o setor público, comprometendo-se a atuar contrariamente a quaisquer manifestações de corrupção, atuando junto a seus fornecedores e parceiros privados a também

conhecer e cumprir as previsões da Lei 12.846/2013,do Decreto nº 8.420/15, da lei 13.303/2016, e da Política de Integridade da Codevasf, abstendo-se, ainda, de cometer atos tendentes a lesar a Administração Pública, denunciando a prática de irregularidades que tiver conhecimento por meios dos canais de denúncias disponíveis.

18.10. Garantir a atualização dos softwares, a qual, deverá ser prestada pelo fabricante, contemplando suporte telefônico em regime 24x7x365 (vinte quatro horas, sete dias por semana, e trezentos e sessenta e cinco dias por ano);

18.11. Garantir as evoluções de versões, quando aplicável, e qualquer outro meio para manter os softwares atualizados em sua última versão que será prestado durante a vigência do contrato;

18.12. Garantir a abertura de chamados: Estes deverão ser abertos no fabricante, através do número telefônico 0800 ou através de endereço web, fornecendo neste momento o número, data e hora da abertura do chamado. Este será considerado o início da contagem dos prazos estabelecidos;

18.13. Caso a CONTRATADA não seja o fabricante do produto, deverá comprovar que é uma revendedora autorizada para os produtos envolvidos no presente certame.

18.14. Apresentação de declaração do licitante, no ato da contatação (ou da assinatura da ordem de fornecimento), que ateste a não ocorrência do registro de oportunidade, de modo a garantir o princípio constitucional da isonomia e a seleção da proposta mais vantajosa para a Administração Pública.

19. SEGURANÇA DA INFORMAÇÃO

19.1. Os procedimentos mínimos de segurança exigidos da empresa CONTRATADA são:

19.1.1. Credenciar junto a CONTRATANTE, seus profissionais autorizados a retirar e a entregar documentos, bem como daqueles que venham a ser designados para prestar serviços nas dependências da CODEVASF.

19.1.2. Identificar qualquer equipamento das empresas que venha a ser instalado nas dependências da CONTRATANTE, utilizando placas de controle patrimonial, selos de segurança etc.

19.1.3. Manter sigilo absoluto sobre informações, dados e documentos integrantes dos serviços a serem executados na CONTRATANTE.

19.1.4. Abster-se, qualquer que seja a hipótese, de veicular publicidade ou qualquer outra informação acerca das atividades objeto do Termo de referência, sem prévia autorização.

19.1.5. Observar, rigorosamente, todas as normas e procedimentos de segurança implementados no ambiente de Tecnologia da Informação - TI da CODEVASF.

19.1.6. Adotar critérios adequados para o processo seletivo dos profissionais, com o propósito de evitar a incorporação de pessoas com características e/ou antecedentes que possam comprometer a segurança ou credibilidade da CONTRATANTE.

19.1.7. Comunicar com antecedência mínima de 3 (três) dias ao Representante da CONTRATANTE qualquer ocorrência de transferência, remanejamento ou demissão, para que seja providenciada a revogação de todos os privilégios de acesso aos sistemas, informações e recursos da empresa.

19.1.8. Manter sigilo sobre todos os ativos de informações e de processos da CONTRATANTE.

19.1.9. Documento assinado digitalmente. Para verificar as assinaturas, acesse https://ecodevasf.codevasf.gov.br?a=autenticidade e informe o e-DOC C98E2A2B9 Ministério do Desenvolvimento Regional – MDR Companhia de Desenvolvimento dos Vales do São Francisco e do Parnaíba Área de Gestão Estratégica.

19.1.10. Adotar a Política de Segurança da Informação da Codevasf (Posin), publicada no sítio da empresa, para o exercício de suas atividades no âmbito da Codevasf.

19.1.11. A Contratada deve firmar aderência, ciência e concordância com as normas, políticas e práticas estabelecidas no Código de Conduta Ética e Integridade da Codevasf e compromete-se a respeitá-las e cumpri-las integralmente, bem como fazer com que seus empregados o façam quando no exercício de suas atividades nas dependências da Codevasf ou para a Empresa.

20. GARANTIA DE EXECUÇÃO

20.1.1. Como garantia para a completa execução das obrigações contratuais e da liquidação das multas convencionais, fica estipulada uma "Garantia de Execução" no montante de 5% (cinco por cento) do valor da ordem de fornecimento, para os bens de valor unitário acima de R$ 100.000,00, em espécie, Seguro Garantia emitida por seguradora autorizada pela SUSEP ou Fiança Bancária, a critério da contratada.

20.1.2. A garantia a que se refere o subitem acima deverá ser entregue na Área de Gestão Estratégica da Codevasf, quando da assinatura da ordem de fornecimento pela contratada, ou seja, quando da devolução da Ordem de Fornecimento assinada pela contratada.

20.1.3. A garantia na forma de Carta de Fiança Bancária ou seguro garantia deverão estar em vigor e cobertura até 90 (noventa) dias após o prazo final de entrega do objeto contratado.

20.1.4. Após a assinatura do Termo de Encerramento Físico do contrato será devolvida a “Caução de Execução”, uma vez verificada a perfeita execução do objeto contratual.

20.1.5. A garantia em espécie deverá ser depositada em instituição financeira oficial, credenciada pela Codevasf, em conta remunerada que poderá ser movimentada somente por ordem da Codevasf.

20.1.6. A não integralização da garantia representa inadimplência contratual, passível de aplicação de multas e de rescisão, na forma prevista nas cláusulas contratuais.

20.1.7. Por ocasião de eventuais aditamentos contratuais que promovam acréscimos ao valor contratado ou prorrogações de prazo contratual, a garantia prestada deverá ser

reforçada e/ou renovada, de forma a manter a observância do disposto no caput desta cláusula, em compatibilidade com os novos valores e prazos pactuados.

20.1.8. Não haverá qualquer restituição de garantia em caso de dissolução contratual, na forma do Disposto na cláusula de rescisão, hipótese em que a garantia reverterá e será apropriada pela Codevasf.

20.1.9. A Contratada deverá manter atualizada a garantia contratual até 90(noventa) dias após o recebimento provisório do objeto contratado.

20.1.10. A garantia, qualquer que seja a modalidade escolhida, assegurará o pagamento de:

- a) Prejuízos advindos do não cumprimento do objeto do contrato;
- b) Prejuízos diretos causados à Administração decorrentes de culpa ou dolo durante a Execução do contrato;
- Multas moratórias e punitivas aplicadas pela Administração à contratada; e
- d) Obrigações trabalhistas e previdenciárias de qualquer natureza, não adimplidas pela Contratada, quando couber.

21. MULTAS

21.1. Nos casos de inexecução total do contrato, por culpa exclusiva da CONTRATADA, cabe a aplicação de multa de até 10% (dez por cento) do contrato ou ordem de fornecimento, independente das demais sanções previstas no Regulamento Interno de Licitações e Contratos.

21.2. Nos casos de inexecução parcial do objeto, por culpa exclusiva da CONTRATADA, será cobrada multa de até 10% (dez por cento) do valor da parte não executada do contrato, sem prejuízo da responsabilidade civil e perdas das garantias contratuais.

21.3. Nos casos de atrasos na execução dos fornecimentos descritos no cronograma físico do objeto ou no atendimento às exigências contratuais e editalícias, por conta exclusiva da CONTRATADA, aplicar-se-á multa moratória conforme os graus de penalidades estabelecidos abaixo:

21.4. Graus de Penalidade:

- Grau 01 – multa de R$ 100,00 (cem reais) por dia de atraso;
- Grau 02 – multa de R$ 500,00 (quinhentos reais) por dia;
- Grau 03 – multa de 0,2% por dia sobre o valor total do item estimado no cronograma físico-financeiro para o período;
- Grau 04 – multa de 0,2% por dia sobre o valor contratual atualizado

Tabela 01 – Inadimplências e o respectivo grau de penalidade

Inadimplências	Grau de Penalidade
Pelo não atendimento à determinação estipulada pela Fiscalização, no prazo por ela estabelecido, desde seja comunicada à Contratada, através de comunicação formal do fiscal	01
Pela não apresentação de itens exigidos em cláusula editalícias ou contratuais, dentro do prozo estabelecido.	02
Por dificultar ou impedir o acesso da Fiscalização a documentos	02
Pelo atraso no cumprimento dos prazos estabelecidos no cronograma físico do objeto, desde que injustificados ou cuja a justificativa não tenha sido aceita pela fiscalização	03
Pelo atraso na conclusão do objeto, em conformidade com o prazo contratado ou aditado	04

21.5. Comprovando o impedimento ou reconhecida a força maior, devidamente justificados e aceitos pela FISCALIZAÇÃO, em relação a um dos eventos arrolados na Tabela 01, a CONTRATADA ficará isenta das penalidades mencionadas.

21.6. Ocorrida a inadimplência, a multa será aplicada pela Codevasf, após regular processo administrativo, observando-se o seguinte:

a) A multa será descontada da garantia prestada pela contratada;
b) Caso o valor da multa seja de valor superior ao valor da garantia prestada, além da perda desta, responderá a contratada pela sua diferença, a qual será descontada dos pagamentos eventualmente devidos pela Administração ou ainda, quando for o caso, cobrada judicialmente;
c) Caso o valor do faturamento seja insuficiente para cobrir a multa, a contratada será convocada para complementação do seu valor no prazo de 5 (cinco) dias a contar da data da convocação;
d) Não havendo qualquer importância a ser recebida pela contratada, esta será convocada a recolher à Gerência de Finanças da Codevasf – AA/GFN o valor total da multa, no prazo de 5 (cinco) dias, contado a partir da data da comunicação.

21.7. O licitante vencedor terá um prazo inicialmente de 10(dez) dias úteis para defesa prévia e, posteriormente, diante de uma eventual decisão que lhe tenha sido desfavorável, terá mais um prazo de 05(cinco) dias úteis, contado a partir da data de cientificação da aplicação multa, para apresentar recurso à Codevasf. Ouvida a fiscalização e acompanhamento do contrato, o recurso será encaminhado à Assessoria Jurídica da Superintendência Regional/Sede, que procederá ao seu exame.

21.8. Após o procedimento estabelecido no item anterior, o recurso será apreciado pela Diretoria Executiva da Codevasf, que poderá relevar ou não a multa.

21.9. Em caso de relevação da multa, a Codevasf se reserva o direito de cobrar perdas e danos porventura cabíveis em razão do inadimplemento de outras obrigações, não constituindo a relevação novação contratual nem desistência dos direitos que lhe forem assegurados.

21.10. Caso a Diretoria Executiva mantenha a multa, não caberá novo recurso administrativo.

22. SANÇÔES ADMINSTRATIVAS

22.1. Ficará impedido de licitar e de contratar com a União e será descredenciado no Sicaf, pelo prazo de até cinco anos, sem prejuízo das multas previstas em edital e no contrato e das demais cominações legais, garantido o direito à ampla defesa, o licitante que, convocado dentro do prazo de validade de sua proposta:

a) Não assinar o contrato ou a ata de registro de preços;
b) Não entregar a documentação exigida no edital;
c) Apresentar documentação falsa;
d) Causar o atraso na execução do objeto;
e) Não mantiver a proposta;
f) Falhar na execução do contrato;
g) Fraudar a execução do contrato;
h) Comportar-se de modo inidôneo;
i) Declarar informações falsas; e
j) Cometer fraude fiscal.

22.2. Nos certames realizados pela modalidade Pregão, aplica-se ao contratado, no que couber, a penalidade prevista no art. 7º da Lei nº 10.520, de 17 de julho de 2002, exclusivamente quanto aos ilícitos praticados durante a etapa da licitação.

22.3. Aos atos praticados após a etapa da licitação, será aplicada a suspensão temporária de participação em licitação e impedimento de contratar COM A CODEVASF, no prazo de até 2 (dois) anos, previsto no art. 83 da Lei 13.303/2016.

22.4. Reputar-se-ão inidôneos atos como os descritos nos artigos 337-E a 337-P do DecretoLei nº 2.848/1940, nos termos do art. 41 da Lei 13.303/2016

22.5. Poderão ser aplicadas ainda as seguintes sanções:

a) Advertência;
b) Multa, conforme previsto no item 21 do Termo de Referência, Anexo I deste Edital;
c) Suspensão temporária

22.6. Deve ser garantido o contraditório e a ampla defesa na aplicação das sanções administrativas, mediante abertura de prazo de 10 (dez) dias úteis para defesa.

22.7. A multa, aplicada após regular processo administrativo, deve ser descontada da garantia do respectivo contratado.

22.8. As sanções de advertência e de suspensão temporária de participação em licitação e impedimento de contratar podem ser cumuladas com a de multa, devendo a defesa prévia do interessado, no respectivo processo, ser apresentada no prazo de 10 (dez) dias úteis

22.9. A sanção de suspensão, prevista no subitem 20.1 observará os parâmetros estabelecidos no Regulamento de Licitações e Contratos da CODEVASF, e pode ser aplicada às empresas ou aos profissionais que, em razão dos contratos:

a) Tenham sofrido condenação definitiva por praticarem, por meios dolosos, fraude fiscal no recolhimento de quaisquer tributos;
b) Tenham praticado atos ilícitos visando a frustrar os objetivos da licitação; ou
c) Demonstrem não possuir idoneidade para contratar com a CODEVASF, em virtude de atos ilícitos praticados.

22.10. Aplicar-se-á **à presente licitação as sanções administrativas, criminais e demais regras previstas no Capítulo II, Seção III da Lei nº 13.303/2016 e artigos 337-E a 337- P do Decreto-Lei nº 2.848/1940, conforme preconiza o art. 41 da Lei 13.303/2016**.

22.11. As penalidades serão obrigatoriamente registradas no SICAF, e no caso de suspensão de licitar, o licitante deverá ser descredenciado por igual período, sem prejuízo das multas previstas neste Edital e das demais cominações legais.

22.12. Caberá recurso no prazo de cinco dias úteis contado a partir da data da intimação ou da lavratura da ata da aplicação das penas de advertência, multa, suspensão temporária de participação em licitação, impedimento de contratar com a Administração Pública e declaração de inidoneidade.

23. OBRIGAÇÕES DA CODEVASF

23.1. Exigir o cumprimento de todas as obrigações assumidas pela CONTRATADA, de acordo com as cláusulas contratuais e os termos de sua proposta.

23.2. Esclarecer as dúvidas que lhe sejam apresentadas pela CONTRATADA, através de correspondências protocoladas.

23.3. Fiscalizar e acompanhar a execução do objeto do contrato.

23.4. Expedir por escrito, as determinações e comunicações dirigidas a CONTRATADA, determinando as providências necessárias à correção das falhas observadas.

23.5. Rejeitar todo e qualquer serviço inadequado, incompleto ou não especificado e estipular prazo para sua retificação.

23.6. Emitir parecer para liberação das faturas, e receber os fornecimentos/serviços contratados.

23.7. Efetuar o pagamento no prazo previsto no contrato.

24. CONDIÇÕES GERAIS

24.1. Este Termo de Referência e seus anexos farão parte integrante do contrato a ser firmado com a CONTRATADA, independente de transições.

25. ANEXOS

25.1. São ainda, documentos integrantes deste Termo de Referência, CD-ROM contendo:

- Anexo A – Especificações Técnicas dos Serviços e Soluções
- Anexo B – Justificativa
- Anexo C – Escopo de Fornecimento e planilhas de quantidades e preços máximos
- Anexo D – Planilha de Riscos
- Anexo E – Propostas

Ministério do Desenvolvimento Regional – MDR
Companhia de Desenvolvimento dos Vales do São Francisco e do Parnaíba
Área de Gestão Estratégica

ANEXO A

Especificações Técnicas dos Serviços e Soluções

Ministério do Desenvolvimento Regional – MDR
Companhia de Desenvolvimento dos Vales do São Francisco e do Parnaíba
Área de Gestão Estratégica

ANEXO B

JUSTIFICATIVAS

.

Ministério do Desenvolvimento Regional – MDR
Companhia de Desenvolvimento dos Vales do São Francisco e do Parnaíba
Área de Gestão Estratégica

ANEXO C

Escopo de Fornecimento e planilhas de quantidades e preços máximos

Ministério do Desenvolvimento Regional – MDR
Companhia de Desenvolvimento dos Vales do São Francisco e do Parnaíba
Área de Gestão Estratégica

ANEXO D
Planilha de Riscos

Ministério do Desenvolvimento Regional – MDR
Companhia de Desenvolvimento dos Vales do São Francisco e do Parnaíba
Área de Gestão Estratégica

ANEXO E
Propostas

CODEVASF
Ministério do Desenvolvimento Regional – MDR
Companhia de Desenvolvimento dos Vales do São Francisco e do Parnaíba
Área de Gestão Estratégica

ANEXO A – Especificação Técnica dos Serviços e Soluções

1. OBJETO

1.1. O objeto da presente licitação é: a CONTRATAÇÃO de atualização de licenças de uso perpétuo dos softwares da solução de segurança centralizada, já instalados na Codevasf, do tipo endpoint protection (Antvírus/Antmalware) CEB e Threat Intelligence Exchange – TIE com repasse de conhecimento, garantias e atualizações, distribuídos em 4 itens conforme descrito abaixo:

2. CLASSIFICAÇÃO DO SERVIÇO

2.1. Os serviços a serem executados são:

GRUPO 1

Item	Tipo	Descrição	CATMAT CATSER	Unid.	Qtd.	Valor Unitário (R$)	Valor Total (R$)
1	**Atualização**	Fornecimento **de Atualização de Licenciamento da solução:** • McAfee Complete EndPoint Protection – Business - CEB de caráter perpétuo, para os ambientes Físicos e virtualizado *Vmware*;	27456	Licença	1750		
2	**Atualização**	Fornecimento **de Atualização de Licenciamento da solução:** • McAfee MVISION Threat Intelligence Exchange – TIE de caráter perpétuo, para os ambientes Físicos e virtualizado *Vmware*;	27456	Licença	1750		

Item	Tipo	Descrição	CATMAT CATSER	Unid.	Qtd.	Valor Unitário (R$)	Valor Total (R$)
3	SERVIÇO	Repasse de conhecimento das funcionalidades / operação da ferramenta (Treinamento)	3840	Aluno	4		

3. FORNECIMENTO DE ATUALIZAÇÃO DE LICENCIAMENTO DA SOLUÇÃO: MCAFEE COMPLETE ENDPOINT PROTECTION – BUSINESS - CEB E MCAFEE MVISION THREAT INTELLIGENCE EXCHANGE – TIE PARA OS AMBIENTES FÍSICOS E VIRTUALIZADO VMWARE - ITEM 01 E 02

3.1. CARACTERÍSTICAS GERAIS DA SOLUÇÃO

3.1.1. Deve possuir capacidade de instalação e pleno funcionamento dos módulos solicitados em estações de trabalho com no mínimo 3Gb de memória RAM.

3.1.2. Deve suportar as seguintes plataformas clientes:

3.1.2.1. Windows 11;

3.1.2.2. Windows 10;

3.1.2.3. Windows 8.1;

3.1.2.4. Windows 8;

3.1.2.5. Monterey 12.0;

3.1.2.6. Big Sur 11.0.x, 11.1 e/ou superiores;

3.1.2.7. Catalina 10.15.6 e superiores;

3.1.3. Deve suportar as seguintes plataformas servidores:

3.1.3.1. Windows Server 2019;

3.1.3.2. Windows Server 2016;

3.1.3.3. Windows Server 2012 R2;

3.1.3.4. Windows Server 2012;

3.1.4. Deve inclusive suportar o modo Server Core.

3.1.5. Deve suportar, **pelo menos as funções de antivírus e firewall de host**, nas seguintes distribuições de Linux:

3.1.5.1. Red Hat Enterprise 7.x e 8.x, 64bits;

3.1.5.2. SUSE Linux Enterprise Server 12.x e 15.x, 64bits;

3.1.5.3. Ubuntu 16.04, 18.04, 19.10, 20.04, 20.10 64bits;

3.1.5.4. CentOS 7.x e 8.x, 64bits;

3.1.5.5. Oracle Linux 7 e 8, 64bits;

3.1.6. Deve suportar a instalação de agente nos sistemas operacionais acima virtualizados nas seguintes plataformas:

3.1.6.1. AWS;

3.1.6.2. Azure;

3.1.6.3. Citrix XenApp;

3.1.6.4. Citrix XenDesktop;

3.1.6.5. Citrix XenServer;

3.1.6.6. Microsoft Hyper-V 2012 R2;

3.1.6.7. Vmware ESXi;

3.1.6.8. Vmware Player;

3.1.6.9. Vmware vShpere;

3.1.6.10. Vmware Workstation;

3.1.7. A solução deve compreender, no mínimo, as seguintes funcionalidades:

3.1.7.1. Módulo antimalware;

3.1.7.2. Módulo de firewall de host;

3.1.7.3. Módulo de filtragem web;

3.1.7.4. Módulo de proteção contra ameaças avançadas;

3.1.7.5. Módulo de reputação de arquivos;

3.1.7.6. Módulo para controle de dispositivos;

3.1.7.7. Módulo de criptografia;

3.1.7.8. Módulo para controle de aplicações;

3.1.8. Todas as funcionalidades deverão ser geridas por uma console única com as capacidades mínimas de:

3.1.8.1. Relatórios;

3.1.8.2. Dashboards;

3.1.8.3. Políticas;

3.1.8.4. Configuração;

3.1.8.5. Instalação/Desinstalação;

3.1.9. O cliente deve ser capaz de operar em modo autônomo (self-managed) e permitir que as configurações sejam aplicadas diretamente no cliente.

3.1.10. O cliente deve ser capaz de atualizar as definições para detecção de ameaças, patches e hotfixes a partir de um servidor definido pelo administrador ou diretamente nos servidores do fabricante.

3.1.11. A solução de prevenção deve ser colaborativa, ou seja, os módulos exigidos devem ser capazes de trocarem informações para uma análise mais inteligente;

3.1.12. A solução deve possuir múltiplas camadas de proteção, não serão aceitas soluções baseadas apenas em assinaturas;

3.1.13. A solução deve conter módulo capaz de garantir uma navegação web segura, prevenindo contra sites maliciosos, downloads de ameaças e garantir a política de acesso (Permitir/Negar)

3.2. Características Módulo Antimalware (Clientes Windows)

3.2.1. Características da prevenção contra exploração

3.2.1.1. Deve ser possível selecionar, no mínimo, dois modos de proteção (Padrão/Máximo).

3.2.1.2. Deve ser possível ativar/desativar a proteção contra escalonamento de privilégios genéricos.

3.2.1.3. Deve ser possível ativar/desativar a prevenção de execução de dados do Windows.

3.2.1.4. Deve ser possível selecionar dentre as ações de apenas bloquear ou apenas relatar ou bloquear e relatar;

3.2.1.5. Deve ser possível bloquear contra falsificação de IP (IP Spoofing).

3.2.1.6. Deve ser possível incluir exclusões por:

3.2.1.6.1. Processo

3.2.1.6.1.1. Nome;

3.2.1.6.1.2. Caminho do Arquivo;

3.2.1.6.1.3. Hash MD5

3.2.1.6.2. Módulo chamador

3.2.1.6.2.1. Nome

3.2.1.6.2.2. Caminho

3.2.1.6.2.3. Hash MD5

3.2.1.6.2.4. Signatário Digital

3.2.2. Características da Proteção de acesso

3.2.2.1. Deve fornecer regras de proteção de maneira nativa, ou seja, pré-definidas pelo fabricante da solução, no mínimo, para:

3.2.2.1.1. Acesso remoto a pastas locais;

3.2.2.1.2. Alteração políticas de direitos dos usuários;

3.2.2.1.3. Alterar os registros de extensão dos arquivos;

3.2.2.1.4. Criação de novos arquivos na pasta Arquivo de Programas;

3.2.2.1.5. Criação de novos executáveis na pasta Windows;

3.2.2.1.6. Criar/Modificar remotamente arquivos Portable Executable, INI, PIF e as localizações do sistema;

3.2.2.1.7. Criar ou Modificar remotamente arquivos ou pastas;

3.2.2.1.8. Desativar o editor de registro e o gerenciador de tarefas;

3.2.2.1.9. Executar arquivos das pastas do usuário;

3.2.2.1.10. Execução de scripts pelo host de script do Windows;

3.2.2.1.11. Instalar objetos de ajuda a navegação ou extensões de shell;

3.2.2.1.12. Instalar novos CLSIDs, APPIDs e TYPELIBs;

3.2.2.1.13. Modificar configurações de rede;

3.2.2.1.14. Modificar configurações do Internet Explorer;

3.2.2.1.15. Modificar processos principais do Windows;

3.2.2.1.16. Navegadores iniciando programas da pasta de downloads;

3.2.2.1.17. Registrar programas para execução automática;

3.2.2.2. As regras especificadas devem permitir o:

3.2.2.2.1. Bloqueio, ou

3.2.2.2.2. Evento de Informação, ou

3.2.2.2.3. Bloqueio e Evento de Informação;

3.2.2.3. Deve permitir ao administrador criar regras de customizadas com no mínimo os seguintes parâmetros:

3.2.2.3.1. Processos;

3.2.2.3.1.1. Nome do processo;

3.2.2.3.1.2. Hash MD5;

3.2.2.3.1.3. Assinatura Digital;

3.2.2.3.2. Usuário;

3.2.2.3.3. Arquivos;

3.2.2.3.3.1. Criação;

3.2.2.3.3.2. Deletar;

3.2.2.3.3.3. Executar;

3.2.2.3.3.4. Alteração de permissão;

3.2.2.3.3.5. Leitura;

3.2.2.3.3.6. Renomear;

3.2.2.3.3.7. Escrever;

3.2.2.3.4. Chave de Registro

3.2.2.3.4.1. Escrever;

3.2.2.3.4.2. Criar;

3.2.2.3.4.3. Deletar;

3.2.2.3.4.4. Ler;

3.2.2.3.4.5. Enumerar;

3.2.2.3.4.6. Carregar;

3.2.2.3.4.7. Substituir;

3.2.2.3.4.8. Restaurar;

3.2.2.3.5. Alterar permissão;

3.2.2.3.6. Valor de Registro

3.2.2.3.6.1. Ler;

3.2.2.3.6.2. Criar;

3.2.2.3.6.3. Deletar;

3.2.2.3.7. Processo

3.2.2.3.7.1. Qualquer acesso;

3.2.2.3.7.2. Criar thread;

3.2.2.3.7.3. Modificar;

3.2.2.3.7.4. Terminar;

3.2.2.3.7.5. Executar;

3.2.2.4. Deve permitir a configuração de exclusões;

3.2.3. Características da varredura ao acessar

3.2.3.1. A Varredura deve ser passível de habilitação/desativação por opção do administrador;

3.2.3.2. Deve iniciar a proteção durante a inicialização do sistema operacional;

3.2.3.3. Deve ser capaz de realizar análise no setor de boot;

3.2.3.4. O administrador da solução deve especificar o tempo máximo de análise para um único arquivo;

3.2.3.5. Deve analisar dos processos durante inicialização do serviço e na atualização de conteúdo;

3.2.3.6. Deve possibilitar ao administrador a análise de instaladores confiáveis;

3.2.3.7. Deve realizar análise durante cópia entre pastas locais;

3.2.3.8. A solução deve possuir conexão com Centro de Inteligência do fabricante, passível de ativação ou desativação por parte do administrador;

3.2.3.9. Deve permitir a configuração do nível de agressividade da análise entre:

3.2.3.9.1. Muito Baixo

3.2.3.9.2. Baixo

3.2.3.9.3. Médio

3.2.3.9.4. Alto

3.2.3.9.5. Muito Alto

3.2.3.10. Deve possibilitar aplicar as configurações a todos os processos do sistema operacional ou a uma lista específica criada pelo administrador;

3.2.3.11. Deve realizar varredura quando o processo:

3.2.3.11.1. Ler o disco;

3.2.3.11.2. Gravar no disco;

3.2.3.11.3. Deixar a solução decidir;

3.2.3.12. Deve possibilitar análise em

3.2.3.12.1. Unidades de Rede;

3.2.3.12.2. Arquivos abertos para backup;

3.2.3.12.3. Arquivos compactados, por exemplo .jar;

3.2.3.12.4. Arquivos codificados (MIME);

3.2.3.13. Deve detectar programas indesejados, ameaças em programas desconhecidos e ameaças em macro desconhecidas;

3.2.3.14. Deve permitir selecionar, no mínimo, uma das seguintes opções de ação após detectar uma ameaça:

3.2.3.14.1. Limpar o arquivo;

3.2.3.14.2. Excluir o arquivo;

3.2.3.14.3. Negar acesso ao arquivo;

3.2.3.15. Deve permitir selecionar, no mínimo, uma das seguintes opções de ação após detectar um programa indesejado:

3.2.3.15.1. Limpar o arquivo;

3.2.3.15.2. Excluir o arquivo;

3.2.3.15.3. Permitir acesso ao arquivo;

3.2.3.15.4. Negar acesso ao arquivo;

3.2.3.16. Deve possibilitar ao administrador a gestão de uma lista de exclusões;

3.2.3.17. Deve possuir módulo capaz de interceptar scripts (Javascript e VBScript) destinados ao Windows Host Scripting e analisá-lo para indicar se é malicioso ou não;

3.2.3.18. Deve permitir a criação de listas de exclusão de URLs que não sofrerão interceptação e análise de scripts;

3.2.3.19. Ao detectar uma ameaça o agente deverá emitir uma notificação ao usuário com uma mensagem a ser customizada pelo administrador da solução.

3.2.4. **Características da Varredura sob demanda**

3.2.4.1. Deve ser possível realizar varreduras agendadas com periodicidade diária ou semanal.

3.2.4.2. Deve permitir a criação de repetição da tarefa.

3.2.4.3. Deve permitir definir a hora da execução da tarefa de análise;

3.2.4.4. Deve permitir a criação da tarefa de varredura de maneira aleatória;

3.2.4.5. Deve permitir a realização de varreduras agendadas após logon do usuário ou durante inicialização do sistema operacional.

3.2.4.6. Deve permitir escolher (um ou mais) os alvos da varredura, dentre eles:

3.2.4.6.1. Os locais da varredura:

3.2.4.6.1.1. Memória para rootkits;

3.2.4.6.1.2. Processos em execução;

3.2.4.6.1.3. Arquivos registrados;

3.2.4.6.1.4. Meu computador;

3.2.4.6.1.5. Todas as unidades locais;

3.2.4.6.1.6. Todas as unidades fixas;

3.2.4.6.1.7. Todas as unidades removíveis;

3.2.4.6.1.8. Todas as unidades mapeadas;

3.2.4.6.1.9. Pasta inicial;

3.2.4.6.1.10. Pasta de perfil do usuário;

3.2.4.6.1.11. Pasta Windows;

3.2.4.6.1.12. Pasta de arquivos de programas;

3.2.4.6.1.13. Pasta temporária;

3.2.4.6.1.14. Lixeira;

3.2.4.6.1.15. Arquivo ou pasta especificada pelo administrador;

3.2.4.6.1.16. Setor de inicialização (boot);

3.2.4.6.1.17. Arquivos compactados;

3.2.4.6.1.18. Arquivos MIME;

3.2.4.6.2. Os tipos de arquivos que serão analisados;

3.2.4.6.3. Opções adicionais, como por exemplo detecção de programas indesejados, ameaças em programas desconhecidos e ameaças em macro desconhecidas.

3.2.4.6.4. Áreas de exclusão que não deverão ser varridas;

3.2.4.7. Deve permitir a integração com o Centro de Inteligência do fabricante durante a varredura agendada.

3.2.4.8. Deve permitir selecionar, no mínimo, uma das seguintes opções de ação após detectar uma ameaça:

3.2.4.8.1. Limpar o arquivo;

3.2.4.8.2. Excluir o arquivo;

3.2.4.8.3. Negar acesso ao arquivo;

3.2.4.9. Deve permitir selecionar, no mínimo, uma das seguintes opções de ação após detectar um programa indesejado:

3.2.4.9.1. Limpar o arquivo;

3.2.4.9.2. Excluir o arquivo;

3.2.4.9.3. Permitir acesso ao arquivo;

3.2.4.9.4. Negar acesso ao arquivo;

3.2.4.10. Para minimizar o impacto ao usuário, a solução deve permitir:

3.2.4.10.1. Utilização de cache, ou seja, arquivos que já foram analisados e não tiveram seu conteúdo alterado não serão novamente analisados;

3.2.4.10.2. Iniciar a varredura apenas quando o sistema estiver ocioso;

3.2.4.10.3. Permitir ao usuário retomar varreduras pausadas;

3.2.4.11. Deve permitir ao administrador inserir uma conta de domínio para realizar a análise de dispositivos de rede;

3.3. Características Módulo Antimalware (Clientes Linux)

3.3.1. Características da prevenção de ameaças

3.3.1.1. Deve permitir a atualização automática das vacinas de detecção;

3.3.1.2. Deve detectar ameaças usando métodos de acesso e de varredura sob demanda;

3.3.1.3. Deve permitir a execução de varreduras por meio da console centralizada por meio de tarefas;

3.3.1.4. Ao detectar uma ameaça, deverá responder com, no mínimo, as seguintes ações:

3.3.1.4.1. Limpar o arquivo

3.3.1.4.2. Deletar o arquivo

3.3.1.4.3. Negar acesso ao arquivo;

3.3.1.5. Deve possibilitar ao administrador, criar exceções de análise, ou seja, não permitir que a ferramenta execute uma análise em determinadas pastas ou arquivos;

3.3.1.6. Deve permitir a opção de manter a configuração de exclusão realizada no agente, não sendo sobrescrita pela política principal;

3.3.1.7. Deve permitir a gestão do agente local por meio de linha de comando;

3.3.1.8. Ao configurar a análise ao acessar, deve permitir:

3.3.1.8.1. Quando analisar (exemplo: ao ler o arquivo)

3.3.1.8.2. O que analisar (exemplo: todos os arquivos);

3.3.1.8.3. Análise de arquivos comprimidos

3.3.1.8.4. Análise de volumes de rede

3.3.1.8.5. Análise de programas não desejados;

3.3.1.9. Ao configurar a análise sob demanda, deve permitir:

3.3.1.9.1. Análise de arquivos compressos

3.3.1.9.2. Análise de PUP;

3.3.1.9.3. Análise de macros desconhecidos

3.3.1.9.4. Análise de programas desconhecidos

3.3.1.9.5. Caminhos da análise (path);

3.3.1.9.6. Análise de pastas e subpastas

3.3.1.9.7. Análise de macros;

3.3.1.9.8. Exclusão de paths, pastas e tipos de arquivos

3.3.1.9.9. Uso de cache

3.3.1.9.10. Ação Primária e Secundária

3.3.1.10. Deve possuir quarentena local para armazenar ameaças desconhecidas;

3.3.1.11. Deve possuir ação para mover artefatos maliciosos para a área de quarentena;

3.3.1.12. Deve usar heurística para detectar arquivos potencialmente maliciosos;

3.3.1.13. Caso aconteça um timeout durante uma análise, deve permitir ao administrador a configuração de permitir ou negar o acesso ao arquivo;

3.4. Características do Módulo de Firewall de Host (Clientes Windows)

3.4.1. Deve permitir a ativação/desativação do módulo de Firewall através da console;

3.4.2. Deve ser capaz de prevenir intrusões e proteger os endpoints garantindo cobertura para ataques dia zero;

3.4.3. Deve possuir um firewall de estação stateful bloqueando tráfego de entrada e controlando o tráfego de saída;

3.4.4. Deve possuir assinaturas de proteção para:

3.4.4.1. Arquivos

3.4.4.2. Chave de Registro

3.4.4.3. Processos

3.4.4.4. Serviços;

3.4.5. Deve permitir o tráfego de saída somente após os serviços de Firewall estiverem iniciados;

3.4.6. Deve ser possível bloquear tráfego bridge;

3.4.7. O módulo deve permitir a criação de regras de maneira adaptativa, ou seja, em uma estação modelo definida pelo administrador deve ser capaz de criar as regras de maneira automática;

3.4.8. Deve ser possível bloquear o tráfego de todos os processos identificados como não confiáveis;

3.4.9. Deve permitir a criação de uma lista de processos identificados como confiáveis por meio das seguintes informações:

3.4.9.1. Nome

3.4.9.2. Nome do arquivo ou Caminho;

3.4.9.3. Hash MD5

3.4.9.4. Assinador Digital

3.4.10. Deve permitir integração com o Centro de Inteligência do próprio fabricante para bloqueio de ameaças advindas por meio de conexões maliciosas;

3.4.10.1. As conexões identificadas pelo Centro de Inteligência podem ser configuradas por meio de reputação mínima a ser bloqueada, por exemplo Risco Alto ou Risco Médio.

3.4.11. Deve ser possível registrar os eventos de conexões bloqueadas e permitidas pelo módulo;

3.4.12. Deve permitir inspeção do protocolo FTP;

3.4.13. Deve ser possível permitir tráfego de protocolos não suportados;

3.4.14. O módulo de Firewall deve vir com regras pré-indicadas pelo próprio fabricante.

3.4.15. O módulo de Firewall deve permitir a criação de regras customizadas, com no mínimo os seguintes parâmetros:

3.4.15.1. Ação

3.4.15.1.1. Bloquear

3.4.15.1.2. Permitir

3.4.15.2. Direção

3.4.15.2.1. Ambas

3.4.15.2.2. Entrada

3.4.15.2.3. Saída

3.4.15.3. Protocolo

3.4.15.3.1. Qualquer protocolo

3.4.15.3.2. Protocolo IP

3.4.15.3.2.1. Ipv4

3.4.15.3.2.2. Ipv6

3.4.15.3.2.3. Protocolo Não-IP

3.4.15.4. Tipo de Conexão

3.4.15.4.1. Rede Sem Fio

3.4.15.4.2. Rede Cabeada

3.4.15.4.3. Rede Virtual

3.4.15.5. Especificação da Rede

3.4.15.5.1. Endereço IP

3.4.15.5.2. Subnet

3.4.15.5.3. Range

3.4.15.5.4. FQDN

3.4.15.6. Protocolo de Transporte

3.4.15.6.1. Todos

3.4.15.6.2. ICMP

3.4.15.6.3. ICMPv6

3.4.15.6.4. TCP

3.4.15.6.5. UDP

3.4.15.6.6. STP

3.4.15.6.7. GRE

3.4.15.6.8. IGMP

3.4.15.6.9. IPSEC AH

3.4.15.6.10. IPSEC ESP

3.4.15.6.11. Ipv6 in Ipv4

3.4.15.6.12. ISIS over Ipv4

3.4.15.6.13. L2TP

3.4.15.7. Agendamento

3.4.15.7.1. Dias da Semana

3.4.15.7.2. Hora Início

3.4.15.7.3. Hora Fim

3.4.15.8. Aplicações

3.5. Características do Módulo de Firewall de Host (Clientes Linux)

3.5.1. Deve permitir a ativação/desativação do módulo de Firewall através da console;

3.5.2. Deve possuir um firewall de estação stateful bloqueando tráfego de entrada e controlando o tráfego de saída;

3.5.3. O módulo deve permitir a criação de regras de maneira adaptativa, ou seja, em uma estação modelo definida pelo administrador deve ser capaz de criar as regras de maneira automática;

3.5.4. Deve permitir inspeção do protocolo FTP;

3.5.5. O módulo de Firewall deve vir com regras pré-indicadas pelo próprio fabricante.

3.5.6. O módulo de Firewall deve permitir a criação de regras customizadas, com no mínimo os seguintes parâmetros:

3.5.6.1. Ação

3.5.6.1.1. Bloquear

3.5.6.1.2. Permitir

3.5.6.2. Direção

3.5.6.2.1. Ambas

3.5.6.2.2. Entrada

3.5.6.2.3. Saída

3.5.6.3. Protocolo

3.5.6.3.1. Qualquer protocolo

3.5.6.3.2. Protocolo IP

3.5.6.3.2.1. Ipv4

3.5.6.4. Tipo de Conexão

3.5.6.4.1. Rede Sem Fio

3.5.6.4.2. Rede Cabeada

3.5.6.4.3. Rede Virtual

3.5.6.5. Especificação da Rede

3.5.6.5.1. Endereço IP

3.5.6.5.2. Subnet

3.5.6.5.3. Range

3.5.6.5.4. FQDN

3.5.6.6. Protocolo de Transporte

3.5.6.6.1. Todos

3.5.6.6.2. ICMP

3.5.6.6.3. TCP

3.5.6.6.4. UDP

3.5.6.7. Agendamento

3.5.6.7.1. Dias da Semana

3.5.6.7.2. Hora Início

3.5.6.7.3. Hora Fim

3.6. Características do Módulo de Filtragem Web

3.6.1. Deve permitir o bloqueio de browsers não suportados, dentre eles:

3.6.1.1. Opera

3.6.1.2. Safari for Windows;

3.6.1.3. Netscape

3.6.1.4. Maxthon

3.6.1.5. Flock;

3.6.1.6. Avant Browser;

3.6.1.7. Deepnet Explorer

3.6.1.8. PhaseOut

3.6.2. Deve permitir o controle de browsers suportados, dentre eles:

3.6.2.1. Chrome

3.6.2.2. Firefox

3.6.2.3. Internet Explorer

3.6.3. Deve ser capaz de utilizar lista de categorias para bloqueio de sites relacionados ao conteúdo não autorizado.

3.6.4. Deve possuir, no mínimo, as seguintes categorias:

3.6.4.1. Browser Exploits;

3.6.4.2. Download Maliciosos;

3.6.4.3. Sites Maliciosos;

3.6.4.4. Phishing;

3.6.4.5. Pornografia;

3.6.4.6. Hacking/Computer Crime;

3.6.4.7. Spyware/Adware/Keyloggers;

3.6.4.8. Anonymizer;

3.6.4.9. Anonymizer Utilities;

3.6.4.10. Dating

3.6.4.11. Dating/Social Networking

3.6.4.12. Discrimination;

3.6.4.13. Drugs;

3.6.4.14. Gambling

3.6.4.15. Games

3.6.4.16. Government/Military

3.6.4.17. Media Downloads

3.6.4.18. Media Sharing

3.6.4.19. Nudity

3.6.4.20. P2P/File Sharing

3.6.4.21. Potentially Unwanted Programs

3.6.4.22. Social Networking

3.6.4.23. Streaming Media

3.6.4.24. Text Translators

3.6.4.25. Web Mail

3.6.5. Deve ser possível bloquear um site conforme a sua classificação:

3.6.5.1. Vermelho: Alto Risco

3.6.5.2. Amarelo: Médio Risco

3.6.5.3. Cinza: Não categorizado

3.6.6. Deve ser possível bloquear um site quando este nunca foi visto pelo Centro de Inteligência do Fabricante;

3.6.7. Deve ser possível bloquear páginas de phishing, mesmo que o conteúdo tenha acesso permitido;

3.6.8. Deve permitir a varredura de arquivos baixados da internet;

3.6.9. Deve ser possível excluir endereços IP da análise;

3.6.10. Deve permitir a busca segura para buscadores, dentre eles:

3.6.10.1. Google;

3.6.10.2. Yahoo

3.6.10.3. Bing;

3.6.10.4. Ask;

3.6.11. Deve bloquear links que direcionem para sites com alto risco.

3.6.12. Deve permitir a customização das mensagens apresentadas para o usuário;

3.7. Características do Módulo de Ameaças Avançadas

3.7.1. A solução deve permitir o confinamento dinâmico de aplicativos e arquivos executáveis com indícios maliciosos (Ransomware)

3.7.2. A solução deve ser capaz de avaliar aplicações desconhecidas e potencialmente maliciosas executando-as em ambiente controlado;

3.7.3. Deve permitir a indicação de aplicações confiáveis para que não caiam no filtro de confinamento dinâmico;

3.7.4. Não deve requerer conexão com centro de inteligência do fabricante para que a proteção seja ativada ou executada

3.7.5. Solução deve manter um cache de reputação local com informações de aplicações - conhecidas, desconhecidas e maliciosas.

3.7.6. Dentre os comportamentos maliciosos, deve ser capaz de:

3.7.6.1. Bloquear acesso local a partir de cookies;

3.7.6.2. Criação de arquivos a partir de arquivos com extensão .bat, .exe, html, hpg, bmp, job e .vbs;

3.7.6.3. Criação de arquivos em qualquer local de rede;

3.7.6.4. Criação de novos CLSIDs, APPIDs e TYPELIBs;

3.7.6.5. Criação de threads em outro processo;

3.7.6.6. Bloquear a desativação de executáveis críticos do sistema operacional;

3.7.6.7. Leitura/Exclusão/Gravação de arquivos visados por Ransomwares;

3.7.6.8. Gravação e Leitura na memória de outro processo;

3.7.6.9. Bloqueio de Modificação da política de firewall do Windows;

3.7.6.10. Bloqueio de Modificação da pasta de tarefas do Windows;

3.7.6.11. Bloqueio de Modificação de arquivos críticos do Windows e Locais do Registro;

3.7.6.12. Bloqueio de Modíficação de arquivos executáveis portáteis;

3.7.6.13. Bloqueio de Modificação de bit de atributo oculto;

3.7.6.14. Bloqueio de Modificação de bit de atributo somente leitura;

3.7.6.15. Bloqueio de Modificação de entradas de registro de DLL AppInit;

3.7.6.16. Bloqueio de Modificação de locais do registro de inicialização;

3.7.6.17. Bloqueio de Modificação de pastas de dados de usuários;

3.7.6.18. Bloqueio de Modificação do local do Registro de Serviços;

3.7.6.19. Bloqueio de Suspensão de um processo;

3.7.6.20. Bloqueio de Término de outro processo.

3.7.7. Dos comportamentos observados, deve ser possível bloquear ou apenas informar caso o mesmo ocorra.

3.7.8. Deve ser capaz de informar ao usuário as ameaças encontradas através de mensagem customizada.

3.7.9. O modo de ativação do confinamento dinâmico para quaisquer arquivos desconhecidos acessados pelo sistema operacional e nunca antes visto pela solução;

3.7.10. Deve ser possível atribuir a regra conforme política equilibrada, visando maior segurança ou produtividade do usuário

3.7.11. A proteção deve estar contida no mesmo agente de proteção, não requerendo outro software ou aplicação adicional na estação de trabalho para a execução e ativação da proteção

3.7.12. Deve possuir capacidade de inspecionar arquivos suspeitos e detectar comportamentos maliciosos utilizando técnicas de "machine-learning";

3.7.13. A solução deve ter a capacidade de remediação de ações efetuadas por artefatos maliciosos, como criação de arquivos e alteração de chaves de registro.

3.7.13.1. A remediação deve ser efetuada de maneira automática, a partir do momento em que o artefato é identificado como malicioso.

3.8. Características do módulo de reputação de arquivos e compartilhamento de informações de segurança:

3.8.1. A solução deve possuir capacidade de criar uma reputação local, além de utilizar uma já existente em nuvem através da catalogação de todos os executáveis existentes no ambiente;

3.8.2. O servidor de reputação deverá habilitar a troca de informação de ameaças entre os endpoints e servidores protegidos.

3.8.3. Este módulo deverá habilitar um protocolo de troca de informações de ameaças que permita o intercâmbio de informações entre soluções do mesmo fabricante e de fabricantes terceiros;

3.8.4. A troca de informação de ameaças deve se dar por meio de protocolo performático;

3.8.5. De forma a permitir menor impacto na rede, para tal método de consulta dos clientes a base de dados poderá ser síncrona ou assíncrona;

3.8.6. A solução deverá apresentar a reputação dos arquivos definida para cada um dos ativos conectados, dentre eles:

3.8.6.1. Reputação local

3.8.6.2. Reputação do centro de inteligência

3.8.7. Ao catalogar um arquivo, a solução deve apresentar, no mínimo as seguintes informações:

3.8.7.1. Nome do arquivo

3.8.7.2. Caminho do arquivo

3.8.7.3. Hash sha-1

3.8.7.4. Hash 256

3.8.7.5. Primeira visualização do arquivo na rede

3.8.7.6. Última visualização do arquivo na rede

3.8.7.7. Tamanho do arquivo

3.8.7.8. Data de compilação

3.8.7.9. Se o mesmo consta no adicionar/remover programas

3.8.7.10. Se está registrado como serviço

3.8.7.11. Se está registrado para ser executado automaticamente

3.8.7.12. Tipo de compactador

3.8.7.13. Se é arquivo do sistema

3.8.7.14. Se foi executado a partir do cmd.exe

3.8.7.15. Se tem entrada no menu iniciar

3.8.7.16. Se foi executado a partir de uma mídia removível

3.8.7.17. Se foi executado a partir da raiz da unidade do sistema

3.8.8. Caso o arquivo tenha como origem a Internet, a solução deverá ser capaz de informar a partir de qual URL o arquivo foi obtido e a reputação desta última;

3.8.9. Deve ser possível realizar uma pesquisa do arquivo em base de conhecimento de terceiros (exemplo: Virus Total);

3.8.10. Após análise pela solução o administrador deve ter a possibilidade de:

3.8.10.1. Rastrear em quais estações o arquivo foi executado;

3.8.10.2. Identificar o arquivo como confiável;

3.8.10.3. Identificar o arquivo como desconhecido;

3.8.10.4. Identificar o arquivo como malicioso

3.8.10.5. Analisar o certificado associado ao arquivo;

3.8.10.6. Identificar o certificado associado como confiável ou malicioso;

3.8.11. Para minimizar o impacto a solução deve ter a capacidade de ser ativada no modo de observação nos endpoints e servidores protegidos;

3.8.12. Deve ser possível bloquear a execução de arquivos nunca antes vistos ou suspeitos no ambiente e informar o usuário por meio de mensagem.

3.8.13. Deve ser capaz de identificar manualmente um arquivo como malicioso impedindo sua execução no ambiente;

3.8.14. Deve ser gerenciado pela mesma console de gerenciamento da solução de proteção de endpoints e servidores.

3.9. Características do Módulo de Controle de Dispositivos

3.9.1. Deve controlar o uso de dispositivos por parte dos usuários, como por exemplo Mídias Removíveis, Unidades USB, Ipods, Dispositivos Bluetooth, DVDs, e CDS regraváveis;

3.9.2. Deve permitir a configuração dos dispositivos nos modos:

3.9.2.1. Bloqueio, ou;

3.9.2.2. Somente Leitura;

3.9.3. Deve classificar os dispositivos removíveis em 3 categorias:

3.9.3.1. Gerenciado;

3.9.3.2. Não Gerenciável (Exemplo: Bateria de Notebooks);

3.9.3.3. Não Gerenciado;

3.9.4. Deve ser capaz de identificar o dispositivo (plug and play) através das seguintes informações:

3.9.4.1. Tipo de BUS;

3.9.4.2. Classe do Dispositivo (Device Class)

3.9.4.3. ID do fabricante (Vendor ID)

3.9.4.4. ID do produto (Product ID)

3.9.5. Deve ser capaz de identificar Dispositivos Removíveis através das seguintes informações:

3.9.5.1. Tipo de BUS

3.9.5.2. Se o sistema de arquivo é passível de escrita;

3.9.5.3. Se o sistema de arquivo é somente leitura;

3.9.5.4. Tipo de Sistema de Arquivo

3.9.5.5. Nome do Sistema de Arquivo;

3.9.5.6. Número de Série do Sistema de Arquivo;

3.9.6. Deve ser possível habilitar ou desabilitar uma determinada regra de proteção uma vez que esteja dentro da rede (Exemplo: Quando conectado à rede do órgão libera o uso de pen-drive);

3.10. Características do Módulo de Criptografia

3.10.1. Deve ser capaz de realizar a proteção a mídia física nos seguintes sistemas operacionais:

3.10.1.1. Windows 8.1 (x86/x64);

3.10.1.2. Windows 10 (x64);

3.10.2. Deve possuir módulo de criptografia para as estações de trabalho (desktops e notebooks), com as seguintes funcionalidades de criptografia para:

3.10.2.1. Disco completo (fde – full disk encryption);

3.10.2.2. Pastas e arquivos;

3.10.2.3. Mídias removíveis;

3.10.2.4. Automática de disco;

3.10.3. Deve possuir autenticação durante a inicialização (boot) da estação de trabalho, antes do carregamento do sistema operacional, para a funcionalidade de criptografia do disco completo;

3.10.4. A autenticação durante a inicialização (boot) deve ser a partir das credenciais sincronizadas com o Active Directory;

3.10.5. Deve possuir suporte ao algoritmo de criptografia aes-256;

3.10.6. Deve possuir a capacidade de exceções para criptografia automática;

3.10.7. Deve possuir criptografia no canal de comunicação entre as estações de trabalho e o servidor de políticas;

3.10.8. Deve possuir certificação FIPS 140-2;

3.10.9. Deve possuir funcionalidade de criptografia por software ou hardware;

3.10.10. Deve ser compatível com os padrões SED ('self-encrypting drive), opal e opal2

3.10.11. Deve permitir atualizações do sistema operacional mesmo quando o disco está criptografado;

3.10.12. Deve possuir políticas por usuários, grupos e dispositivos;

3.10.13. Deve possuir os métodos de autenticação seguintes para desbloquear um disco:

3.10.13.1. Autenticação com ad;

3.10.13.2. Single sign-on com ad;

3.10.13.3. Senha pré-definida;

3.10.13.4. Número pin;

3.10.13.5. Smart card;

3.10.14. Deve possuir autoajuda para usuários que esquecerem a senha com a combinação de perguntas e respostas;

3.10.15. Deve possuir mecanismos de criptografia transparentes para o usuário;

3.10.16. Deve possuir mecanismo para desativar temporariamente a autenticação de pré-inicialização (boot);

3.10.17. O ambiente de autenticação deve disponibilizar um teclado virtual na tela do dispositivo, independente do teclado físico;

3.10.18. O ambiente de autenticação pré-inicialização deve prover um mecanismo de assistência remota que permita a autenticação da estação de trabalho no evento que o usuário não se lembre de sua senha de autenticação;

3.10.19. O ambiente de autenticação pré-inicialização deve prover um mecanismo que permita a substituição da senha e outros códigos de autenticação através da resposta correta a perguntas definidas previamente pelo administrador;

3.10.20. Deve possuir ferramenta integrada ao processo de pré-boot ou não para realizar manutenções em caso de problema com o ambiente de pré-boot ou autenticação.

3.10.21. O acesso à ferramenta de manutenção deve ser controlado através de política gerenciada pelo componente de gerenciamento da solução;

3.10.22. Deve permitir a gerência das seguintes soluções terceiras de criptografia:

3.10.22.1. Microsoft Bitlocker;

3.10.22.2. Apple FileVault;

3.10.23. As capacidades de gerência das soluções terceiras de criptografia devem incluir:

3.10.23.1. Habilitar a criptografia

3.10.23.2. Exibir o estado da criptografia (ativado, desativado)

3.10.23.3. Habilitar o aviso legal

3.10.23.4. Editar o intervalo de sincronia

3.10.24. Deve permitir a visualização das estações de trabalho que tenham aplicação de política pendente a partir da console de administração centralizada;

3.10.25. Deve permitir a visualização do autor de determinada política a partir da console de administração centralizada;

3.10.26. Deve permitir a visualização de estações de trabalho que não possuam nenhuma política aplicada a partir da console de administração centralizada;

3.10.27. Deve permitir a adição de informações de contato a serem exibidas ao usuário final com texto customizável;

3.10.28. Deve permitir, em nível de política, a indicação de pastas a serem criptografadas;

3.10.29. Deve possibilitar que cada política tenha uma chave de criptografia única;

3.10.30. Deve permitir, em nível de política, a escolha da chave de criptografia a ser utilizada, entre as seguintes opções:

3.10.30.1. Chave do usuário: somente o usuário tem acesso aos arquivos;

3.10.30.2. Chave da empresa: qualquer usuário da empresa tem acesso aos arquivos;

3.10.31. Deve permitir a escolha dos diretórios a serem criptografados em dispositivos de armazenamento USB;

3.10.32. Deve possibilitar a desativação de dispositivos de gravação de mídias óticas;

3.10.33. Deve possibilitar a desativação de dispositivos de armazenamento USB;

3.10.34. Deve possibilitar o bloqueio da desinstalação do agente de criptografia por usuários que não sejam administradores da estação de trabalho;

3.10.35. Deve possibilitar o atraso, em intervalo personalizado de tempo, para uma nova tentativa de autenticação de usuários na ocorrência de um número personalizável de tentativas inválidas de autenticação;

3.10.36. Deve possibilitar a instauração de política de gerenciamento de complexidade e intervalo de troca de senha com os seguintes critérios:

3.10.36.1. Definição do intervalo de dias em que o usuário será forçado a mudar sua senha;

3.10.36.2. Definição de número de senhas imediatamente anteriores que não poderão ser reutilizadas como nova senha;

3.10.36.3. Definição do comprimento de caracteres mínimo a ser utilizado na nova senha;

3.10.36.4. Definição do número de caracteres especiais, caracteres numéricos, caracteres em caixa alta e caracteres em caixa baixa que deverão ser utilizados para a nova senha;

3.10.37. Deve permitir a criação de múltiplos painéis (dashboards) personalizáveis, compostos por blocos de informações (widgets), visualizados através de gráficos ou tabelas;

3.10.38. Os blocos de informações pertencentes aos painéis personalizáveis devem permitir filtros personalizados para facilitar na visualização e gerenciamentos;

3.10.39. A seleção de uma informação específica dentro de um bloco de informações, através de um clique, deve redirecionar ao log detalhado que gerou aquela informação;

3.11. Características do Módulo de Controle de Aplicações

3.11.1. O módulo de controle de aplicações deve prover a capacidade de visibilidade sobre as aplicações executadas e aplicar o controle de execução imposto pela política;

3.11.2. Deve ser capaz de realizar um inventário nas estações de trabalho protegidas informando todos os executáveis e arquivos de script presentes.

3.11.3. Como resultado do inventário, a solução deve armazenar o nome completo do arquivo, tamanho, checksum, tipo de arquivo, nome da aplicação e versão;

3.11.4. Ao detectar um executável, a solução deverá consultar a Solução de reputação de arquivos e compartilhamento de informações de segurança e esta deverá informar um nível de confidência (Bom, Mau ou Não Classificado);

3.11.5. Caso não seja possível efetuar comunicação com a Solução de reputação de arquivos e compartilhamento de informações de segurança o módulo deve realizar consulta de reputação para o Centro de Inteligência do fabricante;

3.11.6. Capacidade de trabalhar no modo adaptativo, ou seja, adaptando-se à novas aplicações instaladas na máquina;

3.11.7. A solução deverá permitir a realização de varreduras por demandas em máquinas para executar a blindagem de aplicativos;

3.11.8. Para o controle de aplicativos, deve possuir, no mínimo, os seguintes modos de operação:

3.11.8.1. Desabilitado: proteção desativada

3.11.8.2. Monitoramento: Monitora toda a atividade da Estação de Trabalho;

3.11.8.3. Atualização: a cada execução de aplicativo este é inserido em uma regra ou pacote de autorizações pré-estabelecido;

3.11.9. Deve identificar as aplicações de maneira única através do uso de hash (MD5 ou SHA- 1).

3.11.10. A solução deve suportar as seguintes modalidades de proteção:

3.11.10.1. Application Whitelisting: criação de uma lista de aplicações autorizadas que podem ser executadas no equipamento, onde todas as demais aplicações são impadidas de serem executadas.

3.11.10.2. Memory Protection: monitoração e proteção de aplicativos e componentes críticos do sistema operacional de serem adulterados em tempo de execução, isto é, durante operação e execução em memória.

3.11.11. Solução suporta criação, configuração e manutenção de Whitelist dinamicamente através de definição de regras de confiança.

3.11.12. Em caso de um bloqueio indevido, o usuário poderá submeter o arquivo para revisão do administrador e solicitar a liberação do aplicativo ou arquivo.

3.11.13. Suporta os mecanismos:

3.11.13.1. Application Code Protection: permite que somente os programas em Whitelist (executáveis, binários, DLLs, Scripts, extensões customizadas, entre outros) possam ser executados.

3.11.13.2. Memory Protection: permite proteção para ataques e exploração de vulnerabilidades para os programas em Whitelist.

3.11.14. Suporta criação, configuração e manutenção de políticas, permitindo ou bloqueando a adesão de Whitelist, através de:

3.11.14.1. Binário: binário específico identificado através de seu nome ou de algorítmo de verificação SHA-1.

3.11.14.2. Trusted Publisher: fornecedor específico, assinado digitalmente por um certificado de segurança emitido, para este fornecedor, por uma Autoridade Certificadora (CA - Certificate Authority).

3.11.14.3. Trusted Installer: software instalado por um programa instalador específico, identificações por seu algorítmo de verificação, independentemente de sua origem.

3.11.14.4. Trusted Directories: pasta compartilhada na rede, onde os programas instaladores para aplicações autorizadas e licenciadas são mantidos.

3.11.14.5. Trusted Program / Authorized Updater: programas identificados pelo nome, para adicionar e/ou atualizar aplicações.

3.11.14.6. Trusted Users / Authorized Users: somente usuários selecionados, substituindo a proteção de adulteração, para adicionar e/ou atualizar aplicações.

3.11.14.7. Trusted Time Window / Update Mode: janela de tempo para manutenção de aplicações.

3.11.15. Deve ser capaz de proteger em modo standalone - online ou offline;

3.11.16. Além de possuir um conjunto de regras, deve permitir por parte do administrador que este customize-as de forma a adaptar a necessidade do órgão;

3.11.17. Deve suportar o uso de variáveis de ambiente para a criação de regras de monitoramento (Exemplo: %HOMEPATH%, %HOMEDRIVE%, %USERPROFILE%, %APPDATA%)

3.11.18. Deve suportar variáveis de ambiente em sistemas 64-bits (Exemplo:%PROGRAMFILES (x86)%)

3.11.19. Deve prover, no mínimo, as seguintes técnicas para proteção de memória de forma a prevenir ataques dia zero:

3.11.19.1. Critical Address Space Protection;

3.11.19.2. NX - No eXecute (mp-nx)

3.11.19.3. Virtual Address Space Randomization

3.11.19.4. Mp-vasr-randomization

3.11.19.5. Mp-vasr-relocation

3.11.19.6. Mp-vasr-reloc

3.11.19.7. Forced DLL Relocation

3.11.20. Deve possibilitar o controle e bloqueio da instalação de Active-X nas estações de trabalho.

3.11.21. Permitir o bloqueio de aplicações e os processos que a aplicação interage

3.11.22. Permitir monitoração de aplicações onde se pode determinar quais processos poderão ser executados ou não.

3.12. Características do Módulo de Gerenciamento

3.12.1. Deve ser disponibilizado em solução local (on-premise);

3.12.2. Solução de gerenciamento on-premise:

3.12.2.1. Deve suportar a instalação nos seguintes sistemas operacionais:

3.12.2.1.1. Windows Server 2019;

3.12.2.1.2. Windows Server 2016;

3.12.2.1.3. Windows Server 2012 Release 2;

3.12.2.1.4. Windows Server 2012.

3.12.2.2. A arquitetura dos Sistemas Operacionais deve ser 64-bits;

3.12.2.3. Deve suportar a instalação em Cluster Microsoft;

3.12.2.4. Deve suportar Ipv4 e Ipv6;

3.12.2.5. Deve suportar a virtualização do sistema operacional com base nos seguintes hypervisors:

3.12.2.5.1. Vmware ESX

3.12.2.5.2. Citrix Xen Server

3.12.2.5.3. Microsoft Hyper-V

3.12.2.6. Deve possuir suporte a base de dados:

3.12.2.6.1. SQL Server 2014 ou superior

3.12.2.7. Não serão aceitas soluções que usam SQL Express ou Base de dados embutidas;

3.12.2.8. Deve ser possível segregar a instalação da solução em:

3.12.2.8.1. Servidor Console Central

3.12.2.8.2. Servidor Base de Dados

3.12.2.8.3. Servidor de Interação com os Agentes

3.12.2.8.4. Agentes Distribuidores de Vacina

3.12.2.9. Deve suportar o uso do SQL Server em ambientes SAN;

3.12.2.10. Permitir a instalação dos Módulos da Solução a partir de um único servidor;

3.12.3. A console de gerência deve ser acessada via WEB;

3.12.4. Deve possuir compatibilidade com os seguintes browsers:

3.12.4.1. Google Chrome;

3.12.4.2. Firefox;

3.12.4.3. Internet Explorer 7 ou superior;

3.12.4.4. Safari 6.0 ou superior;

3.12.5. Permitir a alteração das configurações dos Módulos da Solução nos clientes de maneira remota

3.12.6. Permitir a atualização incremental da lista de definições de vírus nos clientes, a partir de um único ponto da rede local.

3.12.7. Visualização das características básicas de hardware das máquinas

3.12.8. Integração e Importação automática da estrutura de domínios do Active Directory já existentes na rede local

3.12.9. Permitir a criação de tarefas de atualização, verificação de vírus e upgrades em períodos de tempo pré-determinados, na inicialização do Sistema Operacional ou no Logon na rede.

3.12.10. Permitir o armazenamento das informações coletadas nos clientes em um banco de dados centralizado.

3.12.11. Permitir diferentes níveis de administração do servidor, de maneira independente do login da rede.

3.12.12. Suporte a múltiplos usuários, com diferentes níveis de acesso e permissões aos produtos gerenciados.

3.12.13. Criação de grupos de máquinas baseadas em regras definidas em função do número IP do cliente.

3.12.14. Permitir a criação de grupos virtuais através de marcadores;

3.12.15. Permitir aplicar as marcações nos sistemas por vários critérios incluindo: produtos instalados, versão de sistema operacional, quantidade de memória, dentre outros;

3.12.16. Forçar a configuração determinada no servidor para os clientes;

3.12.17. Caso o cliente altere a configuração, ela deverá retornar ao padrão estabelecido no servidor, quando ela for verificada pelo agente.

3.12.18. A comunicação entre as máquinas clientes e o servidor de gerenciamento deve ser segura usando protocolo de autenticação HTTPS.

3.12.19. Forçar a instalação dos Módulos da Solução nos clientes;

3.12.20. Caso o cliente desinstale os Módulos da Solução, os mesmos deverão ser reinstalados, quando o agente verificar o ocorrido.

3.12.21. Deve ser possível realizar a customização dos relatórios gráficos gerados;

3.12.22. Exportação dos relatórios para os seguintes formatos: HTML, CSV, PDF, XML

3.12.23. Geração de relatórios que contenham as seguintes informações:

3.12.23.1. Máquinas com a lista de definições de vírus desatualizada;

3.12.23.2. Qual a versão do software (inclusive versão gerenciada pela nuvem) instalado em cada máquina;

3.12.23.3. Os vírus que mais foram detectados;

3.12.23.4. As máquinas que mais sofreram infecções em um determinado período;

3.12.23.5. Os usuários que mais sofreram infecções em um determinado período;

3.12.24. A solução de gestão deve possuir dashboards no gerenciamento da solução;

3.12.25. Estes dashboards devem conter no mínimo todos os seguintes relatórios de fácil visualização:

3.12.25.1. Relatório dos últimos 30 dias da detecção de códigos maliciosos;

3.12.25.2. Top 10 Computadores com Infecções;

3.12.25.3. Top 10 Computadores com Sites bloqueados pela política;

3.12.26. Gerenciar a atualização do antivírus em computadores portáteis (notebooks), automaticamente, mediante conexão em rede local ou remota (VPN);

3.12.27. Suportar o uso de múltiplos repositórios para atualização de produtos e arquivo de vacina com replicação seletiva;

3.12.28. Ter a capacidade de gerar registros/logs para auditoria;

3.12.29. A solução de gerenciamento deve ter a capacidade de atribuir etiquetas as máquinas, facilitando assim a distribuição automática dentro dos grupos hierárquicos na estrutura de gerenciamento.

3.12.30. A solução de gerenciamento deve permitir acesso a sua console via web.

4. DAS GARANTIAS DE: LICENCIAMENTO, ATUALIZAÇÃO, MANUTENÇÃO E VERSIONAMENTOS DA FERRAMENTA DE ANTIVÍRUS (Item 01 e 02)

4.1. A duração das garantias para os itens 01 e 02 será de 30 meses;

4.2. O serviço de atualização de licenciamento consiste na atualização da versão para versões mais atuais, bem como as atualizações de novas versões que forem lançadas durante a vigência da garantia.

4.3. No caso de a solução contratada passar a constar em listas de End-of-Support, End-of-Sales ou End-of-Life do fabricante, durante a garantia, a CONTRATADA deverá substituir a solução por uma outra com características técnicas iguais ou superiores.

4.4. A manutenção evolutiva, corretiva e reinstalação, quando for o caso, deverá ser realizada durante todo o período da garantia do produto, pela CONTRATADA, permitindo cobertura completa e operacional de uso do equipamento/software em todas as funcionalidades atualmente contratadas.

4.5. Deve fazer parte deste item Garantia todos os custos operacionais para reprogramações dos sistemas, correções de falhas de software, atualização de versões dos módulos de software, incluindo sistema operacional do equipamento, quando for o caso, firmwares, disponibilizados pelo fabricante da solução durante o prazo da garantia, sem custo adicional para a CONTRATANTE das novas versões de atualização que por ventura vierem a ser publicadas.

4.6. Deve contemplar a substituição do todo ou em parte dos equipamentos cobertos quando da necessidade de manutenções corretivas e, ou, manutenções evolutivas do hardware.

4.7. Durante a vigência da garantia, todas as funcionalidades da solução, deverão ser atualizadas a medida do lançamento de novas versões sem custos para a CONTRATADA.

4.8. Todas as instalações de novas versões, atualizações, correções sejam do fabricante, sejam de *features* instaladas devem ser executadas pela CONTRATADA.

5. SUPORTE TÉCNICO ESPECIALIZADO (Na Garantia)

5.1. O serviço de manutenção e suporte consiste na desinstalação, reconfiguração ou reinstalação decorrentes de falhas no software, adequação dos softwares às melhores práticas, atualização da versão de software, correção de defeitos, ajustes e reparos necessários, de acordo com os manuais e as normas técnicas específicas para os recursos utilizados. Quanto às atualizações pertinentes aos softwares, entende-se como “atualização” o provimento de toda e qualquer evolução de software, incluindo correções, “patches”, “fixes”, “updates”, “service-packs”, novas “releases”, “versions”, “builds”, “upgrades”, durante a vigência da garantia que será de 30 meses;

5.2. O suporte técnico deve compreender procedimentos destinados a manter os equipamentos em perfeito estado de uso, nos casos de inoperância total ou parcial, defeito ou mau funcionamento, incluindo substituições ou reposições, inclusive de peças, ajustes e reparos, de acordo com os manuais e normas técnicas adotadas e recomendadas pelo fabricante;

5.3. Todo o hardware e software que for empregado para garantir o perfeito funcionamento das funcionalidades dos produtos, em qualidade, quantidade e desempenho requeridos, deverão ser assegurados durante todo o período de garantia;

5.4. Toda nova implementação/criação de serviços, configurações e outros, que surjam durante a vigência da garantia, e que a equipe interna da CONTRATANTE não esteja apta para a sua execução, será aberto um chamado junto a CONTRATADA para prover o suporte técnico especializado e acompanhamento do mesmo. Não incorrendo em custas ou pagamentos extras ao valor contratado;

5.5. Toda e qualquer manutenção de hardware, quando for o caso, no equipamento acima descrito, suas despesas, correrá por parte da CONTRATADA sendo as mais variadas. Em caso de troca ou substituição do equipamento deverá ser por uma igual ou superior ao que está instalado nas dependências da CONTRATADA.

5.6. As atividades de manutenção e suporte técnico corretivo serão realizadas sempre que solicitadas pela Codevasf por meio da abertura de chamado diretamente à CONTRATADA via telefone, e-mail e/ou site.

5.7. Um chamado somente poderá ser fechado após o aceite do fiscal técnico responsável pelo contrato na Codevasf e o término de atendimento se dará com a disponibilidade do recurso para uso em perfeitas condições de funcionamento no local onde ele está instalado.

5.8. Todas as solicitações feitas pela Codevasf deverão ser registradas pela CONTRATADA para acompanhamento e controle da execução dos serviços. Após a realização dos serviços, a CONTRATADA deverá apresentar um Relatório de Atividades, contendo no mínimo as informações descritas no item a seguir, e este relatório deverá ser homologado pelo Fiscal Técnico responsável pelo contrato na Codevasf.

5.9. O relatório de atividades deverá ser emitido pelo Gerente de Suporte encarregado pelo contrato na CONTRATADA e será preenchido pelo técnico da CONTRATADA encarregado de prestar os serviços, contendo no mínimo:

5.9.1. Identificação do Relatório de Atividades;
5.9.2. Data da emissão;
5.9.3. Data e hora de início e término do atendimento;
5.9.4. Número do contrato;
5.9.5. Identificação do requisitante do serviço;

5.9.6. Descrição da atividade realizada e detalhamento da solução aplicada;
5.9.7. Identificação do fiscal técnico da Codevasf que validou o serviço; e
5.9.8. Identificação do técnico da CONTRATADA responsável pela execução do serviço.

5.10. A CONTRATADA, a partir da data de formalização de recebimento da abertura do chamado, terá os prazos estipulados para atendimento segundo TABELA I para iniciar o atendimento remoto ou em casos de extrema urgência presenciais caso seja necessário.
5.11. Os chamados serão categorizados conforme a sua Severidade pela equipe da CONTRATANTE no momento de abertura do chamado conforme TABELA I;
5.12. Os SLAs da TABELA I serão considerados apenas para atendimento remoto, atendimento presenciais em casos excepcionais serão tratados e alinhados com a CONTRATADA;
5.13. A CONTRATADA deverá informar aos responsáveis da Codevasf qualquer situação que possa ensejar em uso inadequado dos recursos.

TABELA I

Severidade	Descrição	Atendimento Técnico (em até)	
1 – Crítica	Situação emergencial ou problema crítico que cause a indisponibilidade do ambiente ou da solução contratada.	2 horas	4 horas
2 – Alta	Impacto de alta significância relacionado à utilização e/ou aplicação da remediação orientada pela solução contratada.	4horas	8 horas
3 – Média	Impacto de baixa significância relacionado à utilização e/ou aplicação da remediação orientada pela solução contratada.	8 horas	12 horas
4 – Baixa	Questionamentos necessários para sanar dúvidas acerca da utilização da solução contratada.	24 horas	72 horas

6. REPASSE DE CONHECIMENTO DAS FUNCIONALIDADES DA FERRAMENTA (TREINAMENTO) – ITEM 03

6.1. O repasse de conhecimento diz respeito ao curso de operação, configuração e utilização de todas as funcionalidades do software, para o total de 4 pessoas, a serem indicados pela CONTRATANTE dos serviços. Toda e qualquer despesa, instalações necessárias, local e o que for necessário para a realização deste curso correrá por conta da CONTRATADA.
6.2. A carga horária mínima deverá ser de, no mínimo, de 20 horas.
6.3. O curso deverá ser preferencialmente presencial. Este não podendo ocorrer devido a restrições da pandemia de Covid 19 poderá ser ministrado remotamente com a presença de instrutor.
6.4. O instrutor deverá ser certificado no item objeto do curso;
6.5. Disponibilização de material impresso ou para download durante o curso.
6.6. Deverá ser emitido pela CONTRATADA, o certificado de conclusão do curso para os 4 participantes, individualizado.

7. SERVIÇO DE IMPLANTAÇÃO DA FERRAMENTA - ITEM 01 e 02

7.1. Instalação da solução (Quando se aplicar) :

- Instalação de console de gerenciamento;
- Configuração das políticas de segurança;
- Criação dos pacotes de instalação para estações e servidores;
- Fazer o Licenciamento da solução;
- Instalação do agente nos servidores e nas estações de trabalho;
- Criptografia dos computadores e notebooks definidos pelo cliente;
- Criar política de varreduras;
- Definir políticas de configuração

8. Obrigações da Contratada

- A instalação do produto deverá ser realizada de forma remota 8x5 em horário comercial (Seg a Sex, 08 as 18 horas);
- Deverá ser compartilhado link, preferencialmente por e-mail, da CONTRATANTE para download do pacote de instalação;
- A CONTRATADA deverá instalar a solução de antivírus adquirida em toda a empresa incluindo ESCRITÓRIOS DE REPRESENTAÇÃO, SUPERINTENDÊNCIAS E A SEDE.

9. Obrigações da Contratante

- Será disponibilizado conexão com a Internet, MPLS ou VPN;
- Não estão previstos configurações, modificações, aquisição ou fornecimento de equipamentos que não estejam contemplados no escopo deste Termo.

Ministério do Desenvolvimento Regional – MDR
Companhia de Desenvolvimento dos Vales do São Francisco e do Parnaíba
Área de Gestão Estratégica

ANEXO B – Justificativas

A Codevasf promove o desenvolvimento e a revitalização das bacias hidrográficas de sua área de atuação com a utilização sustentável dos recursos naturais e estruturação das atividades produtivas para a inclusão econômica e social. Neste contexto, a Companhia necessita de eficiente e contínuo fluxo de informações por meio da rede central de dados para auxiliar todas as atividades precípuas deste Órgão e suas tomadas de decisões. Através desta rede são estabelecidas as comunicações internas e externas à Codevasf bem como com outros órgãos da Administração Pública.

Atualmente a CODEVASF Sede possui um Data Center com servidores físicos e virtuais destinados aos mais diversos serviços. Estrutura semelhante, porém, de porte menor, é encontrada nos rebatimentos regionais.

Todos estes equipamentos necessitam de softwares, e alguns deles com necessidade de licenciamento. As licenças de uso de software são utilizadas para permitir o uso dos sistemas nos equipamentos aos quais se destinam. Essas licenças são renováveis garantindo a manutenção dos equipamentos com soluções novas, mais seguras e amigáveis.

Em 2004 foi realizado licitação na modalidade Tomada de Preços para fornecimento, instalação e configuração de equipamentos e software para implantação da solução integrada de segurança para ambiente de TI da Codevasf. A vencedora implantou a solução de segurança da McAfee por meio do processo 59500.000342/2004-73 com vigência de 24 (vinte e quatro) meses, de novembro de 2004 a novembro de 2006. Nos anos seguintes, entendo que a solução contratada estava atendendo as necessidades, foram celebrados instrumentos para renovação do contrato em vigor.

Em 2011 a Codevasf contratou por meio de adesão à ata de registro de preço nº 149/2010, oriunda do pregão nº 51/2010, do Ministério da Defesa solução integrada de segurança da fabricante McAfee. O contrato 0.055.00/2011 foi assinado em 10/10/2011 com a PSN Tecnologia Ltda., processo 59500.001624/2011-17. Este contrato foi aditivado uma única vez em 10/10/2012, com fim da vigência em 10/10/2013.

Em agosto de 2014, a Codevasf celebrou com a Tecnologia Ltda - PSN o contrato 0.058.00/201, renovando 1300 licenças de manutenção de software - Gold Business Suporte da solução McAfee End Point Protection Advanced Suite, com garantia de 3 anos, incluindo serviços de instalação, configuração, implementação e repasse tecnológico, para atualização da solução integrada de segurança no ambiente corporativo da Codevasf, Brasília/DF. O contrato se encerrou em agosto de 2015, mas as licenças permaneceram vigentes até 08 de agosto de 2017. Assim, um novo processo licitatório foi executado com o pregão eletrônico 11/2017, resultando no contrato 0.068.00/2017, firmado em 12 de dezembro de 2017 com a empresa NetSafe Corp Ltda. por 24 meses. Foi assinado um termo aditivo de 24 meses, a partir de 12 de dezembro de 2019, que encerrará em 12 de dezembro de 2021.

A Codevasf conta uma complexa estrutura computacional para propiciar o bom desempenho das atividades com vistas a garantir o cumprimento de sua missão institucional. Assim, é fundamental a definição de medidas de segurança que garantam a proteção e a preservação das informações institucionais. Atualmente a Codevasf possui solução integrada da fabricante McAfee que é composta de hardware e software.

A contratação de uma solução de segurança antivírus/endpoint para os ambientes Físicos e virtualizado com garantia, atualizações e repasse de conhecimento é imprescindível para proteger esta estrutura computacional de ataques e softwares maliciosos, evitando assim perda de informações, interrupções nos serviços e comprometimento nos trabalhos.

Alinhamento Estratégico

Projeto está em conformidade com o Planejamento Estratégico Institucional – PEI na perspectiva: 1. Desenvolvimento Institucional e no Tema Estratégico 1.2. Gestão; Bem como, com o Plano Estratégico de Tecnologia da Informação – PETI no item: 7. Garantir a continuidade e disponibilidade dos serviços de TI e em total consonância com o Plano Diretor de Tecnologia da Informação – PDTI no plano de Ação 18 Manutenção da infraestrutura de rede (software, servidores, armazenamento e comunicação) em capacidade para sustentar com qualidade as necessidades dos serviços de TI da CODEVASF.

Da adoção pelo uso do Pregão Eletrônico
A adoção do Pregão Eletrônico visa ampliar a eficiência nesta contratação, a competitividade entre os licitantes, assegurar o tratamento isonômico, buscar maior simplificação, celeridade, transparência e eficiência nos procedimentos para dispêndio de recursos públicos e a seleção da proposta mais vantajosa para a administração pública. Os bens objeto desta contratação se classificam como bens ou serviços comuns, conforme Lei Federal nº 10,520, de 17 de julho de 2002.

Permite Participação de Consórcios: Não – Por se tratar de fornecimento de materiais e equipamentos comuns, a logística necessária para cumprimento do objeto não exige o envolvimento de empresas com diferentes especialidades, não sendo consequentemente pertinente a formação de consórcios com intuito de reforçar a capacidade técnica e financeira do licitante. As empresas isoladas podem perfeitamente conseguir preencher os requisitos necessários para tal.

Critério de Julgamento: Menor preço global por grupo e item – Justifica-se pela maior economicidade e vantajosidade para a administração pública.

Assim o grupo 1 apresenta a necessidade de renovação de licença. Elas devem trabalhar em sincronia e os serviços prestados devem ser para solução de forma holística. Assim a empresa responsável pelo fornecimento da renovação e dos serviços poderá ser responsabilizada por qualquer problema ocorrido neste processo. Isso visa diminuir os riscos com instalações incorretas, falta de comunicação entre as soluções e dificuldades em imputar a responsabilidade ao ente correto.

O item 3 trata do fornecimento de curso para a solução contratada a ser ministrada à 4 alunos com certificação individualizada e duração, mínima, de 20 horas.

Sustentabilidade Ambiental: Serão atendidos os requisitos previstos na legislação aplicável.

Justificativa de reserva de cota de até 25% (vinte e cinco por cento) – Considerando que o objeto da presente licitação, em sua essência, é indivisível por se tratar de atualização de licenças de software e a aplicação de cota tornaria a administração das licenças inviável, pois não há como discernir as responsabilidades dos fornecedores frente ao percentual que lhe cabe. Assim, **não justifica-se** a possibilidade de cotas.

Da composição de preços – cotações:
Para composição dos preços máximos estimados para os itens da licitação, foram feitas cotações junto a várias atas de registro de preços vigentes e a diversos fornecedores regionais e nacionais.

Da Fonte de Recursos: A fonte orçamentária será informada no momento da emissão da Ordem de Fornecimento ou contrato.

Permite Subcontratação: Não será aceito a subcontratação devido à impossibilidade de parcelamento do item contratado.

Valor Estimado: Público, conforme Acórdão nº 1502/2018 – Plenário TCU – Nas licitações realizadas pelas empresas estatais, sempre que o orçamento de referência for utilizado como critério de aceitabilidade das propostas, sua divulgação no edital é obrigatória, e não facultativa, em observância ao princípio constitucional da publicidade e, ainda, por não haver no art. 34 da Lei nº 13.303/2016 (Lei das Estatais) proibição absoluta à revelação do orçamento

Ministério do Desenvolvimento Regional – MDR
Companhia de Desenvolvimento dos Vales do São Francisco e do Parnaíba
Área de Gestão Estratégica

ANEXO C
ESCOPO DE FORNECIMENTO E PLANILHA DE QUANTIDADES E PREÇOS MÁXIMOS

GRUPO 1

Item	Tipo	Descrição	CATMAT CATSER	Unid.	Qtd.	Valor Unitário (R$)	Valor Total (R$)
1	Atualização	Fornecimento **de Atualização de Licenciamento da solução:** • McAfee Complete EndPoint Protection – Business - CEB de caráter perpétuo, para os ambientes Físicos e virtualizado *Vmware*;	27456	Licença	1750	R$ 125,153	R$ 219.018,33
2	Atualização	Fornecimento **de Atualização de Licenciamento da solução:** • McAfee MVISION Threat Intelligence Exchange – TIE de caráter perpétuo, para os ambientes Físicos e virtualizado *Vmware*;	27456	Licença	1750	R$ 57,50	R$ 100.625,00
		TOTAL					R$ 319.643,33

Item	Tipo	Descrição	CATMAT CATSER	Unid.	Qtd.	Valor Unitário (R$)	Valor Total (R$)
3	SERVIÇO	Repasse de conhecimento das funcionalidades / operação da ferramenta (Treinamento)	3840	Aluno	4	R$ 3.200,00	R$ 12.800,00
		TOTAL					R$ 12.800,00

ANEXO D
PLANILHA DE RISCO

Ministério do Desenvolvimento Regional - MDR
Companhia de Desenvolvimento dos Vales do São Francisco e do Parnaíba
Área de Gestão Estratégica

METODOLOGIA DE GERENCIAMENTO DE PROJETOS DA CODEVASF

PLANILHA DE RISCOS

Código / Sigla:	4370
Nome do Projeto:	Manutenção da solução de segurança anti-virus
Líder de Projeto:	Antônio Marques da Cruz

Nº	Categoria	Tipo	Descrição do Risco	Consequência	Probabilidade de Ocorrência	Impacto	Severidade	Ação	Gatilho	Resposta ao Risco	Responsável	Status
01	Operacional	Negativo	Demora nos trâmites internos do processo administrativo	Atraso no cronograma	**Baixa**	**Baixo**	Baixa	Mitigar	Trâmite fora do período previsto no cronograma	Identificar a área onde está o processo administrativo, conversar e pedir celeridade	Ana Paula Lima	Aberto
02	Orçamentário	Positivo	Baixa do valor do dólar	Diminuição do custo do projeto	**Baixa**	**Baixo**	Baixa	Aceitar	Variação cambial	Reavaliação dos itens e quantitativos que serão adquiridos	Henrique Guelber Barros	Aberto
03	Orçamentário	Negativo	Aumento do valor do dólar	Aumento no custo do projeto	**Média**	**Alto**	Alta	Mitigar	Variação cambial	Reavaliação dos itens e quantitativos que serão adquiridos	Henrique Guelber Barros	Aberto
04	Operacional	Negativo	Antivirus desatualizado	fragilidade na segurança dos ativos de rede	**Alto**	**Alto**	**Alto**	Mitigar	Falta de atualização e manutenção	Bloqueios mais efetivos da rede	Antônio Marques	Aberto
05	Operacional	Negativo	Disseminaçã o de virus mais novos	Perda de dados	**Média**	**Alto**	Alta	Mitigar	Isolar maquinas contaminadas	Bloqueios mais efetivos da rede	Antônio Marques	Aberto

Tabela de Severidade

		Impacto		
		Baixo	Médio	Alto
Probabilidade	Baixa	Baixa	Baixa	Média
	Média	Baixa	Média	Alta
	Alta	Média	Alta	Alta

ANEXO E
PROPOSTAS

Grupo 1

Item	Tipo	Descrição	CATMAT CATSER	Unid.	Qtd.	Valor Unitário (R$)	Valor Total (R$)
1	Aquisição	Fornecimento **de Atualização de Licenciamento da solução:** • McAfee Complete EndPoint Protection – Business - CEB de caráter perpétuo, para os ambientes Físicos e virtualizado *Vmware*;	27456	Licença	1750		
2	Aquisição	Fornecimento **de Atualização de Licenciamento da solução:** • McAfee MVISION Threat Intelligence Exchange – TIE de caráter perpétuo, para os ambientes Físicos e virtualizado *Vmware*;	27456	Licença	1750		

Item	Tipo	Descrição	CATMAT CATSER	Unid.	Qtd.	Valor Unitário (R$)	Valor Total (R$)
3	SERVIÇO	Repasse de conhecimento das funcionalidades / operação da ferramenta (Treinamento)	3840	Aluno	4		