SERVIÇO PÚBLICO FEDERAL

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP

EDITAL DE PREGÃO ELETRÔNICO Nº 010/2021
PROCESSO ADMINISTRATIVO Nº 066/2021

Torna-se público, para conhecimento dos interessados, que o Conselho Regional de Engenharia e Agronomia do Estado de São Paulo – CREA-SP, por meio da Unidade de Licitações – UL, sediada à Avenida Brigadeiro Faria Lima, 1059, 8º andar – Pinheiros – São Paulo – SP, CEP – 01452-920, realizará licitação, na modalidade PREGÃO, na forma ELETRÔNICA, com o critério de julgamento do tipo **menor preço**, nos termos da Lei nº 10.520, de 17 de julho de 2002, da Lei nº 8.248, de 22 de outubro de 1991, do Decreto nº 10.024, de 20 de setembro de 2019, do Decreto 9.507, de 21 de setembro de 2018, do Decreto nº 7.746, de 05 de junho de 2012, do Decreto nº 7.174, de 12 de maio de 2010, da Instrução Normativa SGD/ME nº 1, de 04 de abril de 2019, das Instruções Normativas SEGES/MP nº 05, de 26 de maio de 2017 e nº 03, de 26 de abril de 2018 e da Instrução Normativa SLTI/MP nº 01, de 19 de janeiro de 2010, da Lei Complementar n° 123, de 14 de dezembro de 2006, da Lei nº 11.488, de 15 de junho de 2007, do Decreto n° 8.538, de 06 de outubro de 2015, aplicando-se, subsidiariamente, a Lei nº 8.666, de 21 de junho de 1993 e as exigências estabelecidas neste Edital.

Data da sessão: **30/08/2021;**
UASG: **389423**;
Horário da Realização do Pregão: 10h.
Local: Portal Compras do Governo Federal – www.comprasgovernamentais.gov.br.

1 DO OBJETO

1.1 O objeto da presente licitação é a escolha da proposta mais vantajosa para a contratação de empresa especializada para fornecimento de serviços de atualização das licenças para o Antivirus Kaspersky, com suporte e capacitação, conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.

1.2. A licitação será realizada em grupo único, formado por 04 (quatro) itens, conforme tabela constante no Termo de Referência, devendo o licitante oferecer proposta para todos os itens que o compõem.

1.3. O critério de julgamento adotado será o de menor preços do grupo único sob a forma de execução indireta, no regime de empreitada por preço global do grupo único, observadas as exigências contidas neste Edital e seus anexos quanto às especificações do objeto.

SERVIÇO PÚBLICO FEDERAL

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP

2. DA DOTAÇÃO ORÇAMENTÁRIA

2.1. A despesa para atender a esta licitação está programada em dotação orçamentária própria da Equipe de Sustentação, Suporte e Infraestrutura de TIC – ESSITIC da Gerência de Desenvolvimento e Execução de Projetos - GDEP, prevista no orçamento do CREA-SP no exercício de financeiro de 2021, oriundo da conta nº 6.2.2.1.1.01.04.09.005 – Serviços de Informática - PJ.

2.2 A despesa com a execução dos serviços de que trata o objeto desta licitação é estimada no período de 36 (trinta e seis) meses.

3 DO CREDENCIAMENTO

3.1 O Credenciamento é o nível básico do registro cadastral no Sistema de Cadastramento Unificado de Fornecedores - SICAF, que permite a participação dos interessados na modalidade licitatória Pregão, em sua forma eletrônica.

3.2 O cadastro no SICAF deverá ser feito no Portal de Compras do Governo Federal, no sítio www.comprasgovernamentais.gov.br, por meio de certificado digital conferido pela Infraestrutura de Chaves Públicas Brasileira – ICP - Brasil.

3.3 O credenciamento junto ao provedor do sistema implica a responsabilidade do licitante ou de seu representante legal e a presunção de sua capacidade técnica para realização das transações inerentes a este Pregão.

3.4 O licitante responsabiliza-se exclusiva e formalmente pelas transações efetuadas em seu nome, assumir como firmes e verdadeiras suas propostas e seus lances, inclusive os atos praticados diretamente ou por seu representante, excluída a responsabilidade do provedor do sistema ou do órgão ou entidade promotora da licitação por eventuais danos decorrentes de uso indevido da senha, ainda que por terceiros.

3.5 É de responsabilidade do cadastrado conferir a exatidão dos seus dados cadastrais no SICAF e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados.

3.5.1 A não observância do disposto no subitem anterior poderá ensejar desclassificação no momento da habilitação

SERVIÇO PÚBLICO FEDERAL

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP

4 DA PARTICIPAÇÃO NO PREGÃO

4.1 Poderão participar deste Pregão interessados cujo ramo de atividade seja compatível com o objeto desta licitação, e que estejam com Credenciamento Regular no Sistema de Cadastramento Unificado de Fornecedores – SICAF, conforme disposto no art. 9º da IN SEGES/MP nº 3, de 2018.

4.2 Os licitantes deverão utilizar o certificado digital para acesso ao Sistema.

4.3 **Não poderão participar desta licitação os interessados:**

4.3.1 Proibidos de participar de licitações e celebrar contratos administrativos, na forma da legislação vigente;

4.3.2 Que não atendam às condições deste Edital e seus anexos;

4.3.3 Estrangeiros que não tenham representação legal no Brasil com poderes expressos para receber citação e responder administrativa ou judicialmente;

4.3.4 Que se enquadrem nas vedações previstas no artigo 9º da Lei nº 8.666, de 1993;

4.3.5 Que estejam sob falência, concurso de credores, concordata ou insolvência, em processo de dissolução ou liquidação;

4.3.6 Entidades empresariais que estejam reunidas em consórcio;

4.3.7 Organizações da Sociedade Civil de Interesse Público - OSCIP, atuando nessa condição (Acórdão nº 746/2014-TCU-Plenário);

4.4 Nos termos do art. 5º do Decreto nº 9.507, de 2018, é vedada a contratação de pessoa jurídica na qual haja administrador ou sócio com poder de direção, familiar de:

a) Detentor de cargo em comissão ou função de confiança que atue na área responsável pela demanda ou contratação; ou

b) De autoridade hierarquicamente superior no âmbito do órgão contratante.

4.4.1 Para os fins do disposto neste item, considera-se familiar o cônjuge, o companheiro ou o parente em linha reta ou colateral, por consanguinidade ou afinidade, até o terceiro grau (Súmula Vinculante/STF nº 13, art. 5º, inciso V, da Lei nº 12.813, de 16 de maio de 2013 e art. 2º, inciso III, do Decreto nº 7.203, de 04 de junho de 2010);

SERVIÇO PÚBLICO FEDERAL

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP

4.5 Nos termos do art. 7° do Decreto n° 7.203, de 2010, é vedada, ainda, a utilização, na execução dos serviços contratados, de empregado da futura Contratada que seja familiar de agente público ocupante de cargo em comissão ou função de confiança neste órgão contratante.

4.6 Como condição para participação no Pregão, o licitante assinalará “sim” ou “não” em campo próprio do sistema eletrônico, relativo às seguintes declarações:Que cumpre os requisitos estabelecidos no artigo 3° da Lei Complementar nº 123, de 2006, estando apto a usufruir do tratamento favorecido estabelecido em seus arts. 42 a 49.

4.6.1.1 Nos itens exclusivos para participação de microempresas e empresas de pequeno porte, a assinalação do campo “não” impedirá o prosseguimento no certame;

4.6.1.2 Nos itens em que a participação não for exclusiva para microempresas e empresas de pequeno porte, a assinalação do campo “não” apenas produzirá o efeito de o licitante não ter direito ao tratamento favorecido previsto na Lei Complementar nº 123, de 2006, mesmo que microempresa, empresa de pequeno porte.

4.6.2 Que está ciente e concorda com as condições contidas no Edital e seus anexos;

4.6.3 Que cumpre os requisitos de habilitação definidos no Edital e que a proposta apresentada está em conformidade com as exigências editalícias;

4.6.4 Que inexistem fatos impeditivos para sua habilitação no certame, ciente da obrigatoriedade de declarar ocorrências posteriores;

4.6.5 Que não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do artigo 7°, XXXIII, da Constituição;

4.6.6 Que a proposta foi elaborada de forma independente, nos termos da Instrução Normativa SLTI/MP nº 2, de 16 de setembro de 2009.

4.6.7 Que não possui, em sua cadeia produtiva, empregados executando trabalho degradante ou forçado, observando o disposto nos incisos III e IV do art. 1º e no inciso III do art. 5º da Constituição Federal;

4.6.8 Que os serviços são prestados por empresas que comprovem cumprimento de reserva de cargos prevista em lei para pessoa com deficiência ou para reabilitado da Previdência Social e que

atendam às regras de acessibilidade previstas na legislação, conforme disposto no art. 93 da Lei nº 8.213, de 24 de julho de 1991.

4.6.9 Que cumpre os requisitos do Decreto nº 7.174, de 2010, estando apto a usufruir dos critérios de preferência.

4.6.9.1 A assinalação do campo "não" apenas produzirá o efeito de o licitante não ter direito ao tratamento favorecido previsto no Decreto nº 7.174, de 2010.

4.7 A declaração falsa relativa ao cumprimento de qualquer condição sujeitará o licitante às sanções previstas em lei e neste Edital.

4.8 **Estimativa de preços e preços referenciais**

4.8.1. A estimativa de preços e preços referenciais para aquisição/contratação é sigiloso e, será tornado público apenas e imediatamente após o encerramento do envio de lances, sem prejuízo da divulgação do detalhamento dos quantitativos e das demais informações necessárias à elaboração das propostas, nos termos do art. 15 do Decreto nº 10.024, de 20 de setembro de 2019, do art. 7º, §3º da Lei nº 12.527, de 2011, e do art. 20 do Decreto nº 7.724, de 2012.

5 DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

5.1 Os licitantes encaminharão, exclusivamente por meio do sistema, concomitantemente com os documentos de habilitação exigidos no Edital, proposta de preços (Anexo II deste Edital), devidamente preenchida com todos os dados, inclusive assinada pelo representante legal, até a data e o horário estabelecidos para a abertura da sessão pública, quando, então, encerrar-se-á automaticamente a etapa de envio dessa documentação.

5.2 O Envio da proposta, acompanhada dos documentos de habilitação exigidos neste Edital, ocorrerá por meio de chave de acesso e senha.

5.3 Os licitantes poderão deixar de apresentar os documentos de habilitação que constem do SICAF, assegurado aos demais licitantes o direito de acesso aos dados constantes dos sistemas.

5.4 As Microempresas e Empresas de Pequeno Porte deverão encaminhar a documentação de habilitação, ainda que haja alguma restrição de regularidade fiscal e trabalhista, nos termos do art. 43, §1º, da LC nº 123, de 2006.

5.5 Incumbirá ao licitante acompanhar as operações no sistema eletrônico durante a sessão pública do Pregão, ficando responsável pelo ônus decorrente da perda de negócios, diante da inobservância de quaisquer mensagens emitidas pelo sistema ou de sua desconexão.

5.6 Até a abertura da sessão pública, os licitantes poderão retirar ou substituir a proposta e os documentos de habilitação anteriormente inseridos no sistema;

5.7 Não será estabelecida, nessa etapa do certame, ordem de classificação entre as propostas apresentadas, o que somente ocorrerá após a realização dos procedimentos de negociação e julgamento da proposta.

5.8 Os documentos que compõem a proposta e a habilitação do licitante melhor classificado somente serão disponibilizados para avaliação do Pregoeiro e para acesso público após o encerramento do envio de lances.

6 DO PREENCHIMENTO DA PROPOSTA

6.1 O licitante deverá enviar sua proposta mediante o preenchimento, no sistema eletrônico, dos seguintes campos:

6.1.1 Valor Total Geral do Grupo 1 – Único – considerando o descrito no Termo de Referencia – Anexo I, deste Edital;

6.1.2 Descrição do objeto, contendo as informações similares à especificação do Termo de Referência.

6.2 Todas as especificações do objeto contidas na proposta vinculam a Contratada.

6.3 Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente no fornecimento de serviços de atualização das licenças, apurados mediante o preenchimento do modelo de proposta de preços, conforme anexo deste Edital.

6.4 A empresa é a única responsável pela cotação correta dos encargos tributários.

6.5 A apresentação das propostas implica obrigatoriedade do cumprimento das disposições nelas contidas, em conformidade com o que dispõe o Termo de Referência, assumindo o proponente o compromisso de executar os serviços nos seus termos, bem como de fornecer os materiais,

equipamentos, ferramentas e utensílios necessários, em quantidades e qualidades adequadas à perfeita execução contratual, promovendo, quando requerido, sua substituição.

6.6 Os preços ofertados, tanto na proposta inicial, quanto na etapa de lances, serão de exclusiva responsabilidade do licitante, não lhe assistindo o direito de pleitear qualquer alteração, sob alegação de erro, omissão ou qualquer outro pretexto.

6.7 O prazo de validade da proposta não será inferior a 60 (sessenta) dias, a contar da data de sua apresentação.

6.8 Os licitantes devem respeitar os preços máximos estabelecidos nas normas de regência de contratações públicas federais, quando participarem de licitações públicas.

6.8.1 O descumprimento das regras supramencionadas pela Administração por parte dos contratados pode ensejar a fiscalização do Tribunal de Contas da União e, após o devido processo legal, gerar as seguintes consequências: assinatura de prazo para a adoção das medidas necessárias ao exato cumprimento da lei, nos termos do art. 71, inciso IX, da Constituição; ou condenação dos agentes públicos responsáveis e da empresa contratada ao pagamento dos prejuízos ao erário, caso verificada a ocorrência de superfaturamento por sobrepreço na execução do contrato.

7 DA ABERTURA DA SESSÃO, CLASSIFICAÇÃO DAS PROPOSTAS E FORMULAÇÃO DE LANCES

7.1. A abertura da presente licitação dar-se-á em sessão pública, por meio de sistema eletrônico, na data, horário e local indicados neste Edital.

7.2. O Pregoeiro verificará as propostas apresentadas, desclassificando desde logo aquelas que não estejam em conformidade com os requisitos estabelecidos neste Edital, contenham vícios insanáveis, ilegalidades, ou não apresentem as especificações exigidas no Termo de Referência.

7.2.1. Também será desclassificada a proposta que identifique o licitante (que se identificar quando do preenchimento no sistema da descrição detalhada do objeto ofertado, de livre acesso a todos os licitantes que servirá de análise prévia antes do início da etapa de lances).

7.2.2. A desclassificação da proposta será sempre fundamentada e registrada no sistema, com acompanhamento em tempo real por todos os participantes.

SERVIÇO PÚBLICO FEDERAL

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP

7.2.3. A não desclassificação da proposta não impede o seu julgamento definitivo em sentido contrário, levado a efeito na fase de aceitação.

7.3. O sistema ordenará automaticamente as propostas classificadas pelo Pregoeiro, sendo que somente estas participarão da fase de lances.

7.4. O sistema disponibilizará campo próprio para troca de mensagens entre o Pregoeiro e os licitantes.

7.5. Iniciada a etapa competitiva, os licitantes deverão encaminhar lances exclusivamente por meio de sistema eletrônico, sendo imediatamente informados do seu recebimento e do valor consignado no registro.

7.5.1. O lance deverá ser ofertado pelo Valor Total Grupo 1 - Único.

7.6. Os licitantes poderão oferecer lances sucessivos, observando o horário fixado para abertura da sessão e as regras estabelecidas no Edital.

7.7. O licitante somente poderá oferecer lance de valor inferior ao último por ele ofertado e registrado pelo sistema.

7.8. O intervalo mínimo de diferença de valores entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta deverá ser de R$ 100,00 (cem reais).

7.9. Será adotado para o envio de lances no pregão eletrônico o modo de disputa **“ABERTO”** em que os licitantes apresentarão lances públicos e sucessivos, com prorrogações.

7.10. A etapa de lances da sessão pública terá duração de 10 (dez) minutos e, após isso, será prorrogada automaticamente pelo sistema quando houver lances ofertado nos últimos 02 (dois) minutos do período de duração da sessão pública.

7.11. A prorrogação automática da etapa de lances, de que trata o item anterior, será de 02 (dois) minutos e ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive no caso de lances intermediários.

7.12. Não havendo novos lances na forma estabelecida nos itens anteriores, a sessão pública encerrar-se-á automaticamente.

7.13. Encerrada a fase competitiva sem que haja prorrogação automática pelo sistema, poderá o Pregoeiro, assessorado pela equipe de apoio, justificadamente, admitir o reinício da sessão pública de lances, em prol da consecução do melhor preço.

7.14. Não serão aceitos dois ou mais lances de mesmo valor, prevalecendo aquele que for recebido e registrado em primeiro lugar.

7.15. Durante o transcurso da sessão pública, os licitantes serão informados, em tempo real, do valor do menor lance registrado, vedada a identificação do licitante.

7.16. No caso de desconexão do sistema eletrônico com o Pregoeiro, no decorrer da etapa competitiva do pregão, o sistema eletrônico poderá permanecer acessível aos licitantes para a recepção dos lances.

7.17. Quando a desconexão do sistema eletrônico para o Pregoeiro persistir por tempos superior a 10 (dez) minutos, a sessão pública será suspensa e reiniciada somente após decorridas 24 (vinte e quatro) horas da comunicação do fato pelo Pregoeiro aos participantes no sítio eletrônico utilizado para divulgação.

7.18. O Critério de julgamento adotado será o menor preço do Grupo 1 – Único, conforme definido neste Edital e seus anexos.

7.19. Caso o licitante não apresente lances, concorrerá com o valor de sua proposta e na hipótese de desistência de apresentar outros lances, valerá o último lance por ele ofertado, para efeito de ordenação das propostas.

7.20. Em relação a itens não exclusivos para participação de microempresas e empresas de pequeno porte, uma vez encerrada a etapa de lances, será efetivada a verificação automática, junto à Receita Federal, do porte da entidade empresarial. O sistema identificará em coluna própria as microempresas e empresas de pequeno porte participantes, procedendo à comparação com os valores da primeira colocada, se esta for empresa de maior porte, assim como das demais classificadas, para o fim de aplicar-se o disposto nos arts. 44 e 45 da LC nº 123, de 2006, regulamentada pelo Decreto nº 8.538, de 2015.

7.21. Nessas condições, as propostas de microempresas e empresas de pequeno porte que se encontrarem na faixa de até 5% (cinco por cento) acima do melhor lance serão consideradas empatadas com a primeira colocada.

7.22. A melhor classificada nos termos do item anterior terá o direito de encaminhar uma última oferta para desempate, obrigatoriamente em valor inferior ao da primeira colocada, no prazo de 05 (cinco) minutos controlados pelo sistema, contados após a comunicação automática para tanto.

7.23. Caso a microempresa ou a empresa de pequeno porte melhor classificada desista ou não se manifeste no prazo estabelecido, serão convocadas as demais licitantes microempresa e empresa de pequeno porte que se encontrem naquele intervalo de 5% (cinco por cento), na ordem de classificação, para o exercício do mesmo direito, no prazo estabelecido no subitem anterior.

7.24. No caso de equivalência dos valores apresentados pelas microempresas e empresas de pequeno porte que se encontrem nos intervalos estabelecidos nos subitens anteriores, será realizado sorteio entre elas para que se identifique aquela que primeiro poderá apresentar melhor oferta.

7.25. Só poderá haver empate entre propostas iguais (não seguidas de lances), ou entre lances finais da fase fechada do modo de disputa aberto e fechado.

7.26. Havendo eventual empate entre propostas, o critério de desempate será aquele previsto no art. 3º, § 2º, da Lei nº 8.666, de 1993, assegurando-se a preferência, sucessivamente, aos bens produzidos:

7.27.1. Prestados por empresas brasileiras;

7.27.3 Prestados por empresas que invistam em pesquisa e no desenvolvimento de tecnologia no País;

7.27.4 Prestados por empresas que comprovem cumprimento de reserva de cargos prevista em lei para pessoa com deficiência ou para reabilitado da Previdência Social e que atendam às regras de acessibilidade previstas na legislação.

7.27. Persistindo o empate, a proposta vencedora será sorteada pelo sistema eletrônico dentre as propostas empatadas.

7.28. Encerrada a etapa de envio de lances da sessão pública, o Pregoeiro deverá encaminhar, pelo sistema eletrônico, contraproposta ao licitante que tenha apresentado o melhor preço, para que seja obtida melhor proposta, vedada a negociação em condições diferentes das prevista deste Edital.

7.28.1. A negociação será realizada por meio do sistema, podendo ser acompanhada pelos demais licitantes.

7.28.2. O Pregoeiro solicitará ao licitante melhor classificado que, no prazo de 02 (duas) horas, envie a proposta adequada ao último lance ofertado após a negociação realizada, acompanhada, se for o caso, dos documentos complementares, quando necessários à confirmação daqueles exigidos neste Edital e já apresentados.

7.28.2.1. É facultado ao Pregoeiro prorrogar o prazo estabelecido, a partir de solicitação fundamentada feita no chat pelo licitante, antes de findo o prazo.

7.29. Após a negociação do preço, o Pregoeiro iniciará a fase de aceitação e julgamento da proposta.

7.30. Será assegurado o direito de preferência previsto no seu art. 3º, conforme procedimento estabelecido nos arts. 5° e 8° do Decreto n° 7.174, de 2010.

7.30.1. Os licitantes qualificados como microempresas ou empresas de pequeno porte que fizerem jus ao direito de preferência previsto no Decreto nº 7.174, de 2010, terão prioridade no exercício desse benefício em relação às médias e às grandes empresas na mesma situação.

8 DA ACEITABILIDADE DA PROPOSTA VENCEDORA

8.1. Encerrada a etapa de negociação, o Pregoeiro examinará a proposta classificada em primeiro lugar quanto à adequação ao objeto e à compatibilidade de preço em relação ao máximo estipulado para contratação neste Edital e em seus anexos, observado o disposto no parágrafo único do art. 7º e no §9º do art. 26 do Decreto nº 10.024/2019.

8.2. A análise da exequibilidade da proposta de preços deverá ser realizada com o auxílio da proposta de formação de Preços, a ser preenchida pelo licitante em relação à sua proposta final, conforme anexo deste Edital.

8.3. A proposta a ser encaminhada deverá conter:

8.3.1. Prazo de validade da proposta não inferior a 60 (sessenta) dias, a contar da data de abertura do certame.

8.3.2. Especificações do objeto de forma clara, observadas as especificações constantes neste Edital e seus anexos;

8.3.3. Preços unitários e valor global da proposta, em algarismo, expresso em moeda corrente nacional (real), de acordo com os preços praticados no mercado, considerando o modelo de proposta de preços anexo ao Edital;

8.3.4. Nos preços cotados deverão estar incluídos todos os insumos que os compõem, tais como despesas com impostos, taxas, fretes, seguros e quaisquer outros que incidam na contratação do objeto;

8.4. A proposta de Preços deverá ser encaminhada pelo licitante exclusivamente via sistema, no prazo de 02 (duas) horas, contado da solicitação do Pregoeiro, com os respectivos valores adequados ao lance vencedor e será analisada pelo Pregoeiro no momento da aceitação do lance vencedor.

8.4.1. Nas contratações de serviços com regime de dedicação exclusiva de mão de obra executados de forma contínua ou não, e nas contratações que tenham por métrica o uso de “horas”, a licitante classificada em primeiro lugar deverá apresentar a Planilha de Custos e Formação de Preços, nos termos da IN 05/2017. A mesma deverá ser encaminhada pelo licitante exclusivamente via sistema, juntamente com a Proposta, devidamente readequada, no prazo acima estipulado.

8.5. A inexequibilidade dos valores referentes a itens isolados da proposta de preços não caracteriza motivo suficiente para a desclassificação da proposta, desde que não contrariem exigências legais.

8.6. Será desclassificada a proposta, nos termos do item 9.1 do Anexo VII-A da In SEGES/MPDG nº 5/2017, que:

8.6.1. Não estiver em conformidade com os requisitos estabelecidos neste Edital;

8.6.2. Contenha vício insanável ou ilegalidade;

8.6.3. Não apresente as especificações técnicas exigidas pelo Termo de Referência;

8.6.4. Apresentar preço final superior ao preço máximo fixado (Acórdão nº 1455/2018-TCU – Plenário), ou que apresentar preço manifestamente inexequível.

8.7. Quando o licitante não conseguir comprovar que possui ou possuirá recursos suficientes para executar a contento o objeto, será considerada inexequível a proposta de preços que:

8.7.1. For insuficiente para a cobertura dos custos da contratação, apresente preços global ou unitários simbólicos, irrisórios ou de valor zero, incompatíveis com os preços dos insumos e salários de mercado, acrescidos dos respectivos encargos, ainda que o ato convocatório da licitação não tenha estabelecido limites mínimos, exceto quando se referirem a materiais e instalações de propriedade do próprio licitante, para os quais ele renuncie a parcela ou à totalidade da remuneração.

8.8. Se houver indícios de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, poderão ser efetuadas diligências, na forma do § 3° do artigo 43 da Lei n° 8.666, de 1993 e a exemplo das enumeradas no item 9.4 do Anexo VII-A da IN SEGES/MPDG nº 5, de 2017, para que a empresa comprove a exequibilidade da proposta.

8.9. Quando o licitante apresentar preço final inferior a 30% (trinta por cento) da média dos preços ofertados para o mesmo item, e a inexequibilidade da proposta não for flagrante e evidente pela análise da proposta, não sendo possível a sua imediata desclassificação, será obrigatória a realização de diligências para aferir a legalidade e exequibilidade da proposta.

8.10. Qualquer interessado poderá requerer que se realizem diligências para aferir a exequibilidade e a legalidade das propostas, devendo apresentar as provas ou os indícios que fundamentam a suspeita.

8.10.1. Na hipótese de necessidade de suspensão de sessão pública para a realização de diligências, com vista ao saneamento das propostas, a sessão pública somente poderá ser reiniciada mediante aviso prévio no sistema com, no mínimo, 24 (vinte e quatro) horas de antecedência, e a ocorrência será registrada em ata.

8.11. O Pregoeiro poderá convocar o licitante para enviar documento digital complementar, por meio de funcionalidade disponível no sistema, no prazo de **02 (duas) horas**, sob pena de não aceitação da proposta.

8.11.1. É facultado ao Pregoeiro prorrogar o prazo estabelecido, a partir da solicitação fundamentada feita no chat pelo licitante, antes de finfo o prazo.

8.12. Erros no preenchimento da proposta não constituem motivo para a desclassificação da proposta. A proposta poderá ser ajustada pelo licitante, no prazo indicado pelo Pregoeiro, desde que não haja majoração do preço proposto.

8.12.1. O ajuste de que trata este dispositivo se limita a sanar erros ou falhas que não alterem a substância das propostas.

8.13. Para fins de análise da proposta quanto ao cumprimento das especificações do objeto, poderá ser colhida a manifestação escrita do setor requisitante ou da área especializada no objeto.

8.14. Se a proposta for desclassificada, o Pregoeiro examinará a proposta subsequente, e, assim sucessivamente, na ordem de classificação.

8.15. Havendo necessidade, o Pregoeiro suspenderá a sessão, informando no “chat” a nova data e horário para a sua continuidade.

8.16. Nos itens não exclusivos para a participação de microempresas e empresas de pequeno porte, sempre que a proposta não for aceita, e antes de o Pregoeiro passar à subsequente, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto nos artigos 44 e 45 da LC nº 123, de 2006, seguindo-se a disciplina antes estabelecida, se for o caso.

8.17. Encerrada a análise quanto à aceitação da proposta, o Pregoeiro verificará a habilitação do licitante, observado o disposto neste Edital.

9. DA HABILITAÇÃO

9.1. Como condição prévia ao exame da documentação de habilitação do licitante detentor da proposta classificada em primeiro lugar, o Pregoeiro verificará o eventual descumprimento das condições de participação, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

NOTA: - Visando melhor organização processual, solicitamos aos licitantes que, quando forem inserir no sistema do Comprasnet os documentos relativos a este item (habilitação), observem a ordem crescente dos subitens conforme se apresentam.

a) www.comprasgovernamentais.gov.br/ - SICAF;

b) Cadastro Nacional de Empresas Inidôneas e Suspensas - CEIS, mantido pela Controladoria-Geral da União - www.portaldatransparencia.gov.br/ceis

c) Cadastro Nacional de Condenações Cíveis por Atos de Improbidade Administrativa, mantido pelo Conselho Nacional de Justiça www.cnj.jus.br/improbidade_adm/consultar_requerido.php

SERVIÇO PÚBLICO FEDERAL

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP

d) Lista de Inidôneos e o Cadastro Integrado de Condenações por Ilícitos Administrativos - CADICON, mantidos pelo Tribunal de Contas da União - TCU;

9.1.1. Para a consulta de licitantes pessoa jurídica poderá haver a substituição das consultas das alíneas “b”, “c” e “d” acima pela Consulta Consolidada de Pessoa Jurídica do TCU - https://certidoesapf.apps.tcu.gov.br/

9.1.2. A consulta aos cadastros será realizada em nome da empresa licitante e também de seu sócio majoritário, por força do artigo 12 da Lei n° 8.429, de 1992, que prevê, dentre as sanções impostas ao responsável pela prática de ato de improbidade administrativa, a proibição de contratar com o Poder Público, inclusive por intermédio de pessoa jurídica da qual seja sócio majoritário.

9.1.2.1. Caso conste na Consulta de Situação do Fornecedor a existência de Ocorrências Impeditivas Indiretas, o gestor diligenciará para verificar se houve fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas.

9.1.2.2. A tentativa de burla será verificada por meio dos vínculos societários, linhas de fornecimento similares, dentre outros.

9.1.2.3. O licitante será convocado para manifestação previamente à sua desclassificação.

9.1.3. Constatada a existência de sanção, o Pregoeiro reputará o licitante inabilitado, por falta de condição de participação.

9.1.4. No caso de inabilitação, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto nos arts. 44 e 45 da Lei Complementar nº 123, de 2006, seguindo-se a disciplina antes estabelecida para aceitação da proposta subsequente.

9.2. Caso atendidas as condições de participação, a habilitação do licitante será verificada por meio do SICAF, nos documentos por ele abrangidos, em relação à habilitação jurídica, à regularidade fiscal e à qualificação econômica financeira, conforme o disposto na Instrução Normativa SEGES/MP nº 03, de 2018.

9.2.1. O interessado, para efeitos de habilitação prevista na Instrução Normativa SEGES/MP nº 03, de 2018 mediante utilização do sistema, deverá atender às condições exigidas no cadastramento no SICAF até o 3º (terceiro) dia útil anterior à data prevista para recebimento das propostas;

9.2.2. É dever do licitante atualizar previamente as comprovações constantes do SICAF para que estejam vigentes na data da abertura da sessão pública, ou encaminhar, em conjunto com a apresentação da proposta, a respectiva documentação atualizada.

9.2.3. O descumprimento do subitem acima implicará a inabilitação do licitante, exceto se a consulta aos sítios eletrônicos oficiais emissores de certidões feita pelo Pregoeiro lograr êxito em encontrar a(s) certidão(ões) válida(s), conforme art. 43, §3º, do Decreto 10.024, de 2019.

9.3. Havendo a necessidade de envio de documentos de habilitação complementares, necessários à confirmação daqueles exigidos neste Edital e já apresentados, o licitante será convocado a encaminhá-los, em formato digital, via sistema, no prazo de **02 (duas) horas**, sob pena de inabilitação.

9.4. Somente haverá a necessidade de comprovação do preenchimento de requisitos mediante a apresentação dos documentos originais não-digitais quando houver dúvida em relação à integridade do documento digital.

9.5. Não serão aceitos documentos de habilitação com indicação de CNPJ/CPF diferentes, salvo aqueles legalmente permitidos.

9.6. Se o licitante for a matriz, todos os documentos deverão estar em nome da matriz, e se o licitante for a filial, todos os documentos deverão estar em nome da filial, exceto aqueles documentos que, pela própria natureza, comprovadamente, forem emitidos somente em nome da matriz.

9.6.1. Serão aceitos registros de CNPJ de licitante matriz e filial com diferentes números de documentos pertinentes ao CND e ao CRF/FGTS, quando for comprovada a centralização do recolhimento dessas contribuições.

9.7. Ressalvado o disposto do item "**5.3"**, os licitantes deverão encaminhar, nos termos deste Edital, a documentação nos itens a seguir, para fins de habilitação.

9.8. **HABILITAÇÃO JURÍDICA**

9.8.1. No caso de sociedade empresária ou empresa individual de responsabilidade limitada - EIRELI: ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado na Junta Comercial da respectiva sede, acompanhado de documento comprobatório de seus administradores;

9.8.2. Inscrição no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz, no caso de ser a participante sucursal, filial ou agência;

9.8.3. No caso de sociedade simples: inscrição do ato constitutivo no Registro Civil das Pessoas Jurídicas do local de sua sede, acompanhada de prova da indicação dos seus administradores;

9.8.4. Decreto de autorização, em se tratando de sociedade empresária estrangeira em funcionamento no País;

9.8.5. Os documentos acima deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

9.9. REGULARIDADE FISCAL E TRABALHISTA

9.9.1. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas - CNPJ;

9.9.2. Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02/10/2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional;

9.9.3. Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

9.9.4. Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943;

9.9.5. Prova de inscrição no cadastro de contribuintes municipal, relativo ao domicílio ou sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

9.9.6. Prova de regularidade com a Fazenda Municipal do domicílio ou sede do licitante, relativa à atividade em cujo exercício contrata ou concorre;

9.9.7. Prova de inscrição no cadastro de contribuintes estadual, relativo ao domicílio ou sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

9.9.8. Prova de regularidade com a Fazenda Estadual do domicílio ou sede do licitante, relativa à atividade em cujo exercício contrata ou concorre.

9.9.9. **Caso o licitante seja considerado isento dos tributos municipais ou estaduais relacionados ao objeto licitatório, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda Municipal ou Fazenda Estadual do seu domicílio ou sede, ou outra equivalente, na forma da lei.**

9.10. QUALIFICAÇÃO ECONÔMICO-FINANCEIRA

9.10.1. **Certidão negativa de falência** expedida pelo distribuidor da sede da pessoa jurídica;

9.10.2. **Balanço patrimonial e demonstrações contábeis** do último exercício social, já exigíveis e apresentados na forma da lei, que comprovem a boa situação financeira da empresa, vedada a sua substituição por balancetes ou balanços provisórios, podendo ser atualizados por índices oficiais quando encerrado há mais de 03 (três) meses da data de apresentação da proposta;

9.10.2.1. No caso de empresa constituída no exercício social vigente, admite-se a apresentação de balanço patrimonial e demonstrações contábeis referentes ao período de existência da sociedade;

9.10.2.2. É admissível o balanço intermediário, se decorrer de lei ou contrato/estatuto social.

9.10.3. **Comprovação da boa situação financeira** da empresa mediante obtenção de índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), superiores a 1 (um), obtidos pela aplicação das seguintes fórmulas:

LG	**=**	Ativo Circulante + Realizável a Longo Prazo
		Passivo Circulante + Passivo Não Circulante
SG	**=**	Ativo Total
		Passivo Circulante + Passivo Não Circulante
LC	**=**	Ativo Circulante
		Passivo Circulante

9.10.4. As empresas, cadastradas ou não no SICAF, que apresentarem resultado inferior ou igual a 1 (um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), deverão comprovar patrimônio líquido mínimo de 10% (dez por cento) do valor total estimado da contratação.

9.11. QUALIFICAÇÃO TÉCNICA

9.11.1. O licitante deverá apresentar comprovação de aptidão para o fornecimento de bens/serviços em características, quantidades e prazos compatíveis com o objeto desta licitação, por meio de apresentação de atestados fornecidos por pessoas jurídicas de direito público ou privado.

9.11.1.1. Os atestados deverão referir-se a vendas/serviços prestados no âmbito de sua atividade econômica principal ou secundária especificadas no contrato social vigente;

9.11.1.2. Somente serão aceitos atestados expedidos após a conclusão do contrato ou se decorrido, pelo menos, um ano do início de sua execução, exceto se firmado para ser executado em prazo inferior, conforme item 10.8 do Anexo VII-A da IN SEGES/MPDG nº 5, de 2017.

9.11.2. Poderá ser admitida, para fins de comprovação de quantitativo mínimo do serviço, a apresentação de diferentes atestados de serviços executados de forma concomitante, pois essa situação se equivale, para fins de comprovação de capacidade técnico-operacional, a uma única contratação, nos termos do item 10.9 do Anexo VII-A da IN SEGES/MPDG nº 5/2017.

9.11.3. O licitante disponibilizará, caso seja solicitado, todas as informações necessárias à comprovação da legitimidade dos atestados apresentados, apresentando, dentre outros documentos, cópia do contrato que deu suporte à contratação, endereço atual da contratante e local em que foram prestados os serviços, consoante o disposto no item 10.10 do Anexo VII-A da IN SEGES/MPDG nº 5/2017.

9.11.4. A recusa do emitente do atestado em prestar esclarecimentos, informações, fornecer documentos comprobatórios, etc., desconstituirá o atestado de capacidade técnica e poderá configurar prática de falsidade ideológica, ensejando comunicação ao Ministério Público Federal e abertura de Processo Administrativo Disciplinar, para fins de apuração de responsabilidade.

9.11.4.1. Os atestados deverão ser apresentados em papel timbrado do emitente, conter identificação do signatário, nome, endereço, telefone e, se for o caso, correio eletrônico para contato, a fim de possibilitar possíveis diligências.

9.11.4.2. Encontrada divergência entre o especificado nos atestados e o apurado em eventual diligência, além da desclassificação no processo licitatório, fica sujeita a licitante às penalidades cabíveis.

SERVIÇO PÚBLICO FEDERAL

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP

9.12. O licitante enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar nº 123, de 2006, estará dispensado **(a)** da prova de inscrição nos cadastros de contribuintes estadual e municipal e **(b)** da apresentação do balanço patrimonial e das demonstrações contábeis do último exercício.

9.13. A existência de restrição relativamente à regularidade fiscal e trabalhista não impede que o licitante qualificado como microempresa ou empresa de pequeno porte seja declarado vencedor, uma vez que atenda a todas as demais exigências do Edital.

9.13.1. A declaração do vencedor acontecerá no momento imediatamente posterior à fase de habilitação.

9.14. Caso a proposta mais vantajosa seja ofertada por licitante qualificado como microempresa, ou empresa de pequeno porte, e uma vez constatada a existência de alguma restrição no que tange à regularidade fiscal e trabalhista, a mesma será convocada para, no prazo de 05 (cinco) dias úteis, após a declaração do vencedor, comprovar a regularização. O prazo poderá ser prorrogado por igual período, a critério da administração pública, quando requerida pelo licitante, mediante apresentação de justificativa.

9.15. A não regularização fiscal e trabalhista no prazo previsto no subitem anterior acarretará a inabilitação do licitante, sem prejuízo das sanções previstas neste Edital, sendo facultada a convocação dos licitantes remanescentes, na ordem de classificação. Se, na ordem de classificação, seguir-se outra microempresa, empresa de pequeno porte ou sociedade cooperativa com alguma restrição na documentação fiscal e trabalhista, será concedido o mesmo prazo para regularização.

9.16. Havendo necessidade de analisar minuciosamente os documentos exigidos, o Pregoeiro suspenderá a sessão, informando no “chat” a nova data e horário para a continuidade da mesma.

9.17. Será inabilitado o licitante que não comprovar sua habilitação, seja por não apresentar quaisquer dos documentos exigidos, ou apresentá-los em desacordo com o estabelecido neste Edital.

9.18. Nos itens não exclusivos a microempresas e empresas de pequeno porte, em havendo inabilitação, haverá nova verificação, pelo sistema, da eventual ocorrência do empate ficto, previsto nos artigos 44 e 45 da LC nº 123, de 2006, seguindo-se a disciplina antes estabelecida para aceitação da proposta subsequente.

9.19. Constatado o atendimento às exigências de habilitação fixadas no Edital, o licitante será declarado vencedor.

10. DO ENCAMINHAMENTO DA PROPOSTA VENCEDORA

10.1. A proposta final do licitante declarado vencedor deverá ser encaminhada no prazo de 02 (duas) horas, a contar da solicitação do Pregoeiro no sistema eletrônico e deverá:

10.1.1. Ser redigida em língua portuguesa, sem emendas, rasuras, entrelinhas ou ressalvas, devendo a última folha ser assinada e as demais rubricadas pelo licitante ou seu representante legal.

10.1.1. Apresentar a proposta de preços, devidamente ajustada ao lance vencedor, em conformidade com o modelo anexo a este instrumento convocatório.

10.2. A proposta final deverá ser documentada nos autos e será levada em consideração no decorrer da execução do contrato e aplicação de eventual sanção à Contratada, se for o caso.

10.2.1. Todas as especificações do objeto contidas na proposta,tais como marca, modelo, tipo, fabricante e procedência, vinculam a Contratada.

10.3. Os preços deverão ser expressos em moeda corrente nacional, o valor unitário em algarismos e o valor global em algarismos e por extenso (art. 5º da Lei nº 8.666/93).

10.3.1. Ocorrendo divergência entre os preços unitários e o preço global, prevalecerão os primeiros; no caso de divergência entre os valores numéricos e os valores expressos por extenso, prevalecerão estes últimos.

10.4. A oferta deverá ser firme e precisa, limitada, rigorosamente, ao objeto deste Edital, sem conter alternativas de preço ou de qualquer outra condição que induza o julgamento a mais de um resultado, sob pena de desclassificação.

10.5. A proposta deverá obedecer aos termos deste Edital e seus anexos, não sendo considerada aquela que não corresponda às especificações ali contidas ou que estabeleça vínculo à proposta de outro licitante.

10.6. As propostas que contenham a descrição do objeto, o valor e os documentos complementares estarão disponíveis na *internet*, após a homologação.

SERVIÇO PÚBLICO FEDERAL

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP

11. DOS RECURSOS

11.1. Declarado o vencedor e decorrida a fase de regularização fiscal e trabalhista do licitante qualificado como microempresa ou empresa de pequeno porte, se for o caso, será concedido o prazo de no mínimo 30 (trinta) minutos, para que qualquer licitante manifeste a intenção de recorrer, de forma motivada, isto é, indicando contra qual(is) decisão(ões) pretende recorrer e por quais motivos, em campo próprio do sistema.

11.2. Havendo quem se manifeste, caberá ao Pregoeiro verificar a tempestividade e a existência de motivação da intenção de recorrer, para decidir se admite ou não o recurso, fundamentadamente.

11.2.1. Nesse momento o Pregoeiro não adentrará no mérito recursal, mas apenas verificará as condições de admissibilidade do recurso.

11.2.2. A ausência de manifestação motivada do licitante quanto à intenção de recorrer, nos termos do disposto no item “11.1”, importará na decadência desse direito, e o Pregoeiro estará autorizado a adjudicar o objeto ao licitante declarado vencedor.

11.2.3. Uma vez admitido o recurso, o recorrente terá, a partir de então, o prazo de 03 (três) dias para apresentar as razões, pelo sistema eletrônico, ficando os demais licitantes, desde logo, intimados para, querendo, apresentarem contrarrazões também pelo sistema eletrônico, em outros 03 (três) dias, que começarão a contar do término do prazo do recorrente, sendo-lhes assegurada vista imediata dos elementos indispensáveis à defesa de seus interesses.

11.2.4. O recurso será dirigido à autoridade superior, por intermédio da que praticou o ato recorrido, a qual poderá reconsiderar sua decisão, no prazo de 05 (cinco) dias úteis, ou no mesmo prazo fazê-lo subir, devidamente informados para decisão.

11.3. O acolhimento do recurso invalida tão somente os atos insuscetíveis de aproveitamento.

11.4. Os autos do processo permanecerão com vista franqueada aos interessados, no endereço constante neste Edital.

12. DA REABERTURA DA SESSÃO PÚBLICA

12.1. A sessão pública poderá ser reaberta:

12.1.1. Nas hipóteses de provimento de recurso que leve à anulação de atos anteriores à realização da sessão pública precedente ou em que seja anulada a própria sessão pública, situação em que serão repetidos os atos anulados e os que dele dependam.

12.1.2. Quando houver erro na aceitação do preço melhor classificado ou quando o licitante declarado vencedor não assinar o contrato, não retirar o instrumento equivalente ou não comprovar a regularização fiscal e trabalhista, nos termos do art. 43, §1º da LC nº 123/2006, serão adotados os procedimentos imediatamente posteriores ao encerramento da etapa de lances.

12.2. Todos os licitantes remanescentes deverão ser convocados para acompanhar a sessão reaberta.

12.2.1. A convocação se dará por meio do sistema eletrônico (“chat”), *e-mail*, de acordo com a fase do procedimento licitatório.

12.2.2. A convocação feita por *e-mail* dar-se-á de acordo com os dados contidos no SICAF, sendo responsabilidade do licitante manter seus dados cadastrais atualizados.

13. DA ADJUDICAÇÃO E HOMOLOGAÇÃO

13.1. O objeto da licitação será adjudicado ao licitante declarado vencedor, por ato do Pregoeiro, caso não haja interposição de recurso, ou pela autoridade competente, após a regular decisão dos recursos apresentados.

13.2. Após a fase recursal, constatada a regularidade dos atos praticados, a autoridade competente homologará o procedimento licitatório.

14. DA GARANTIA DE EXECUÇÃO

14.1. Não será exigida a prestação de garantia de execução para celebrar a contratação decorrente deste certame licitatório, conforme estabelecido no item “14.2.5” do Termo de Referência – Anexo I, deste Edital.

15. DO TERMO DE CONTRATO OU INSTRUMENTO EQUIVALENTE

15.1. Após a homologação da licitação, em sendo realizada a contratação, será firmado Termo de Contrato, ou emitido instrumento equivalente.

15.2. O adjudicatário terá o prazo de 05 (cinco) dias úteis, contados a partir da data de sua convocação, para assinar o Termo de Contrato ou aceitar instrumento equivalente, conforme o caso

SERVIÇO PÚBLICO FEDERAL

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP

(Nota de Empenho/Carta Contrato/Autorização),sob pena de decair do direito à contratação, sem prejuízo das sanções previstas neste Edital.

15.2.1. Alternativamente à convocação para comparecer perante o CREA-SP para a assinatura do Termo de Contrato, o CREA-SP poderá encaminhá-lo para assinatura, mediante correspondência postal com aviso de recebimento (AR) ou meio eletrônico, para que seja assinado e devolvido no prazo de 05 (cinco) dias, a contar da data de seu recebimento.

15.2.2. O prazo previsto no subitem anterior poderá ser prorrogado, por igual período, por solicitação justificada do adjudicatário e aceita pelo CREA-SP.

15.3. O Aceite da Nota de Empenho ou do instrumento equivalente, emitida à empresa adjudicada, implica no reconhecimento de que:

15.3.1. Referida Nota está substituindo o contrato, aplicando-se à relação de negócios ali estabelecida as disposições da Lei nº 8.666, de 1993;

15.3.2. A Contratada se vincula à sua proposta e às previsões contidas no Edital e seus anexos;

15.3.3. A Contratada reconhece que as hipóteses de rescisão são aquelas previstas nos artigos 77 e 78 da Lei nº 8.666/93 e reconhece os direitos da Administração previstos nos artigos 79 e 80 da mesma Lei.

15.4. O prazo de vigência da contratação é de 36 (trinta e seis) meses, podendo ser prorrogado até o limite de 48 (quarenta e oito) meses, na forma da Lei nº 8.666/93.

15.5. Previamente à contratação o CREA-SP realizará consulta ao SICAF para identificar possível suspensão temporária de participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas, observado o disposto no art. 29, da Instrução Normativa nº 3, de 26 de abril de 2018, e nos casos do art. 6º, III, da Lei nº 10.522, de 19 de julho de 2002, consulta prévia ao CADIN.

15.5.1. Nos casos em que houver necessidade de assinatura do instrumento de contrato, e o fornecedor não estiver inscrito no SICAF, este deverá proceder ao seu cadastramento, sem ônus, antes da contratação.

15.5.2. Na hipótese de irregularidade do registro no SICAF, o contratado deverá regularizar a sua situação perante o cadastro no prazo de até 05 (cinco) dias úteis, sob pena de aplicação das penalidades previstas no Edital e anexos.

15.6. Na assinatura do contrato, será exigida a comprovação das condições de habilitação consignadas no Edital, que deverão ser mantidas pelo licitante durante a vigência do contrato.

15.7. **Deverá ainda, apresentar obrigatoriamente, na assinatura do contrato, cópia autenticada de declaração feita pela KASPERSKY, declarando que a empresa é revenda autorizada a fornecer o produto adquirido através do certame.**

15.8. Na hipótese de o vencedor da licitação não comprovar as condições de habilitação consignadas no Edital ou se recusar a assinar o contrato, a Administração, sem prejuízo da aplicação das sanções das demais cominações legais cabíveis a esse licitante, poderá convocar outro licitante, respeitada a ordem de classificação, para, após a comprovação dos requisitos para habilitação, analisada a proposta e eventuais documentos complementares e, feita a negociação, assinar o contrato.

16. DA SUBCONTRATAÇÃO

16.1. Não será permitida a subcontratação, no todo ou em parte, do objeto, conforme estabelecido no item “14.2.2” do Termo de Referência - Anexo I, deste Edital.

17. DO REAJUSTAMENTO EM SENTIDO GERAL

17.1. As regras acerca do reajustamento em sentido geral do valor contratual são as estabelecidas no item “9.1.4” do Termo de Referência – Anexo I, deste Edital.

18. DO MODELO DE EXECUÇÃO DO CONTRATO E DO PROCEDIMENTO DE FISCALIZAÇÃO DA EXECUÇÃO CONTRATUAL

18.1. O modelo de execução do contrato e do critérios do procedimento de fiscalização da execução contratua estão estabelecidos nos itens “9” e “10” do Termo de Referência – Anexo I, deste Edital.

19. DAS OBRIGAÇÕES E RESPONSABILIDADES DO CONTRATANTE

19.1. As obrigações e responsabilidades do Contratante são as estabelecidas no item "7" do Termo de Referência – Anexo I, deste Edital.

20. DAS OBRIGAÇÕES E RESPONSABILIDADES DA CONTRATADA

20.1. As obrigações e responsabilidades da Contratada são as estabelecidas no item "8" do Termo de Referência – Anexo I, deste Edital.

21. FORMA DO PAGAMENTO EM FUNÇÃO DOS RESULTADOS

21.1. As regras acerca do pagamento são as estabelecidas no item "9.4" - (forma de pagamento em função dos resultados), do Termo de Referência – Anexo I, deste Edital.

22. DAS SANÇÕES ADMINISTRATIVAS

22.1. Comete infração administrativa, nos termos da Lei nº 10.520, de 2002, o licitante/adjudicatário que:

22.1.1. Não assinar o termo de contrato, quando convocado dentro do prazo de validade da proposta;

22.1.2. Apresentar documentação falsa;

22.1.3. Deixar de entregar os documentos exigidos no certame;

22.1.4. Ensejar o retardamento da execução do objeto;

22.1.5. Não mantiver a proposta;

22.1.6. Cometer fraude fiscal;

22.1.7. Comportar-se de modo inidôneo;

22.2. Considera-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de participação, quanto ao enquadramento como ME/EPP ou o conluio entre os licitantes, em qualquer momento da licitação, mesmo após o encerramento da fase de lances.

22.3. O licitante/adjudicatário que cometer qualquer das infrações discriminadas nos subitens anteriores ficará sujeito, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

22.3.1. **Advertência por faltas leves**, assim entendidas como aquelas que não acarretarem prejuízos significativos ao objeto da contratação;

22.3.2. **Multa** de 10% (dez por cento) sobre o valor estimado do item prejudicado pela conduta do licitante;

22.3.3. **Suspensão de licitar** e impedimento de contratar com o órgão, entidade ou unidade administrativa pela qual a Administração Pública opera e atua concretamente, pelo prazo de até 02 (dois) anos;

22.3.4. **Impedimento de licitar** e de contratar com a União e descredenciamento no SICAF, pelo prazo de até 05 (cinco) anos;

22.3.4.1. A Sanção de impedimento de licitar e contratar prevista neste subitem também é aplicável em quaisquer das hipóteses previstas como infração administrativa no subitem "22.1" deste Edital;

22.4. A penalidade de multa pode ser aplicada cumulativamente com as demais sanções.

22.5. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa ao licitante/adjudicatário, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente na Lei nº 9.784, de 1999.

22.6. A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

22.7. As penalidades serão obrigatoriamente registradas no SICAF.

22.8. As sanções por atos praticados no decorrer da contratação estão previstas na Cláusula Décima Quinta da Minuta do Termo de Contrato – Anexo III, deste Edital.

23. DA VIGÊNCIA DA CONTRATAÇÃO

23.1. Será firmado contrato com cláusula de vigência de 36 (trinta e seis) meses, a contar da data de assinatura do Contrato, podendo ser prorrogado até o limite de 48 (quarenta e oito) meses, na forma da Lei nº 8.666/93, e suas atualizações.

23.2. O contrato poderá ser rescindindo nos termos e hipóteses dos arts. 77 a 80 da Lei nº 8.666/93, e suas atualizações.

SERVIÇO PÚBLICO FEDERAL

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP

24. DA IMPUGNAÇÃO AO EDITAL

24.1. Qualquer pessoa poderá impugnar os termos do Edital do pregão, por meio eletrônico, na forma prevista no Edital, até 03 (três) dias úteis anteriores à data fixada para abertura da sessão pública, conforme Decreto n° 10.024/2019.

24.2. A impugnação não possui efeito suspensivo e caberá ao Pregoeiro, auxiliado pelos responsáveis pela elaboração do Edital e dos anexos, decidir sobre a impugnação no prazo de 02 (dois) dias úteis, contado da data de recebimento da impugnação.

24.3. Acolhida a impugnação contra o Edital, será definida e publicada nova data para a realização do certame.

24.4. A impugnação poderá ser realizada por forma eletrônica, pelo *e-mail* compras.licitacao@creasp.org.br, ou, por petição dirigida ou protocolada no seguinte endereço: Avenida Brigadeiro Faria Lima, 1059 – 8º andar – Pinheiros – São Paulo, SP – CEP – 01452-920, na Unidade de Licitações – UL, nos dias úteis, no horário das 8h30min às 16h30min.

25. DOS PEDIDOS DE ESCLARECIMENTOS

25.1. Os pedidos de esclarecimentos referentes ao processo licitatório deverão ser enviados ao Pregoeiro, até 03 (três) dias úteis anteriores à data fixada para abertura da sessão pública, por meio eletrônico, pelo *e-mail* compras.licitacao@creasp.org.br.

25.1.1. O Pregoeiro responderá aos pedidos de esclarecimentos no prazo de 02 (dois) dias úteis, contados da data de recebimento do pedido, podendo requisitar subsídios formais aos responsáveis pela elaboração do Edital e dos anexos.

25.1.2. As respostas aos pedidos de esclarecimentos prestados pelo Pregoeiro serão entranhados nos autos do processo licitatório e estarão disponíveis para consulta por qualquer interessado, bem como serão disponibilizadas nos seguintes sistemas eletrônicos www.comprasgovernamentais.gov.br e www.creasp.org.br – Link Licitação e, vincularão os participantes e o CREA-SP.

26. DAS DISPOSIÇÕES GERAIS

26.1. Da sessão pública do Pregão divulgar-se-á Ata no sistema eletrônico.

SERVIÇO PÚBLICO FEDERAL

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP

26.2. Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a realização do certame na data marcada, a sessão será automaticamente transferida para o primeiro dia útil subsequente, no mesmo horário anteriormente estabelecido, desde que não haja comunicação em contrário, pelo Pregoeiro.

26.3. Todas as referências de tempo no Edital, no aviso e durante a sessão pública observarão o horário de Brasília – DF.

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

26.5. A homologação do resultado desta licitação não implicará direito à contratação.

26.6. As normas disciplinadoras da licitação serão sempre interpretadas em favor da ampliação da disputa entre os interessados, desde que não comprometam o interesse da Administração, o princípio da isonomia, a finalidade e a segurança da contratação.

26.7. Os licitantes assumem todos os custos de preparação e apresentação de suas propostas e a Administração não será, em nenhum caso, responsável por esses custos, independentemente da condução ou do resultado do processo licitatório.

26.8. Na contagem dos prazos estabelecidos neste Edital e seus anexos, excluir-se-á o dia do início e incluir-se-á o do vencimento. Só se iniciam e vencem os prazos em dias de expediente na Administração.

26.9. O desatendimento de exigências formais não essenciais não importará o afastamento do licitante, desde que seja possível o aproveitamento do ato, observados os princípios da isonomia e do interesse público.

26.10. Em caso de divergência entre disposições deste Edital e de seus anexos ou demais peças que compõem o processo, prevalecerá as deste Edital.

26.11. O Edital está disponibilizado, na íntegra, no endereço eletrônico: www.comprasgovernamentais.gov.br e www.creasp.org.br no link Licitação, e também poderão ser lidos e/ou obtidos no endereço Avenida Brigadeiro Faria Lima, 1059 – 8° andar, Pinheiros, São Paulo, SP – CEP – 01452-920, nos dias úteis de segunda a sexta-feira, no horário das 8h30min às 16h30min,

mesmo endereço e período no qual os autos do processo administrativo permanecerão com vista franqueada aos interessados.

26.12. Integram este Edital, para todos os fins e efeitos, os seguintes anexos:

26.12.1. ANEXO I - Termo de Referência;

26.12.1.1. ANEXO A - Características e funcionalidades mínimas do Software Antivírus.

26.12.2. ANEXO II – Modelo de Proposta de Preços;

26.12.3. ANEXO III - Minuta do Termo de Contrato.

São Paulo, 16 de agosto de 2021.

Alessandro Baumgartner
Superintendente Administrativo Financeiro
Portaria nº 46/2021

SERVIÇO PÚBLICO FEDERAL

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP

ANEXO I

TERMO DE REFERÊNCIA

SERVIÇO PÚBLICO FEDERAL

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP

ANEXO A

CARACTERÍSTICAS E FUNCIONALIDADES MÍNIMAS DO SOFTWARE ANTIVÍRUS

SERVIÇO PÚBLICO FEDERAL

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP

ANEXO II

MODELO DE PROPOSTA DE PREÇOS

Ao CREA-SP
Pregão Eletrônico nº 010/2021
Processo Administrativo nº 0066/2021

A empresa _____, sediada à Av. / Rua _____, Cidade, Bairro e CEP, inscrita no CNPJ/MF sob o nº _____, Inscrição Municipal _____ Inscrição Estadual _____, vem através desta apresentar proposta de preço, conforme solicitado. CONTATO: nome _____ Telefone: ( ) _____ e-mail ____.

GRUPO 1 – ÚNICO

Item	Código	Descrição	Quant.	Unidade	Valor Unitário	Valor Total
1	KL4867KAVFR	Licenças de Antivirus denominadas pelo fabricante de: "Kaspersky Endpoint Security for Business - Advanced Renewal 3 year Band V: 1000-1499"	1369	Licenças	R$	R$
2	KL 002.11.6	Capacitação de implantação, configuração e gerenciamento da solução.	4	Pessoas	R$	R$
3	KL 009.12	Capacitação em gerenciamento de vulnerabilidades a atualizações de software e integração com o sistema SIEM	4	Pessoas	R$	R$
4	N.A.	Suporte 8x5, monitoramento, atualização do servidor e clientes.	36	Meses	R$	R$
VALOR TOTAL GERAL DO GRUPO 1 – ÚNICO……						R$

Deverá constar na proposta comercial:

1) Validade da Proposta: não inferior a 60 (sessenta) dias a contar da data de abertura do certame;

2) **Dados bancários para pagamento:** Banco; número da conta; agência;

3) **Para fins de assinatura contrato, informar:**

3.1) Razão Social;

3.2) CNPJ, Inscrição Estadual e Municipal;

3.3) Endereço completo da empresa, inclusive CEP;

3.4) Telefone e *e-mail* do responsável (preposto);

3.5) Nome, número do CPF, número do RG e cargo do Representante Legal da empresa com poderes para assinatura do contrato;

SERVIÇO PÚBLICO FEDERAL

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP

3.6) Nome, número do CPF, número do RG do responsável (preposto), que deverá ser mantido, aceito pelo CREA-SP, para representa-la na execução do contrato.

4 Custos contemplados na Proposta: nos preços apresentados acima já estão computados todos os custos necessários decorrentes da prestação dos serviços, bem como já incluídos todos os impostos, encargos trabalhistas, previdenciários, fiscais, comerciais, taxas, seguros, deslocamentos de pessoal e quaisquer outros que incidam direta ou indiretamente.

5 Nos valores indicados estão considerado as condições, quantidades, exigências e demais especificações estabelecidas no Termo de Referência – Anexo I do Edital.

6 Declaramos, para todos os fins e efeitos legais, aceitar, irrestritamente, todas as condições e exigências estabelecidas no Edital da licitação em referência, nos seus anexos, e no Contrato a ser celebrado, cuja minuta constitui anexo do Edital.

7 Declaramos, ainda, que inexiste qualquer vínculo de natureza técnica, comercial, econômica, financeira ou trabalhista com serviço ou dirigente do CREA-SP.

(Local) ....., de 2021.

Nome e Assinatura do Representante Legal
Cargo/Função
Carimbo do CNPJ
(Apresentar em papel timbrado do licitante)

SERVIÇO PÚBLICO FEDERAL

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP

ANEXO III
MINUTA DO TERMO DE CONTRATO

Contrato nº /2021
Processo Administrativo nº 0066/2021

TERMO DE CONTRATO DE EMPRESA ESPECIALIZADA PARA FORNECIMENTO DE SERVIÇOS DE ATUALIZAÇÃO DAS LICENÇAS PARA O ANTIVIRUS KASPERSKY, COM SUPORTE E CAPACITAÇÃO.

O **CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA DO ESTADO DE SÃO PAULO**, instituído pelo Decreto Federal nº 23.569, de 11 de dezembro de 1933 e mantido pela Lei Federal nº 5.194, de 24 de dezembro de 1966, com sede e foro na Avenida Brigadeiro Faria Lima nº 1.059, nesta Capital, inscrito no CNPJ sob nº 60.985.017/0001-77, neste ato representado por seu Presidente, o Engenheiro **VINICIUS MARCHESE MARINELLI**, brasileiro, portador da cédula de identidade RG nº 34.123.915-X – SSP/SP e inscrito no CPF/MF nº 304.423.178-75, registrado no **CREA-SP** sob nº **5062051089**, doravante denominado simplesmente **CREA-SP**, e de outro lado a Empresa _____, com sede na _____, ____ – _____ – _____/____ - CEP: _____, inscrita no CNPJ sob o nº _____, Inscrição Estadual _____, CCM nº _____, neste ato representado por seu _____, _____, portador da Cédula de Identidade RG. nº _____ e CPF sob nº _____, doravante denominada simplesmente **CONTRATADA**, resolvem de comum acordo firmar o presente Contrato, conforme Edital de Pregão Eletrônico nº 010/2021 e respeitável despacho de fls. ____, nos termos da Lei nº 10.520, de 17/07/2002, do Decreto nº 3.555 de 8/08/2000, Decreto n° 10.024, de 20/09/2019, e, subsidiariamente, a Lei nº 8.666, de 21/06/1993, e suas atualizações, contidos nos autos do Processo Administrativo nº 0066/2021, e regido pelas seguintes cláusulas e condições:

CLÁUSULA PRIMEIRA – DO OBJETO

1.1. O presente instrumento tem como objeto a contratação de empresa especializada para fornecimento de serviços de atualização das licenças para o Antivirus Kaspersky, com suporte e capacitação, por 36 (trinta e seis) meses, a fim de atender as necessidades do CREA-SP, conforme condições, quantidades e exigências estabelecidas no Edital de Pregão Eletrônico nº 010/2021 e seus anexos, que passa a fazer parte integrante deste contrato como se nele estivesse transcrito.

1.2. Este Termo de Contrato vincula-se ao Edital do Pregão, identificado no preâmbulo e à proposta vencedora, independentemente de transcrição.

SERVIÇO PÚBLICO FEDERAL

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP

2. CLÁUSULA SEGUNDA – DO PREÇO

2.1. O valor deste Termo de Contrato é de R$ _____ (_____)**.**

2.1.1. Descrição, quantitativos e preços:

Item	Código	Descrição	Quant.	Unidade	Valor Unitário	Valor Total
1	KL4867KAVFR	Licenças de Antivirus denominadas pelo fabricante de: "Kaspersky Endpoint Security for Business - Advanced Renewal 3 year Band V: 1000-1499"	1369	Licenças	R$	R$
2	KL 002.11.6	Capacitação de implantação, configuração e gerenciamento da solução.	4	Pessoas	R$	R$
3	KL 009.12	Capacitação em gerenciamento de vulnerabilidades a atualizações de software e integração com o sistema SIEM	4	Pessoas	R$	R$
4	N.A.	Suporte 8x5, monitoramento, atualização do servidor e clientes.	36	Meses	R$	R$
VALOR TOTAL GERAL DO GRUPO 1 – ÚNICO……						R$

2.1.2. No valor acima estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução do objeto, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação.

CLÁUSULA TERCEIRA – DA VIGÊNCIA

3.1. Será firmado contrato com cláusula de vigência de 36 (trinta e seis) meses, a contar da data de assinatura do Contrato, podendo ser prorrogado até o limite de 48 (quarenta e oito) meses, na forma da Lei nº 8.666/93, e suas atualizações.

3.2. O contrato poderá ser rescindido nos termos e hipóteses dos artigos 77 a 80 da Lei nº 8.666/93 e suas atualizações.

CLÁUSULA QUARTA – DA DOTAÇÃO ORÇAMENTÁRIA

4.1. A despesa para atender a esta licitação está programada em dotação orçamentária própria da Equipe de Sustentação, Suporte e Infraestrutura de TIC – ESSITIC da Gerência de Desenvolvimento e Execução de Projetos - GDEP, prevista no orçamento do CREA-SP no exercício de financeiro de 2021, oriundo da conta nº 6.2.2.1.1.01.04.09.005 – Serviços de Informática – PJ.

SERVIÇO PÚBLICO FEDERAL

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP

4.2. A despesa com a execução dos serviços de que trata o objeto desta licitação é estimada no período de 36 (trinta e seis) meses.

CLÁUSULA QUINTA – FORMA DO PAGAMENTO EM FUNÇÃO DOS RESULTADOS

5.1. As regras acerca do pagamento são as estabelecidas no item "9.4" – (forma de pagamento em função dos resultados), do Termo de Referência – Anexo I, do Edital.

CLÁUSULA SEXTA – DA DESCRIÇÃO DA SOLUÇÃO E DA ESTIMATIVA DAS QUANTIDADES

6.1. A composição da solução e a estimativa das quantidades de licenças estão previstas nos itens "3" e "4" do Termo de Referência – Anexo I, do Edital.

CLÁUSULA SÉTIMA – DAS ESPECIFICAÇÃO TÉCNICA

7.1. DESCRIÇÃO DA SOLUÇÃO

7.1.1. A descrição da solução estão estabelecidas no item "6" do Termo de Referência – Anexo I, do Edital.

CLÁUSULA OITAVA – DO MODELO DE EXECUÇÃO DO CONTRATO – ROTINAS DE EXECUÇÃO

8.1. As rotinas de execução do contrato são as elencadas no item "9" do Termo de Referência – Anexo I, do Edital.

CLÁUSULA NONA – DO PROCEDIMENTO DE FISCALIZAÇÃO DA EXECUÇÃO CONTRATUAL

9.1. O procedimento de fiscalização da execução contratual estão estabelecidos no item "10" do Termo de Referência – Anexo I, do Edital.

CLÁUSULA DÉCIMA – DO LOCAL DE ENTREGA

10.1. A definição do local de entrega está descrito no item "13" do Termo de Referência – Anexo I, do Edital.

CLÁUSULA DÉCIMA PRIMEIRA – DA PRORROGAÇÃO E FORMA DE REAJUSTAMENTO DO VALOR CONTRATUAL

11.1. A prorrogação contratual somente será concretizada quando:

11.1.1. Ficar caracterizado, mediante pesquisa a ser realizada pelo CREA-SP, que os preços a serem praticados na prorrogação contratual serão condizentes aos praticados no mercado, e

11.1.2. Houver comunicação formal do CREA-SP à Contratada, com no mínimo 30 (trinta) dias anteriores ao do vencimento do Contrato.

11.2. Para cada prorrogação contratual, serão reajustadas pelo índice IPC-FIPE.

11.3. A data base de pedido de reajuste será da apresentação da proposta comercial, ou seja, da sessão de abertura do presente certame.

11.4. O reajuste incidirá apenas sobre os serviços não executados, não incidirá sobre os serviços em atrasos.

11.5. Caso o índice estabelecido para reajustamento venha a ser extinto ou de qualquer forma não possa mais ser utilizado, será adotado, em substituição, o que vier a ser determinado pela legislação então em vigor.

11.6. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.

CLÁUSULA DÉCIMA SEGUNDA – DA GARANTIA DE EXECUÇÃO

12.1. Não será exigida a prestação de garantia de execução para celebrar a contratação decorrente deste certame licitatório, conforme estabelecido no item “14.2.5” do Termo de Referência – Anexo I, do Edital.

CLÁUSULA DÉCIMA TERCEIRA – DAS OBRIGAÇÕES E RESPONSABILIDADES DA CONTRATANTE

13.1. As obrigações e responsabilidades da Contratante são as estabelecidas no item “7” do Termo de Referência – Anexo I, do Edital.

CLÁUSULA DÉCIMA QUARTA – DAS OBRIGAÇÕES E RESPONSABILIDADES DA CONTRATADA

14.1. As obrigações e responsabilidades da Contratada são as estabelecidas no item “8” do Termo de Referência – Anexo I, do Edital.

SERVIÇO PÚBLICO FEDERAL

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP

CLÁUSULA DÉCIMA QUINTA – DAS SANÇÕES ADMINISTRATIVAS

15.1. Comete infração administrativa nos termos da Lei nº 8.666, de 1993 e da Lei nº 10.520, de 2002, a Contratada que:

a) Não assinar o Termo de Contrato, quando convocado dentro do prazo de validade da proposta de preços;

b) Apresentar documentação falsa;

c) Deixar de executar total ou parcialmente qualquer das obrigações assumidas em decorrência da contratação;

d) Ensejar o retardamento da execução do objeto;

e) Falhar ou fraudar na execução do contrato;

f) Comportar-se de modo inidôneo; ou

g) Cometer fraude fiscal;

15.2. Considerar-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de participação, e/ou o conluio entre licitantes, em qualquer momento da licitação, mesmo após o encerramento da fase de lances.

15.3. A contratada que cometer qualquer das infrações discriminadas no subitem acima ficará sujeita, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

15.3.1. **Advertência por faltas leves** , assim entendidas aquelas que não acarretem prejuízos significativos para a Contratante;

15.3.2. **Multa Moratória** de 1% (um por cento) **por dia** de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 10 (dez) dias;

15.3.3. **Multa Compensatória** de 20% (vinte por cento) sobre o valor total da contratação, no caso de inexecução total do objeto.

15.3.3.1. Em caso de inexecução parcial, a multa compensatória, no mesmo percentual do subitem acima, será aplicada de forma proporcional à obrigação inadimplida.

SERVIÇO PÚBLICO FEDERAL

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP

15.3.4. **Suspensão de licitar** e impedimento de contratar com o órgão, entidade ou unidade administrativa pela qual a Administração Pública opera e atua concretamente, pelo prazo de até dois anos;

15.3.5. **Impedimento de licitar e contratar** com órgãos e entidades da União, com o consequente descredenciamento no SICAF pelo prazo de até cinco anos.

15.3.6. A Sanção de impedimento de licitar e contratar prevista neste subitem também é aplicável em quaisquer das hipóteses previstas como infração administrativa no subitem "15.1" deste instrumento.

15.4. As sanções previstas nos subitens "15.3.1", "15.3.4" e "15.3.5" poderão ser aplicadas à contratada juntamente com as de multa, descontando-a dos pagamentos a serem efetuados.

15.5. Também ficam sujeitas às penalidades do art. 87, III e IV da Lei nº 8.666, de 1993, as empresas ou profissionais que:

a) Tenham sofrido condenação definitiva por praticar, por meio dolosos, fraude fiscal no recolhimento de quaisquer tributos;

b) Tenham praticado atos ilícitos visando a frustrar os objetivos da licitação;

c) Demonstrem não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.

15.6. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa à Contratada, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente a Lei nº 9.784, de 1999.

15.7. A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

15.8. As penalidades serão obrigatoriamente registradas no SICAF.

SERVIÇO PÚBLICO FEDERAL

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP

CLÁUSULA DÉCIMA SEXTA – DA ALTERAÇÃO SUBJETIVA

16.1. É admissível a fusão, cisão ou incorporação da Contratada com/por 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.

CLÁUSULA DÉCIMA SÉTIMA – DA SUBCONTRATAÇÃO

17.1. Não será permitida a subcontratação, no todo ou em parte, do objeto, conforme estabelecido no item "14.2.2" do Termo de Referência – Anexo I, do Edital.

CLÁUSULA DÉCIMA OITAVA – DAS ALTERAÇÕES, ACRÉSCIMOS OU SUPRESSÕES

18.1. Eventuais alterações contratuais reger-se-ão pela disciplina do art. 65 da Lei nº 8.666, de 1993.

18.1.1. A Contratada é obrigada a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

18.2. As supressões resultantes de acordo celebrado entre as partes contratantes poderão exceder o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

CLÁUSULA DÉCIMA NONA - DA RESCISÃO

19.1. O presente Termo de Contrato poderá ser rescindido:

19.1.1. Por ato unilateral e escrito da Administração, nas situações previstas nos incisos I a XII e XVII do art. 78 da Lei nº 8.666, de 1993, e com as consequências indicadas no art. 80 da mesma Lei, sem prejuízo da aplicação das sanções previstas;

19.1.2. Amigavelmente, nos termos do art. 79, inciso II, da Lei nº 8.666, de 1993.

19.2. Os casos de rescisão contratual serão formalmente motivados, assegurando-se à Contratada o direito à prévia e ampla defesa.

19.3. A Contratada reconhece os direitos do CREA-SP em caso de rescisão administrativa prevista no art. 77 da Lei nº 8.666, de 1993.

SERVIÇO PÚBLICO FEDERAL

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP

19.4. O termo de rescisão, sempre que possível, será precedido:

19.4.1. Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;

19.4.2. Relação dos pagamentos já efetuados e ainda devidos;

19.4.3. Indenizações e multas.

CLÁUSULA VIGÉSIMA – DA GESTÃO DO CONTRATO

20.1. A gestão do contrato será acompanhada por Gestor a ser indicado através de Portaria da autoridade competente após a assinatura do Contrato.

20.1.1. Será dada ciência da Portaria ao preposto da Contratada.

20.2. O Gestor do Contrato poderá, quando da emissão da Ordem de Serviço, exigir a entrega de relatório do prestador de serviço/fornecedor, referente à execução do Contrato, indicando nesta ocasião o formato e a periodicidade de entrega.

20.3. Os pagamentos devidos serão sempre condicionados a entrega dos relatórios.

CLÁUSULA VIGÉSIMA PRIMEIRA – DO PREPOSTO DA CONTRATADA

21.1. Fica estabelecido que o preposto da Contratada para representá-la perante o CREA-SP na execução deste Contrato é o(a) Sr.(a). ____, função____, portador da Cédula de Identidade RG nº _____ e CPF/MF nº _____, endereço eletrônico: ____.

CLÁUSULA VIGÉSIMA SEGUNDA – DAS VEDAÇÕES E PERMISSÕES

22.1. É vedado à Contratada interromper a execução dos serviços sob alegação de inadimplemento por parte da Contratante, salvo nos casos previstos em lei.

22.2. É permitido à Contratada caucionar ou utilizar este Termo de Contrato para qualquer operação financeira, nos termos e de acordo com os procedimentos previstos na Instrução Normativa SEGES/ME nº 53, de 8 de julho de 2020.

22.3. A cessão de crédito, a ser feita mediante celebração de termo aditivo, dependerá de comprovação da regularidade fiscal e trabalhista da cessionária, bem como da certificação de que a

cessionária não se encontra impedida de licitar e contratar com o Poder Público, conforme a legislação em vigor, nos termos do Parecer JL-01, de 18 de maio de 2020.

22.4. A crédito a ser pago à cessionária é exatamente aquele que seria destinado à cedente (Contratada) pela execução do objeto contratual, com o desconto de eventuais multas, glosas e prejuízos causados à Administração, sem prejuízo da utilização de institutos tais como os da conta vinculada e do pagamento direto previstos na IN SEGES/ME nº 5, de 2017, caso aplicáveis.

CLÁUSULA VIGÉSIMA TERCEIRA – DA PUBLICAÇÃO

23.1. O CREA-SP providenciará a publicação do extrato deste contrato e de seus eventuais termos aditivos no Diário Oficial da União, a suas expensas, na forma prevista no Parágrafo único do art. 61 da Lei nº 8.666/1993.

CLÁUSULA VIGÉSIMA QUARTA – DAS CONSIDERAÇÕES GERAIS

24.1. É vedada a utilização, na execução do objeto pela Contratada, de empregado que seja familiar de agente público ocupante de cargo em comissão ou função de confiança no CREA-SP, nos termos do art. 7º do Decreto nº 7.203/2010.

24.2. Constituem direitos e prerrogativas do CREA-SP, além dos previstos em outras leis, os constantes da Lei nº 8.666/1993, que a Contratada aceita e a eles se submete.

24.3. A omissão ou tolerância das partes – em exigir o estrito cumprimento das disposições deste Contrato ou em exercer prerrogativa dele decorrente não constituirá novação ou renúncia nem lhes afetará o direito de, a qualquer tempo, exigirem o fiel cumprimento do avençado.

24.4. Fica ressalvada a possibilidade de alteração das condições contratuais, em face da superveniência de normas federais, estaduais ou municipais, bem como em razão da conveniência e oportunidade da Administração, devidamente justificadas.

24.5. A Contratada se compromete a manter durante a execução do presente Contrato, todas as condições de habilitação e qualificação exigidas no Edital do Pregão Eletrônico nº 010/2021.

24.6. Integram o presente Contrato como se nele estivesse transcrito o Edital do Pregão Eletrônico nº 010/2021, seus anexos e a Proposta Comercial de fls. ___ apresentada pela Contratada, anexados no processo administrativo V-0066/2021.

SERVIÇO PÚBLICO FEDERAL

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP

24.7. Este Contrato não autoriza, nem a Contratada tem direito, tampouco poderes e nem deverá comprometer ou vincular a CREA-SP a qualquer acordo, Contrato ou reconhecimento, nem induzir, renunciar ou transigir quaisquer dos direitos do CREA-SP ou, ainda, assumir qualquer obrigação em nome deste, a qual não se responsabilizará por quaisquer reclamações de lucros cessantes ou danos pleiteados por Terceiros em decorrência ou relacionados com a celebração, execução ou rescisão deste Contrato.

24.8. Caso qualquer das cláusulas deste Contrato seja ou se torne legalmente ineficaz, a validade do documento como um todo não deverá ser afetada.

CLÁUSULA VIGÉSIMA QUINTA – DOS CASOS OMISSOS

25.1. Os casos omissos serão decididos pelo CREA-SP, segundo as disposições contidas na Lei nº 8.666, de 1993, na Lei nº 10.520, de 2002 e demais normas federais aplicáveis e, subsidiariamente, segundo as disposições contidas na Lei nº 8.078, de 1990 – Código de Defesa do Consumidor – e normas e princípios gerais dos contratos.

CLÁUSULA VIGÉSIMA SEXTA – DO FORO DE ELEIÇÃO

26.1. As partes, de comum acordo, elegem o Foro da Justiça Federal de São Paulo para dirimir qualquer lide oriunda deste Contrato, com renúncia expressa de qualquer outro, por mais privilegiado que seja.

E, por estarem assim justas e contratadas, assinam as partes este Contrato, em 02 (duas) vias de igual teor e forma, para os mesmos efeitos, na presença de 02 (duas) testemunhas.

São Paulo, de de 2021.

Ao assinar este Contrato as partes declaram ciência de todo seu conteúdo, independente de rubricas em todas as páginas.

Assinam este Contrato, nesta ordem:

Pela CONTRATADA:
TESTEMUNHA:
REPRESENTANTE LEGAL:

Pelo CREA-SP:
TESTEMUNHA:

SERVIÇO PÚBLICO FEDERAL

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP

RERPESENTANTE LEGAL:

SERVIÇO PÚBLICO FEDERAL

CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP

ANEXO ÚNICO

O Termo de Referência Anexo Único do Contrato será juntado quando da lavratura do instrumento contratual.

SERVIÇO PÚBLICO FEDERAL
CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA DO ESTADO DE SÃO PAULO

CREA-SP

TERMO DE REFERÊNCIA

INTRODUÇÃO

A presente análise tem por objetivo descrever os elementos necessários e suficientes, com nível de precisão adequado, para subsidiar o processo licitatório, demonstrando sua viabilidade e conveniência. Seu conteúdo dependerá da natureza da solução a ser licitada, sendo mais complexo e minucioso na medida em que a contratação assim exigir. Ele será elaborado com base nas informações constantes do Estudo Técnico preliminar.

1 - OBJETO DA CONTRATAÇÃO

1.1. Constitui objeto da presente licitação a contratação de empresa especializada em fornecimento de serviços de atualização das licenças para ao Antivírus Kaspersky, com suporte e capacitação.

2 - JUSTIFICATIVA E FUNDAMENTAÇÃO DA CONTRATAÇÃO

2.1. OBJETIVO DA CONTRATAÇÃO

1. Renovação das Licenças para a atualização de assinaturas de vírus e ameaças utilizadas no antivírus que o CREA-SP atualmente possui instalado em seus computadores, bem como fornecer o suporte adequado e a capacitação para operar o sistema.

2.2. DA JUSTIFICATIVA PARA LOTE ÚNICO

1. A opção por lote único está fundamentada na IN 05/2017-SLTI/MPOG, onde admite-se a aquisição por lote único quando, comprovada e justificadamente, for tecnicamente inviável o parcelamento, por haver inter-relação entre os serviços contratados, gerenciamento centralizado ou implicar em vantagem para a Administração, requisitos que serão comprovados adiante.

2. Quando analisado sob os aspectos técnicos, tem-se configurado o inter-relacionamento e a interdependência entre os serviços a serem contratados, uma vez que não é possível estabelecer os limites, por serem extremamente tênues, de onde se iniciam e terminam as repercussões entre um e outro, especialmente por se ter como meta alcançar a maturidade do ambiente como um todo, a alta disponibilidade e a gestão de riscos da contratação e dos negócios.

3. Além disso, o agrupamento dos itens em Grupo Único é imprescindível, pois em se tratando de gestão contratual torna-se inviável que os serviços associados sejam fornecidos por diferentes fornecedores, dado que traz maior custo de gestão e controle deste Órgão.

4. Em se tratando do viés econômico, o parcelamento dos serviços associados do objeto pode impactar diretamente os custos da contratação, considerando que a execução desses serviços por uma única empresa se traduz em diluição do custo administrativo da empresa possibilitando menor preço global.

5. Neste sentido, o objeto possui características de dependências entre os serviços a serem prestados, sendo certo que seu parcelamento aumentaria os riscos de execução insatisfatória do serviço.

6. A aquisição em lote único embasa-se no Parecer no 2086/00, elaborado no Processo no 194/2000 do TCDF, da lavra do Professor Jorge Ulisses Jacoby Fernandes e outros doutrinadores a seguir citados:

> “a regra do parcelamento deve ser coordenada com o requisito que a própria lei definiu: só se pode falar em parcelamento quando há viabilidade técnica para sua adoção. (...) Um exame atento dos tipos de objeto licitados pela Administração Pública evidência que embora sejam divisíveis, há interesse técnico na manutenção unicidade, da licitação ou do item dela. Não é, pois, a simples divisibilidade, mas a viabilidade técnica que dirige processo decisório. (...) Se um objeto, divisível, sob o aspecto econômico for mais vantajoso, mas houver inviabilidade técnica em que seja licitado em separado, de nada valerá a avaliação econômica. Imagine-se ainda esse elementar exemplo do automóvel: se por exemplo as peças isoladamente custassem mais barato, mesmo assim, seria recomendável o não parcelamento, pois sob o aspecto técnico é a visão do conjunto que iria definir a garantia do fabricante, o ajuste das partes compondo todo único, orgânico e harmônico".
>
> “Segundo Marçal Justen Filho, "a obrigatoriedade do fracionamento respeita limites de ordem técnica econômica. Não se admite o fracionamento quando tecnicamente isso não for viável ou, mesmo, recomendável. O fracionamento em lotes deve respeitar a integridade qualitativa do objeto a ser executado. (...) a unidade do objeto a ser executado não pode ser destruída através do fracionamento" (JUSTEN FILHO, Marçal. Comentários à Lei de Licitações e Contratos Administrativos. 11.ed. Brasília: 2005, Dialética.
>
> “Carvalho Carneiro esclarece acerca do conceito de viabilidade técnica e econômica, informando que a viabilidade técnica diz respeito à integridade do objeto, não se admitindo o parcelamento quando tal medida implicar na sua desnaturação, onde em risco a satisfação do interesse público em questão” (CARNEIRO, Daniel Carvalho. O parcelamento da contratação na lei de licitações. Revista Diálogo Jurídico, ano IV, n.3., setembro/2004, p.85/95).

7. Ao se avaliar tecnicamente há uma intensa correlação dos serviços prestados com a disponibilização do licenciamento da solução, a qual necessita-se de profissionais que trabalhem de forma integrada, que entendam do objeto a ser contratado de forma a se ter treinamento, suporte técnico e manutenções evolutivas e adaptativas com qualidade, bem como explorar melhor forma as capacidades da solução para atendimento às necessidades deste CREA-SP.

8. Assim, os itens que compõem a solução devem ser fornecidos em Grupo Único, pelo mesmo licitante ou fornecedor, pois somente assim haverá melhor prestação dos serviços associados, com melhoria da gestão contratual por parte deste CREA-SP.

9. Nesse sentido, a opção deste Órgão respeita a legislação vigente e busca aliar tecnicamente e economicamente os aspectos da gestão contratual.

10. Pode-se inferir que está contratação é técnica e economicamente viável e que haverá diminuição do custo administrativo das empresas participantes por diluição em serviços agregados. Já para este CREA-SP haverá diminuição no custo de gestão contratual ao gerenciar uma empresa, ao invés de várias empresas.

11. Por fim, avalia-se que também haverá melhor aproveitamento do mercado e ampliação da competitividade.

2.3. DA FUNDAMENTAÇÃO LEGAL

1. A presente licitação, que trata da contratação do objeto deste Termo de Referência e seus anexos será realizada conforme regulamentação da Lei no 8.666/93.

2. O objeto a ser contratado configura serviço de natureza continuada, nos termos da Instrução nº 2.594/2018 do CREA-SP, de 23 de abril de 2018, e será prestado no prazo de 36 (trinta e seis) meses, podendo haver prorrogação do contrato conforme a previsão do artigo 57, Inciso IV da Lei nº 8.666/1993 e se enquadra no conceito de serviço comum, nos termos da Lei 10.520/02, onde os requisitos técnicos são suficientes para determinar o conjunto da solução escolhida, constatando-se, ainda, que a solução é fornecida por mais de uma empresa no mercado.

3. Instrução Normativa SLTI/ME nº 01/2010, que dispõe sobre os critérios de sustentabilidade ambiental na aquisição de bens, contratação de serviços ou obras pela Administração Pública Federal direta;

4. Portaria ME nº 443, de 27 de dezembro de 2018, que dispõe sobre os serviços que deverão ser preferencialmente objeto de execução indireta;

5. Instrução Normativa SGD/ME nº 01, de 4 de abril de 2019, que dispõe sobre as contratações de soluções de TIC;

6. Instrução Normativa SGD/ME nº 73, de 05 de agosto de 2020, que dispõe sobre pesquisa de preços para contratações pela administração pública federal.

3 - DESCRIÇÃO DA SOLUÇÃO

3.1. COMPOSIÇÃO DA SOLUÇÃO

Item	Descrição	Código	Qtde.	Unidade
1	Licenças de Antivírus denominadas pelo fabricante de: "Kaspersky Endpoint Security for Business - Advanced Renewal 3 year Band V: 1000-1499"	KL4867KAVTR	1.369	Licenças
2	Capacitação de implantação, configuração e gerenciamento da solução.	KL 002.11.6	4	Pessoas
3	Capacitação em gerenciamento de vulnerabilidades a atualizações de software e integração com o sistema SIEM	KL 009.12	4	Pessoas
4	Serviço de Suporte 8x5, monitoramento, atualização do servidor e clientes.	N.A.	36	Meses

4 - ESTIMATIVA DAS QUANTIDADES

Estimativa da quantitativo de Licenças

Da quantidade de Estações de Trabalho

A equipe de planejamento, consultou o contrato de locação de computadores e notebooks C-027 / 2018 e verificou que atualmente o CREA-SP conta com um contingente, efetivamente instalado, de:

- 910 Desktops com 8GB de memória
- 170 Desktops com 4GB de memória
- 150 Notebooks com 8GB de memória.

Totalizando 1230 equipamentos.

Da quantidade de Servidores

O CREA-SP possui ativos e funcionando um total de 139 Servidores.

Desta forma, há necessidade de 139 licenças para cobrir todo o parque instalado de servidores.

Da quantidade total de Licenças

Somando-se a quantidade de licenças de estações de trabalho (1230), com as licenças de servidores (139) chegamos a um total de **1369** licenças.

Estimativa de quantitativo de capacitação

Atualmente a equipe de suporte do CREA/SP conta com 4 (quatro) analistas e 2 (dois) técnicos.

A equipe que vai efetivamente trabalhar com o antivírus: dois analistas que pertencem a equipe de atualização/segurança e dois técnicos que pertence a equipe de atendimento ao usuário:

Desta forma há necessidade de contratação de capacitação para 4 (quatro) funcionários efetivos do CREA-SP.

5 - PLANILHA PARA COTAÇÃO DE PREÇO

Item	Descrição	Código	Qtde	Unidade	Valor Unitário	Valor Total
1	Licenças de Antivírus denominadas pelo fabricante de: "Kaspersky Endpoint Security for Business - Advanced Renewal 3 year Band V: 1000-1499"	KL4867KAVTR	1.369	Licenças	R$	R$
2	Capacitação de implantação, configuração e gerenciamento da solução.	KL 002.11.6	4	Pessoas	R$	R$
3	Capacitação em gerenciamento de vulnerabilidades a atualizações de software e integração com o sistema SIEM	KL 009.12	4	Pessoas	R$	R$
4	Serviço de Suporte 8x5, monitoramento, atualização do servidor e clientes.	N.A.	36	Meses	R$	R$
TOTAL GERAL.....						R$

6 - ESPECIFICAÇÃO TÉCNICA

6.1. DESCRIÇÃO DA SOLUÇÃO

1. A Solução contratada constitui-se de produtos e serviços.

2. O produto aqui considerado é a licença que permite a renovação dos bancos de dados de vírus utilizados pelo software da Kaspersky e sua constante atualização durante o prazo da contratação.

3. Os serviços aqui considerados são a capacitação dos profissionais técnicos do CREA-SP e o suporte continuado que a empresa contratada deverá prestar durante a vigência contratual.

6.1.1. DESCRIÇÃO DO PRODUTO - Kaspersky Endpoint Security for Business - Advanced Renewal

Estas Licenças devem possibilitar ao CREA-SP, através do console de gerenciamento e dos softwares clientes instalados nos computadores, usufruir e utilizar as funcionalidades descritas no ANEXO_A_Funcionalidades_mínimas_do_antivirus.pdf.

6.1.2. DESCRIÇÃO DOS SERVIÇOS

1. Este termo de referência descreve dois tipos de serviços que serão contratados:

a. Serviços de Capacitação;

b. Serviços de Suporte;

6.1.2.1. DESCRIÇÃO DOS SERVIÇOS DE SUPORTE

1. O Contrato de suporte consiste no monitoramento pró-ativo e atendimento reativo às solicitações do CREA-SP. A demanda ou solicitação deverá ser realizada através de abertura de chamado pelo CREA-SP, descrevendo a atividade ou suporte necessário, que serão atendidas por profissionais qualificados para o exercício de atividades compatíveis com os tipos de servidores ou dispositivos na rede, levando sempre em consideração as características e limitações dos produtos suportados.

2. O CREA-SP poderá utilizar qualquer combinação dos seguintes Serviços descritos abaixo.

6.1.2.1.1. GERENCIAMENTO DA CONTA DE SUPORTE

1. Os serviços de Gerenciamento de Conta de Suporte são planejados para ajudar na coordenação da relação de suporte e de serviços.

2. A CONTRATADA deverá possuir um representante dos serviços de suporte, o qual chamaremos de Gerente Técnico de Suporte. Este Gerente é o representante do CREA dentro da CONTRATADA, e coordenará a equipe que fornecerá os Serviços de Solução de Problemas.

6.1.2.1.1.1. ATIVIDADES DO GERENTE TÉCNICO DE SUPORTE

1. O Gerente Técnico de Suporte também realizará as seguintes atividades:

a. O Gerente Técnico de Suporte funcionará como canal de comunicação e pode ainda transmitir a percepção do CREA-SP, com relação aos Serviços, para outras instâncias dentro da CONTRATADA.

b. Reunião de Orientação e Planejamento, também denominada reunião inicial do Contrato, ou reunião de “Kick off", a qual está descrita neste termo de referência.

c. Gerenciamento de Escalação. Questões de suporte que requerem o envolvimento de diversos profissionais e níveis hierárquicos podem ser gerenciadas de perto pelo Gerente Técnico de Suporte ou outro representante para acelerar a solução.

6.1.2.1.2. SERVIÇOS DE SUPORTE AO SOFTWARE

1. Nesta modalidade de serviço, no decorrer do período de duração do contrato, a CONTRATADA irá atuar na resolução dos problemas relativos ao Antivírus instalado no CREA-SP, tanto no Servidor, quanto nos clientes, os quais utilizam as licenças contratadas e fornecidas. Conforme os seguintes requisitos:

6.1.2.2 DESCRIÇÃO DOS SERVIÇOS DE CAPACITAÇÃO

1. A CONTRATADA deverá fornecer a capacitação solicitada a quatro membros da equipe de Sustentação de TI do CREA. Através de treinamentos de instalação e operação do ambiente e do sistema de Antivírus atrelado às licenças de software atualizadas, nas versões fornecidas pela CONTRATADA.

2. A CONTRATADA deverá fornecer a transferência de conhecimento sobre o ambiente atualizado do CREA-SP em até 10 dias depois da finalização dos serviços de atualização do Servidor e dos Clientes. Os serviços de transferência de conhecimento devem ser executados remotamente e não devem gerar nenhum ônus financeiro ao CREA-SP.

6.1.2.2.1. DESCRIÇÃO DA CAPACITAÇÃO KL 002.11.6

1. O objetivo principal é fornecer todo o conhecimento necessário para implantar, configurar e gerenciar a solução.

2. O curso deve ensinar como projetar, implantar e manter sistemas de proteção baseados no Kaspersky Endpoint Security e gerenciá-los centralmente por meio do Kaspersky Security Center.

3. A parte teórica do curso e os laboratórios práticos devem fornecer aos alunos conhecimentos e habilidades necessárias para:

3.1. Descrever os recursos do Kaspersky Endpoint Security para Windows e Kaspersky Security Center

3.2. Projetar e implantar uma solução de proteção ideal com base no Kaspersky Endpoint Security em uma rede Windows e gerenciá-la através do Kaspersky Security Center

3.3. Manter o sistema implantado

6.1.2.2.1.1. CONTEÚDO PROGRAMÁTICO MÍNIMO

1. Introdução

1.1. Noções básicas do Kaspersky Endpoint Security for Business

1.2. Como implantar o Kaspersky Endpoint Security for Business

1.3. Como instalar o Kaspersky Security Center

1.3.1. Laboratório 1. Instale o Kaspersky Security Center

1.4. Como instalar o Kaspersky Endpoint Security em computadores

1.4.1. Laboratório 2. Implantar o Kaspersky Endpoint Security

1,5. Como organizar computadores em grupos

1.5.1. Laboratório 3. Crie uma estrutura de computadores gerenciados

2. Gestão de proteção

2.1. Como o Kaspersky Endpoint Security protege os computadores

2.2. Como configurar a proteção de arquivos

2.2.1. Laboratório 4. Testar proteção contra ameaças a arquivos

2.3. Como configurar a proteção contra ameaças de rede

2.3.1. Laboratório 5. Configure a proteção contra ameaças por e-mail

3.5.1. Laboratório 19. Configure o controle adaptativo de anomalias

4. Manutenção

4.1. Como manter a proteção

4.1.1. Laboratório 20. Configure o painel

4.2. O que fazer diariamente

4.3. O que fazer se algo aconteceu

4.3.1. Laboratório 21. Configure as ferramentas de manutenção

4.3.2. Laboratório 22. Colete informações de diagnóstico

4.4. O que fazer periodicamente

6.1.2.2.2. DESCRIÇÃO DA CAPACITAÇÃO KL 009.12

1. Objetivo: Gerenciar vulnerabilidades e atualizações de software nos computadores da rede. Capturar, reconfigurar e instalar imagens do sistema operacional.

Trabalhar com os registros de hardware e software, gerenciar as licenças de aplicativos de terceiros e configure a integração com sistemas SIEM.

6.1.2.2.2.1. CONTEÚDO PROGRAMÁTICO MÍNIMO

1. Introdução

1.1. Vulnerabilidade e gerenciamento de patches no Kaspersky Security Center

1.2. Licenciamento

1.3. Acesso à funcionalidade de gerenciamento de vulnerabilidades e patches na interface do Kaspersky Security Center

2. Vulnerabilidade e gerenciamento de patches

2.1. Declaração do problema

2.2. Procure vulnerabilidades e atualizações necessárias

2.3. Sincronização do Windows Update

3.6.1. Laboratório 10. Como capturar uma imagem do sistema operacional

3.6.2. Laboratório 11. Como implantar uma imagem do sistema operacional em um computador gerenciado

3.6.3. Laboratório 12. Como implantar uma imagem do sistema operacional em um computador "bare metal"

6.2. REQUISITOS

6.2.1. REQUISITOS ESPECÍFICOS DOS SERVIÇOS

6.2.1.1. REQUISITOS DO SERVIÇO DE SUPORTE, MONITORAMENTO E ATUALIZAÇÃO

6.2.1.1.1. REQUISITOS DE ACEITAÇÃO DOS SERVIÇOS PRESTADOS

1. A CONTRATADA deverá apresentar relatório mensal de atendimentos contendo registro de todas as atividades de suporte bem como capacitações realizadas no período mensal de prestação de serviços encerrado.

2. Após a avaliação do relatório apresentado, de acordo com os REQUISITOS DE NÍVEL DE SERVIÇO MÍNIMO (NMS) a CONTRATANTE emitirá um termo de Aceite.

6.2.1.1.1.1. REQUISITOS DE RELATÓRIOS MENSAIS

1. O Relatório deve ser entregue em formato de documento, .pdf, ou docx. Não serão aceitos relatórios na nuvem, ou em outros formatos.

2. O Relatório deve ser encaminhado ao CREA-SP em até 5 (cinco) dias uteis contados a partir do dia seguinte ao fim do período mensal de prestação de serviços.

3. Qualquer gráfico adicionado ao relatório deve conter explicação do significado das informações em ambos os eixos (abscissas e ordenadas) bem como a conclusão do que o mesmo representa, e quais informações úteis tal gráfico fornece para o CREA e para a administração do sistema.

4. O Relatório deve conter no mínimo, mas não se limitando, às seguintes informações:

a. Lista de chamados abertos pelo CREA, e suas respectivas informações sumarizadas:

- Número identificativo do chamado/O.S.
- Descrição do objeto;
- Severidade;

- Data e horário de abertura;

- Tempos de atendimento conforme a tabela de níveis mínimos de serviço abaixo (proatividade, reação, Solução);

b. Assertividade mensal para cada nível de severidade (Sumário do atendimento mensal, contendo totais de chamados por severidade, destacando quais foram solucionados no prazo de atendimento, ou não, e destacando a assertividade mensal);

c. Descrição de atividades realizadas no sistema do Antivírus, solicitadas por via de chamado técnico, ou não. A quais devem conter os respectivos descritivos e conclusões;

d. Análise CONCLUSIVA da situação de segurança do sistema de antivírus (Servidor e estações);

e. Lista de pendências que possam haver entre o CREA-SP e a CONTRATADA, com seus respectivos planos de ações para resolução com responsabilidades claramente definidas (quem faz o que, como e quando);

f. Plano de ações com responsabilidades claramente definidas (quem faz o que, como e quando) para solucionar possíveis anomalias, discrepâncias, ou qualquer situação detectada que possa colocar em risco a segurança do sistema, no que tange a Vírus, ameaças, e todas as funcionalidades do sistema de Segurança oferecido pela Kaspersky;

g. Plano de ações com responsabilidades claramente definidas (quem faz o que, como e quando) para solução de chamados abertos há mais de um mês, que estejam sem solução;

6.2.1.1.2. REQUISITOS DO SERVIÇO DE SUPORTE TÉCNICO

a) O Atendimento e resolução dos chamados do suporte técnico deverá estar disponível, no mínimo, 8 (horas) horas por dia, 05 (cinco) dias por semana, durante o horário comercial, das 9:00 as 18:00, em português ou por meio de um tradutor.

b) A CONTRATADA deverá prestar assistência técnica durante todo o período contratual.

c) Deve haver Abertura ilimitada de chamados de suporte.

d) Não haverá limitante algum, inclusive de quantidade de horas, para o atendimento dos chamados abertos durante a vigência do contrato.

e) O atendimento será preferencialmente remoto. Caso haja necessidade de intervenção presencial "onsite", por qualquer motivo que impeça o atendimento remoto, independente de culpa ou responsabilidade do CREA, ou da CONTRATADA, este deverá ser executada pela CONTRATANTE.

f) Toda e qualquer despesa relacionadas a prestação do serviço de suporte presencial "onsite", inclusive, mas não se limitando a locomoção, estadia, alimentação e despesas trabalhistas são de responsabilidade inteira e exclusiva da CONTRATADA.

g) Qualquer atendimento presencial "onsite" deverá ser executado em uma das sedes do CREA na Capital de São Paulo.

h) Todos os atendimentos, (remotos ou locais), deverão ser executados sempre com acompanhamento e supervisão da equipe técnica da CONTRATANTE.

i) A CONTRATADA deverá oferecer manutenção e suporte técnico conforme o nível de severidade de cada chamado e dentro dos tempos de resposta definidos abaixo:

j) Quando um chamado for aberto pela CONTRATADA, a CONTRATANTE deverá atribuir ao chamado o nível de severidade de acordo com a avaliação do tipo do problema e do impacto/dano.

k) O CREA-SP poderá a qualquer momento, a seu próprio critério solicitar a mudança da severidade do chamado.

No qual deve ser prontamente atendido pela CONTRATADA, que deve passar a atendê-lo de acordo com a nova severidade.

l) A tabela abaixo traz exemplos de tipos de problemas e níveis de severidade.

Nível de Severidade	**Descrição de suporte e operações**
Severidade A (Crítica)	1 - Ambiente sem condições de funcionamento. 2 - Um ou mais serviços não estão acessíveis ou não podem ser usados. A produção, as operações ou as datas limite para implantação são gravemente afetadas, ou há um grave impactos obre a produção ou as atividades da instituição, ou de algum (qualquer) usuário da mesma. 3 - Um único, ou mais usuários, clientes ou serviços é afetado parcial ou totalmente. 4 - Situação que, mesmo não representando problema técnico grave, possa estar impactando na prestação do serviço do CREA-SP. Ex. Máquina do pregoeiro com problema de vírus, impedindo que seja realizado um pregão na data e hora marcados.
Severidade B (Médio)	Problema que gera restrições ao pleno funcionamento do ambiente. O serviço pode ser usado, mas com limitações. A situação tem impacto operacional moderado e é possível lidar com ela durante o horário comercial. Um único usuário, cliente ou serviço é afetado parcial ou totalmente.

Severidade C (Baixo)	Problema que não afeta o funcionamento do ambiente. A situação tem impacto operacional mínimo. O problema é importante, mas não tem impacto expressivo na produtividade e no serviço atual do cliente. Um único usuário experimenta interrupção parcial, mas existe uma solução alternativa aceitável

6.2.1.1.3. REQUISITOS DE NÍVEL DE SERVIÇO MÍNIMO (NMS)

1. Quanto ao tempo de resposta inicial do suporte técnico, deverá ser baseado nos níveis de severidade descritos acima.

A tabela abaixo descreve as metas de tempo de resposta.

Impacto	Tempo de Proatividade	Tempo de Reação	Tempo de Solução	Assertividade
Crítica	Até 5 minutos	Até 30 min.	Até 2 horas	95 %
Médio	Até 10 minutos	Até 1 hora	Até 4 horas	95 %
Baixo	Não se aplica	Até 06 horas	Até 8 horas	95 %

a) Tempo de Proatividade refere-se ao tempo decorrente entre a detecção da falha e a abertura do chamado. O sistema de Monitoramento/proatividade deve ao detectar uma falha, imediatamente abrir um chamado na operadora dentro dos tempos mínimos especificados.

b) Tempo de reação refere-se ao tempo decorrente entre a abertura do chamado e o contato telefônico (não é contabilizado contato por e-mail, SMS ou outro meio de mão única) entre a contratada e o analista do CREA-SP.

c) Tempo de solução é o tempo decorrido da abertura do chamado até a solução de contorno ou definitiva;

d) Solução de contorno entende se por uma solução temporária que restaure a funcionalidade perdida de forma que os efeitos do problema não sejam mais percebidos pelos usuários.

e) Solução definitiva entende-se pela solução que sanará a causa do problema.

f) Nas situações em que for detectado e/ou comprovado um problema de software (bug) na solução ofertada, o prazo de atendimento será fornecido diretamente pela engenharia do fabricante da solução ofertada.

g) Não será aceito fechamento unilateral de qualquer chamado, por qualquer motivo, ou seja, para que algum chamado seja encerrado deverá haver a anuência do CREA-SP.

h) Chamados que dependam de ação do CREA poderão ficar em estado de pausa, em que o tempo para solução não é contato, até que o CREA execute a ação que retire de sua responsabilidade a referida dependência. Nesses Casos, todos os tempos de atendimento e pausa devem ser registrados pela CONTRATADA.

i) Os chamados abertos não poderão, em hipótese alguma, ser fechados e/ou pausados unilateralmente pela CONTRATADA sem anuência por escrito do CREA-SP.

j) Qualquer chamado que seja fechado e/ou pausado sem anuência por escrito do CREA-SP deverá ser imediatamente reaberto pela CONTRATADA, permanecendo assim até que seja dada solução, ou justificativa para o fechamento/pausa. E em quaisquer dos casos devem ser aceitos formalmente, por escrito, pelo CREA-SP.

k) A empresa contratada deverá apresentar mensalmente relatório contendo todos os chamados abertos pelo CREA-SP, os tempos de reação, tempos de atendimento, assertividade, e plano de ação para solucionar problemas recorrentes ou sem solução os quais estejam impactando no funcionamento do ambiente, resguardando o direito do CREA-SP em elaborar seus próprios relatórios de auditoria para confrontá-los ao relatório da contratada.

6.2.1.1.4. REQUISITOS DE CENTRAL DE ATENDIMENTO

1. A CONTRATADA deverá disponibilizar uma Central de Atendimento para que a equipe técnica do CREA-SP faça registros de ocorrências e solicitações de reparo, bem como o acompanhamento da solução dos problemas.

2. O serviço de registro de chamadas deverá estar disponível nas 24 (vinte e quatro) horas do dia e nos 7 (sete) dias da semana.

3. A CONTRATADA deverá disponibilizar um número telefônico para receber as chamadas técnicas do CREA-SP, e realizar a comunicação entre o CREA-SP e a central de Atendimento da Contratada.

4. A Central de Atendimento deverá gerar um identificador de registro de chamadas que deverá ser informado ao CREA-SP no momento da abertura do chamado, e que terá por finalidade identificar a qualquer momento o problema específico, possibilitando o controle de chamados.

5. O CREA-SP poderá também realizar a abertura de chamados técnicos e solicitações de serviços para todos os itens desta especificação técnica diretamente no sistema de atendimento da CONTRATADA através de um Portal de Atendimento com acessos web, para abertura de chamados técnicos e solicitações de serviços e acompanhamento dos mesmos.

6. As informações relativas aos chamados deverão ser atualizadas automaticamente sempre que houver alguma alteração em sua situação. O acompanhamento on-line da resolução de chamados pelo CREA-SP poderá ser feito também através do sistema de atendimento.

7. Os chamados abertos no sistema de atendimento ou na Central de Atendimento serão referentes a todas as atividades de responsabilidade da CONTRATADA.

8. Os registros dos chamados deverão conter todas as informações relativas ao chamado aberto, como tempo de início e fim de atendimento, identificação do elemento (cliente, servidor) afetado, nome, fone e e-mail do contato no CREA-SP que foi posicionado acerca do reparo e restabelecimento do serviço, descrição detalhada da resolução do chamado com um código associado e responsabilidades.

9. A Contratada deverá atender chamados abertos por usuário, não técnicos, previamente cadastrados, relacionados à: Lentidão da rede, Indisponibilidade e Solicitação de Permissão de acesso à sites; (Apenas gestores);

6.2.1.1.5. REQUISITOS DOS SERVIÇOS DE ATUALIZAÇÃO

1. Os Serviços de atualização devem estar atrelados a chamados abertos no sistema da CONTRATADA, que possibilitarão o acompanhamento das atividades por parte da CONTRATANTE.

2. A CONTRATANTE deverá fornecer as senhas e usuários necessários para que os serviços de atualização possam ser executados adequadamente.

6.2.1.1.5.1. REQUISITOS DE LOCALIDADE DOS SERVIÇOS DE ATUALIZAÇÃO

1. Todo o Serviço de atualização poderá ser realizado remotamente, não obstante, caso haja necessidade de visita "on-site" para atendimento dos requisitos ou funcionalidades das atualizações dentro do prazo, todas as despesas de estadia, alimentação, transporte, etc. deverão ser pagas pela CONTRATADA, sem nenhum ônus financeiro para a CONTRATANTE.

2. A visita, caso necessária, se dará no site do CREA-SP situado à Av. Brigadeiro Faria Lima, 1059, Pinheiros, São Paulo, SP.

3. A decisão da solicitação de visita técnica "on-site" para atendimento deste requisito do contrato é de responsabilidade ÚNICA da CONTRATANTE, desde que baseada nas necessidades de cumprimento de prazo de instalação, ou de impossibilidade técnica da realização do serviço de forma remota, não havendo, depois de solicitado oficialmente pela CONTRATANTE, a possibilidade da CONTRATADA negar por qualquer motivo.

4. A Solicitação de Serviço de Atualização "on-site" deve ser realizada através da emissão de um oficio do CREA-SP para a CONTRATADA.

6.2.1.1.5.2 REQUISITOS DE ATUALIZAÇÃO DO SERVIDOR

1. A CONTRATADA deverá atualizar o banco de dados do Servidor de console do Antivírus, sendo de sua responsabilidade todas as atividades necessárias para entregar o servidor gerenciando todas as 1369 máquinas clientes, incluindo, mas não se limitando às seguintes atividades:

a. instalar/atualizar licenças.

b. Atualizar softwares clientes nos computadores dos usuários.

c. Atualizar softwares no Servidor.

d. Configurar parâmetros do Antivírus no servidor de console.

e. Parametrizar, caso necessário, o próprio console de gerenciamento.

6.2.1.1.5.3. REQUISITOS DE ATUALIZAÇÃO DOS CLIENTES

1. É responsabilidade da CONTRATADA atualizar todos os 1369 clientes do antivírus instalados nos computadores da Rede do CREA-SP, incluindo, mas não limitando-se às seguintes atividades:

a. instalar e atualizar licenças.

b. conectar-se remotamente no computador, celular, tablet, ou qualquer que seja o cliente, caso necessário.

c. configurar parâmetros

d. parametrizar, caso necessário o próprio sistema operacional do host cliente.

2. O Serviço de atualização dos clientes deverá ser executado imediatamente após o Serviço de Atualização do Servidor.

6.2.1.2. REQUISITOS DOS SERVIÇOS DE CAPACITAÇÃO

1. Os treinamentos devem ser fornecidos exclusivamente em Português.

2. Os treinamentos devem fornecer a cada participante um certificado reconhecido pela Kaspersky.

3. Os treinamentos devem ser fornecidos preferencialmente através de recursos online.

6.2.2. REQUISITOS GERAIS

6.2.2.1. REQUISITOS TEMPORAIS

1. As licenças dos softwares contratados, bem como suas chaves de ativação, devem ser disponibilizadas em até 15 dias corridos após a assinatura do contrato, podendo ser prorrogado por igual período, desde que justificado pela CONTRATADA e autorizado pela CONTRATANTE.

2. Os documentos pertinentes aos licenciamentos de softwares deverão ser entregues no endereço: Av. Brigadeiro Faria Lima, 1059 - Pinheiros - São Paulo/SP - CEP 01452-920, aos cuidados do Gestor do Contrato.

3. De comum acordo entre o CREA-SP e a CONTRATADA, a entrega da documentação previstas no item anterior poderá ser realizada de forma eletrônica.

4. Os instaladores dos softwares previstos neste termo de referência, assim como suas atualizações, deverão estar disponíveis para download em conta registrada em nome do CREA-SP ou de representante indicado pelo CREA-SP em site oficial designado pelo fabricante.

5. As versões das licenças deverão ser as mais recentes disponibilizadas no mercado pelo fabricante.

6. As atualizações ou correções das versões das licenças serão realizadas durante todo o período de vigência contratual.

6.2.2.2. REQUISITOS GERAIS PARA A EXECUÇÃO DOS SERVIÇOS

1. Serem realizados com base nas boas práticas preconizadas por modelos como ITIL (IT lnfrastructure Library), COBIT e PMBOK (Project Management Body of Knowledge);

2. Serem executados dentro dos parâmetros estabelecidos neste processo de contratação, com observância às recomendações aceitas pela boa técnica, normas e legislação, bem como observar conduta adequada na utilização dos materiais, equipamentos, ferramentas e utensílios, observando sempre os critérios de qualidade;

3. Adequar-se aos padrões normativos orientados pela Política de Segurança do CREA-SP;

4. Realizar os serviços de modo que não prejudiquem o andamento normal das atividades do Órgão em horário de seu expediente;

5. Implantar o planejamento, a execução e a supervisão permanente dos serviços demandados;

6. Responsabilizar-se pela definição da forma, metodologia, processos, local e modelo e execução dos serviços;

6.2.2.3. REQUISITOS DE QUALIFICAÇÕES DOS PROFISSIONAIS

1. Todos os serviços realizados pela CONTRATADA no âmbito desta CONTRATAÇÃO devem ser executados por profissionais qualificados certificados pela fabricante dos Softwares.

6.2.2.4. OUTROS REQUISITOS LEGAIS

1. A CONTRATADA deve executar o objeto do certame em estreita observância dos ditames estabelecido pela Lei no13.709/2018 (Lei Geral de Proteção de Dados Pessoais (LGPD)).

7 - DEVERES E RESPONSABILIDADES DA CONTRATANTE

7.1. OBRIGAÇÕES E RESPONSABILIDADES DA CONTRATANTE

1. Observar e fazer cumprir fielmente o que estabelece este Termo de Referência;

2. Receber o objeto no prazo e condições estabelecidas no Termo de Referência;

3. Prestar as informações e os esclarecimentos que venham a ser solicitados pela CONTRATADA;

4. Comunicará a CONTRATADA toda e qualquer ocorrência relacionada com a execução do Contrato;

5. Acompanhar e fiscalizar o cumprimento das obrigações da CONTRATADA por meio de um fiscal;

6. Colocar à disposição da CONTRATADA os elementos e informações necessárias à consecução do objeto do Contrato;

7. Atestar a entrega do objeto, receber e promover o pagamento das faturas correspondentes, quando apresentadas na forma estabelecida neste Termo;

8. Aplicar à CONTRATADA as penalidades contratuais e regulamentares cabíveis, garantidos o contraditório e a ampla defesa;

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

8 - DEVERES E RESPONSABILIDADES DA CONTRATADA

8.1. OBRIGAÇÕES E RESPONSABILIDADES DA CONTRATADA

1. Executar os serviços conforme especificações deste Termo de Referência e de sua proposta;

2. Reparar, corrigir, remover ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os serviços efetuados em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;

3. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, de acordo com os artigos 14 e 17 a 27, do Código de Defesa do Consumidor (Lei no 8.078, de 1990);

4. Responsabilizar-se por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas em legislação específica, cuja inadimplência não transfere responsabilidade à CONTRATANTE;

5. Relatar à CONTRATANTE toda e qualquer irregularidade verificada no decorrer da prestação dos serviços;

6. Executar o objeto do certame em estrita observância dos ditames estabelecido pela Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais (LGPD)).

7. Prestar as informações e os esclarecimentos que venham a ser solicitados pela CONTRATANTE por intermédio de preposto designado para acompanhamento do contrato) Indicar no prazo máximo de 24 horas úteis após a assinatura do contrato, junto à CONTRATANTE, um preposto para representar a CONTRATADA, principalmente no tocante à eficiência e agilidade da execução dos serviços objeto deste Termo de Referência, e que deverá responder pela fiel execução do contrato; Na hipótese de afastamento do preposto definitivamente ou temporariamente, a CONTRATADA deverá comunicar ao Gestor do Contrato por escrito o nome e a forma de comunicação de seu substituto até o fim do próximo dia útil.

8. Reconhecer o Gestor do Contrato, bem como outros servidores que forem indicados pela CONTRATANTE, para realizar as solicitações relativas ao contrato firmado, tais como manutenção, configuração, entre outras;

9. Apresentar Nota Fiscal/Fatura com a descrição dos serviços prestados, nas condições deste Termo de Referência, como forma de dar início ao processo de pagamento pela CONTRATANTE;

10. Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual;

11. Assumir as responsabilidades pelos encargos fiscais e comerciais resultantes da contratação.

12. Reparar, corrigir, remover ou substituir, às suas expensas, no total ou em parte, no prazo fixado em contrato, os serviços efetuados em que se verificarem vícios, defeitos ou incorreções resultantes da execução;

13. Propiciar todos os meios necessários à fiscalização do contrato pela CONTRATANTE, cujo representante terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, sempre que considerar a medida necessária;

14. Acatar as orientações da CONTRATANTE, sujeitando-se à mais ampla e irrestrita fiscalização, prestando os esclarecimentos solicitados e atendendo as reclamações formuladas;

15. Prestar esclarecimentos à CONTRATANTE sobre eventuais atos ou fatos noticiados que se refiram à CONTRATADA, independente de solicitação;

16. Comunicar à CONTRATANTE, por escrito, qualquer anormalidade nos serviços e prestar os esclarecimentos julgados necessários;

17. Não veicular publicidade ou qualquer outra informação acerca da prestação dos serviços do Contrato, sem prévia autorização da CONTRATANTE;

18. Não fazer uso das informações prestadas pela CONTRATANTE para fins diversos do estrito e absoluto cumprimento do contrato em questão;

9 - MODELO DE EXECUÇÃO DO CONTRATO

9.1 - Rotinas de Execução

9.1.1. FASE INICIAL DA CONTRATAÇÃO

1. A Fase inicial da contratação é definida como sendo os primeiros sessenta dias de contrato, no qual a contratada DEVERÁ realizar a atualização das licenças contratadas no Servidor de Antivírus e nos computadores do CREA-SP e seus respectivos clientes de Antivírus.

2. A Fase de Iniciação compreende as seguintes atividades:

a. A Reunião de Início do contrato

b. Atualização do Servidor de Antivírus

c. Atualização dos computadores/celulares/etc. onde roda o respectivo cliente do Antivírus.

9.1.1.1. DA REUNIÃO INICIAL DO CONTRATO

1. As partes, CONTRANTE e CONTRATADA deverão, em até 05 (cinco) dias úteis após a assinatura do contrato, prorrogáveis uma única vez, a pedido justificado pela CONTRATADA, promover a reunião inicial do Contrato ("kick off") para o estabelecimento e planejamento dos procedimentos relacionados ao updade/atualização das licenças no servidor e clientes.

2. A reunião inicial deve ter como resultado final um documento, que deve ser elaborado pela CONTRATADA e entregue ao CREA-SP para validação até o 10o dia útil após o início da execução dos serviços contratados, contemplando as seguintes premissas/atividades para o prazo de 60 dias:

a. O Plano de atualização do Servidor

b. O Plano de atualização dos clientes

c. Plano de Treinamento dos servidores do CREA-SP;

d. Plano para início dos atendimentos dos chamados de suporte técnico aos usuários do CREA-SP;

e. Entrega dos manuais de procedimentos para abertura de chamados na Central de Serviços para disseminação aos usuários de TIC do CREA-SP.

9.1.2. FASE DE OPERAÇÃO

1. A Fase de operação inicia com o aceite por parte do CREA da atualização das Licenças contratadas, tanto no Servidor quanto nos seus respectivos clientes, conforme os planejamentos efetuados na fase inicial da contratação.

2. A Fase de operação termina com o término do contrato.

3. Durante a Fase de Operação, a CONTRATADA entra em regime de Suporte continuado, conforme requisitos de suporte definidos neste termo de referência.

4. Durante esta fase o CREA-SP solicitará intervenções da CONTRATADA através da abertura de chamados no sistema da CONTRATADA, os quais devem ser atendidos pela CONTRATADA de acordo com o acordo de NMS (Nível Mínimo de Serviço) definido neste Termo de referência.

9.1.3. DA VIGÊNCIA

1. O Contrato terá vigência de 36 (trinta e seis) meses a partir da data de sua assinatura, podendo ser prorrogado até o limite de 48 (quarenta e oito) meses, na forma da Lei nº 8.666/93.

2. O Contratado deverá sujeitar-se aos acréscimos e supressões contratuais estabelecidos na forma do Art. 65 da Lei nº 8.666/93.

9.1.4. DO REAJUSTAMENTO DE PREÇOS

1. Os preços serão fixos e irreajustáveis pelos primeiros 12 (doze) meses da vigência contratual.

2. A cada 12 (doze) meses de execução contratual, o valor vigente do contrato sofrerá reajuste pelo índice IPC-FIPE para fins de atualização dos valores inicialmente contratados, tomando por base a data da apresentação da proposta comercial.

3. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

9.1.5. DA TRANSIÇÃO CONTRATUAL

1. Em casos de interrupção contratual e ocorrendo mudança de fornecedor da solução, todo conhecimento adquirido ou desenvolvido, bem como toda informação produzida pelos atendimentos de chamados de suporte deverão ser disponibilizados à CONTRATANTE ou empresa por ela designada em até 30 (trinta) dias corridos após o encerramento do contrato. As informações disponibilizadas devem ser em formato digital, inteligível para humanos, e na língua portuguesa.

2. A CONTRATADA deverá elaborar o Plano de Transição, no prazo de 60 (sessenta) dias corridos antes do encerramento do contrato, para a transferência integral e irrestrita dos conhecimentos e das competências necessárias e suficientes para promover a continuidade dos serviços.

3. A CONTRATANTE poderá estabelecer prazo inferior caso haja rescisão contratual.

4. Nenhum pagamento será devido à CONTRATADA pela elaboração ou pela execução do Plano de Transição. O fato da empresa CONTRATADA ou seus representantes não cooperarem ou reterem qualquer informação ou dado solicitado pela CONTRATANTE, que venha a prejudicar, de alguma forma, o andamento da transição das tarefas e serviços para um novo prestador, constituirá quebra de contrato, sujeitando-a as obrigações em relação a todos os danos causados à CONTRATANTE.

9.2. - Quantidade Mínima de Bens ou Serviços para Comparação e Controle

9.2.1. SERVIÇO DE SUPORTE CONTINUADO

1. O Serviço será auferido por meio do ACORDO DE NÍVEL DE SERVIÇO - NÍVEIS MÍNIMOS DE SERVIÇOS (NMS).

9.2.1.1. A execução contratual será acompanhada e fiscalizada por representantes da CONTRATANTE, que poderá utilizar-se da contratação de terceiros para assisti-la e subsidiá-la de informações pertinentes a essa atribuição, em consonância com as disposições do art. 67 da Lei no 8.666/1993.

9.2.1.2. A avaliação da qualidade e da adequação dos serviços ocorrerá na entrega do relatório mensal dos serviços prestados e será realizada pelo Fiscal Técnico do Contrato com base nos indicadores definidos no item REQUISITO DE NÍVEL DE SERVIÇO MÍNIMO (NMS) deste termo de referência, aos quais a CONTRATADA deverá atender.

9.2.1.3. A CONTRATADA estará sujeita, garantido o contraditório e a ampla defesa, às sanções administrativas em função dos indicadores obtidos abaixo da faixa de ajuste.

9.2.1.4. A aplicação dos ajustes do pagamento não exclui a aplicação de multas e sanções previstas neste documento.

9.2.2. DEMAIS SERVIÇOS

1. Os serviços serão auferidos mediante recebimento dos itens contratados, nas datas previamente acordadas entre o CREA-SP e a Contratada devidamente atestados pelo gestor do contrato.

9.3. - Mecanismos Formais de Comunicação entre a Contratada e a Administração

9.3.1. São mecanismos formais de comunicação entre a CONTRATADA e a CONTRATANTE:

a) E-mails: forma rápida de comunicação para tratar de informações pouco críticas;

b) Ofícios: Comunicação para tratar de assuntos gerais;

9.3.2. Toda a comunicação entre a CONTRATANTE e a CONTRATADA deverá ser sempre formal como regra, exceto em casos excepcionais que justifiquem outro canal de comunicação.

9.4 - Forma de Pagamento em Função dos Resultados

9.4.1. FORMAS DE PAGAMENTO

9.4.1.1. FORMA DE PAGAMENTO MEDIANTE ENTREGA

1. Os pagamentos dos seguintes itens da TABELA DE COMPOSIÇÃO DA SOLUÇÃO serão realizados mediante a entrega dos mesmos, após atesto do gestor do contrato e emissão da devida nota fiscal.

a. Capacitação código KL 002.11.6.

b. Capacitação código KL 009.12.

c. Licenças código KL4867KAVTR - Licenças, denominadas pela fabricante como: Kaspersky Endpoint Security for Business - Advanced Renewal 3 year.

9.4.1.2. FORMA DE PAGAMENTO DOS SERVIÇOS DE SUPORTE

1. O pagamento do Serviço de Suporte, Serviço de Atendimento 8x5, também chamado de Suporte Continuado, por sua característica de serviço continuado, será pago mensalmente após a emissão da devida nota fiscal e atesto do gestor do contrato.

9.4.2. DA NOTA FISCAL

1. O CREA-SP efetuará o pagamento até o 15º (décimo quinto) dia após a apresentação da nota fiscal/fatura, a qual deverá ser entregue na Sede Faria Lima, na Equipe de Suporte e Sustentação de TI, localizada na Av. Brigadeiro Faria Lima, 1059 – Pinheiros – CEP 01452-920 – São Paulo/SP, ficando a CONTRATADA obrigada a manter durante execução dos serviços os documentos abaixo relacionados acompanhados da nota fiscal/fatura:

2. Comprovante de Regularidade com o Fundo de Garantia do Tempo de Serviço– Certificado de Regularidade do FGTS CRF.

3. Comprovante de regularidade para com a Fazenda Federal- Certidão de débitos relativos a créditos tributários Federais e à Dívida ativa da União.

4. Comprovante de inexistência de débitos inadimplidos perante a Justiçado Trabalho, mediante a apresentação de Certidão

5. A nota fiscal/fatura será analisada, minimamente, quanto aos itens a seguir descritos:

a. Correlação entre os valores indicados na nota fiscal/fatura o da proposta da empresa.

b. Ausência de emendas ou rasuras na nota fiscal/fatura.

c. O correto preenchimento dos dados do CREA-SP (nome, CNPJ, dados contratuais) e da discriminação dos serviços;

d. Pertinência dos cálculos aritméticos da nota fiscal/fatura – o valor total deverá corresponder ao somatório dos valores individuais lançados na mesma,

e. Correlação entre o valor da nota fiscal e os valores empenhados;

f. Correlação entre o CNPJ da CONTRATADA e o constante na proposta e na nota de empenho;

6. O Crea-SP efetuará retenção de impostos eventualmente incidentes sobre o valor do bem/serviço, conforme previsto na Lei Federal nº 9.430, de 27 de dezembro de 1996 e Instrução Normativa RFB nº 1.234, de 11 de janeiro de 2012 e anexo;

7. A CONTRATADA é responsável pelos encargos fiscais, trabalhistas e previdenciários incidentes sobre os serviços contratados;

8. Se a CONTRATADA descumprir qualquer termo ou condição a que se obrigar no presente certame, por sua exclusiva culpa, poderá a Administração reter o pagamento, até que seja sanado o respectivo inadimplemento, não sobrevindo, portanto, qualquer ônus ao Conselho resultante desta situação;

9. Na hipótese do Crea-SP, por sua exclusiva culpa, efetuar com atraso qualquer pagamento previsto no Contrato, ficará sujeito multa de 2% (dois por cento) ao mês sobre o valor devido, calculada proporcionalmente aos dias de atraso.

9.4.3. CRONOGRAMA FÍSICO FINANCEIRO

1. A Tabela a seguir lista os principais marcos e eventos que ocorrerão durante a execução do Contrato:

Item	Descrição	Ano 1	Ano 2	Ano 3
1	Assinatura do contrato	N.A	N.A	N.A
2	Licenças e capacitação, itens 1, 2 e 3 da tabela de composição da solução	- Pagamento total mediante recebimento	N.A	N.A
3	Serviço de Suporte item 4 da tabela de composição da solução	- Pagamento de 1/3 do valor do contrato - Pagamento Mensal	- Pagamento de 1/3 do valor do contrato - Pagamento Mensal	- Pagamento de 1/3 do valor do contrato - Pagamento Mensal

10 - PROCEDIMENTOS DE FISCALIZAÇÃO DA EXECUÇÃO CONTRATUAL

10.1. PAPÉIS E RESPONSABILIDADES

10.1.1. PAPEIS E RESPONSABILIDADES DO CREA NA FISCALIZAÇÃO CONTRATUAL

10.1.1.1. Gestor do Contrato

Servidor com atribuições gerenciais, designado para coordenar e comandar o processo de gestão e fiscalização da execução contratual, indicado por autoridade competente.

10.1.1.2. Fiscal Técnico

Servidor representante da Área de Tecnologia da Informação, indicado pela autoridade competente dessa área para fiscalizar tecnicamente o contrato.

10.1.1.3. Fiscal Administrativo

Servidor representante da Área Administrativa, indicado pela autoridade competente dessa área para fiscalizar o contrato quanto aos aspectos administrativos.

10.1.2. PAPEIS E RESPONSABILIDADES DA CONTRATADA NA FISCALIZAÇÃO CONTRATUAL

10.1.2.1. Preposto

Representante da CONTRATADA, responsável por acompanhar a execução do contrato e atuar como interlocutor principal junto ao Órgão, incumbido de receber, diligenciar, encaminhar e responder às principais questões técnicas, legais e administrativas referentes ao andamento contratual:

1. Fazer a gestão geral do contrato, mantendo o controle de todas os chamados, com o objetivo de garantir a execução dos serviços dentro dos prazos estabelecidos, atendendo a todos os requisitos de qualidade;

2. Realizar a gestão, por parte da CONTRATADA, quanto aos aspectos de caráter administrativo e legal do contrato;

3. Informar ao CREA-SP sobre problemas de qualquer natureza que possam impedir o andamento normal dos serviços;

4. Elaborar e entregar ao Gestor os documentos mensais referentes ao cumprimento dos Níveis mínimos de Serviço (NMS);

5. Garantir a execução dos procedimentos administrativos referentes aos recursos envolvidos na execução dos serviços contratados;

6. Estar apto a prestar tempestivamente todas as informações (por meio de documentos impressos ou digitais) sobre as regularidades fiscais e financeiras da empresa, bem como a manutenção de todos os requisitos contratuais. Irregularidades administrativas ou contratuais poderão ensejar rescisão contratual;

7. Supervisionar todos os processos do trabalho, garantindo a qualidade dos serviços prestados e o cumprimento dos Níveis Mínimos de Serviço estabelecidos;

8. Propor novas rotinas, processos e fluxos de trabalho, visando maior eficácia no serviço prestado;

9. Gerenciar o cumprimento de prazos e prioridades estabelecidos;

10. Gerenciar e acompanhar o desempenho da prestação de serviço.

10.2. CONTROLE E FISCALIZAÇÃO DA EXECUÇÃO

1. O acompanhamento e a fiscalização da execução do contrato consistem na verificação da conformidade da prestação dos serviços e da alocação dos recursos necessários, de forma a assegurar o perfeito cumprimento do ajuste, devendo ser exercidos por um ou mais representantes da CONTRATANTE, especialmente designados, na forma dos arts. 67 e 73 da Lei nº 8.666, de 1993, e do art. 10 do Decreto nº 9.507, de 2018.

2. O representante da CONTRATANTE deverá ter a experiência necessária para o acompanhamento e controle da execução dos serviços e do contrato.

3. A verificação da adequação da prestação do serviço deverá ser realizada com base nos critérios previstos neste Termo de Referência e Anexos.

4. A execução do contrato será acompanhada e fiscalizada por meio de instrumentos de controle, que compreendam a mensuração dos aspectos mencionados no art. 47 e no ANEXO V, item 2.6, i, ambos da IN nº 05/2017.

5. A fiscalização técnica do contrato avaliará constantemente a execução do objeto e utilizará o Instrumento de Medição de Resultado (IMR), conforme previsto na TABELA DE NÍVEIS MÍNIMOS DE SERVIÇOS (NMS) deste Termo de Referência, ou outro instrumento substituto para aferição da qualidade da prestação dos serviços, devendo haver o redimensionamento no pagamento com base nos indicadores estabelecidos, sempre que a CONTRATADA:

- Não produzir os resultados, deixar de executar, ou não executar com a qualidade mínima exigida as atividades contratadas; ou

- Deixar de utilizar materiais e recursos humanos exigidos para a execução do serviço, ou utilizá-los com qualidade ou quantidade inferior à demandada.

6 A utilização da tabela NMS não impede a aplicação concomitante de outros mecanismos para a avaliação da prestação dos serviços.

7. Durante a execução do objeto, o fiscal técnico deverá monitorar constantemente o nível de qualidade dos serviços para evitar a sua degeneração, devendo intervir para requerer à CONTRATADA a correção das faltas, falhas e irregularidades constatadas.

10.3. ENTREGA E CRITÉRIOS DE ACEITAÇÃO DO OBJETO

10.3.1. ACEITAÇÃO DOS SERVIÇOS DE SUPORTE CONTINUADO

Os Serviços de suporte continuado serão aceitos mensalmente pelo gestor do contrato, através do seu Atesto. Os Critérios utilizados para dar aceitação são os definidos no NMS (Nível mínimo de Serviço) deste Termo de Referência.

10.3.1.1. ACEITAÇÃO DOS SERVIÇOS DE ATUALIZAÇÃO DO SERVIDOR

1. A aceitação referente ao primeiro mês da contratação, além dos critérios definidos no NMS (Níveis Mínimos de Serviço), somente será emitida após o término do Serviço de atualização do Servidor, conforme definido nos requisitos de atualização do Servidor (6.2.1.1.5.2)

10.3.1.2. ACEITAÇÃO DOS SERVIÇOS DE ATUALIZAÇÃO DOS CLIENTES

1. A aceitação referente ao segundo mês da contratação, além dos critérios definidos no NMS (Níveis Mínimos de Serviço), somente será emitida após o termino do Serviço de atualização dos Clientes, conforme definido nos requisitos de atualização dos Clientes (6.2.1.1.5.3).

10.3.2. ACEITAÇÃO DOS DEMAIS ITENS DO OBJETO

O Critério de aceitação é o seu recebimento e a verificação de que atendem ao tipo e quantitativo solicitado no objeto da Contratação.

10.4. DA ACEITAÇÃO DO OBJETO

1. A recusa parcial ou total de um relatório de serviços emitido, será oficiada à CONTRATADA pela CONTRATANTE, que deverá prontamente prestar o serviço de acordo com o solicitado e em acordo com os requisitos estabelecidos pelo contrato;

SERVIÇO PÚBLICO FEDERAL
CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA DO ESTADO DE SÃO PAULO

CREA-SP

11 - ESTIMATIVA DE PREÇO

Item	Bem/serviço	Qtde	Unidade	Valor unitário	Valor Total
1	Licenças de Antivírus denominadas pelo fabricante de: "Kaspersky Endpoint Security for Business - Advanced Renewal 3 year Band V: 1000-1499"- código KL4867KAVFR	1369	Licenças	R$	R$
2	Capacitação de implantação, configuração e gerenciamento da solução.	4	Pessoas	R$	R$
3	Capacitação em gerenciamento de vulnerabilidades a atualizações de software e integração com o sistema SIEM.	4	Pessoas	R$	R$
4	Serviço de Suporte 8x5, monitoramento, atualização do servidor e clientes	36	Serviço Mensal	R$	R$
TOTAL (R$)					

12 - FONTE DE RECURSOS ORÇAMENTÁRIOS

12.1. DOTAÇÃO ORÇAMENTÁRIA

Os recursos orçamentários para a presente contratação são oriundos:

- Conta Contábil: 6.2.2.1.1.01.04.09.005
- Centro de Custo: 01.03.17.09.01.01

13 - LOCAIS DE ENTREGA

13.1 Endereço: Av. Brigadeiro Faria Lima, 1059 - Pinheiros - São Paulo - SP

- Telefone para informações: (11) 3095 – 6484

SERVIÇO PÚBLICO FEDERAL
CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA DO ESTADO DE SÃO PAULO

CREA-SP

14 - CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

REGIME DE EXECUÇÃO	( ) Empreitada	( ) Preço Global	(X) Preço Unitário
ADJUDICAÇÃO DO OBJETO	(X) Global	( ) Por Lote	( ) Por Item

14.1. – Qualificação Técnica

1. Comprovação de aptidão para a para o fornecimento de bens/serviços em características, quantidades e prazos compatíveis com o objeto desta licitação, por meio de apresentação de Atestado fornecido por pessoas jurídicas de direito público ou privado.

2. O(s) atestado(s) deverão ser apresentados em papel timbrado do emitente, conter identificação do signatário, nome, endereço, telefone e se for o caso, correio eletrônico para contato, a fim de possibilitar possíveis diligências.

OBS.: A Licitante Vencedora deverá apresentar obrigatoriamente, na assinatura do Contrato, cópia autenticada da declaração feita pela Kaspersky, declarando que a empresa é revenda autorizada a fornecer o produto adquirido através do certame.

14.2 - Critérios de Seleção
14.2.1 - Critérios Gerais

14.2.1.1. DO TRATAMENTO DIFERENCIADO ÀS MICROEMPRESAS, EMPRESAS DE PEQUENO PORTE E COOPERATIVA

1. As microempresas e empresas de pequeno porte, que se beneficiarem do regime diferenciado e favorecido concedido pela Lei Complementar n. 123 de 2006, por ocasião da participação neste certame licitatório, deverão apresentar toda a documentação exigida para habilitação, inclusive para efeito de comprovação de regularidade fiscal, mesmo que apresente alguma restrição.

2. Está vedada a participação de cooperativas nos termos da seção da vedação à participação de Cooperativas.

14.2.1.2. DA VEDAÇÃO À PARTICIPAÇÃO DE COOPERATIVAS

1. Fica vedada a participação de cooperativas por não atender aos termos do Artigo 10, inciso I da Instrução Normativa nº 05/2017:

> *Art. 10. A contratação de sociedades cooperativas somente poderá ocorrer quando, pela sua natureza, o serviço a ser contratado evidenciar:*

> *I - a possibilidade de ser executado com autonomia pelos cooperados, de modo a não demandar relação de subordinação entre a cooperativa e os cooperados, nem entre a Administração e os cooperados; e*
>
> *II - que a gestão operacional do serviço seja executada de forma compartilhada ou em rodízio, em que as atividades de coordenação e supervisão da execução dos serviços e as de preposto, conforme determina o art. 68 da Lei nº 8.666, de 1993, sejam realizadas pelos cooperados de* forma alternada ou aleatória, para que tantos quanto possíveis venham a assumir tal atribuição.

2. Avalia-se que no contexto do presente objeto há de se ter diversos perfis de conhecimento e funções distintas para o gerenciamento, desenvolvimento, análise, suporte técnico, operacionalização, treinamento, desenvolvimento de manutenções evolutivas e adaptativas, para a execução das atividades relacionadas à prestação de serviço, que guardam correlação técnica entre si, em função de sua interdependência a começar pelo fornecimento do licenciamento.

3. Portanto, neste caso, há falta de atendimento ao inciso I, o que impossibilita a participação de cooperativas.

14.2.1.3. REGIME DE EXECUÇÃO

1. O regime da execução dos contratos é de EMPREITADA POR PREÇO UNITÁRIO.

14.2.1.4. CRITÉRIO DE JULGAMENTO

1. O tipo e critério de julgamento da licitação é o MENOR PREÇO GLOBAL para a seleção da proposta mais vantajosa.

14.2.2 - Subcontratação

14.2.2.1. Não será permitida a subcontratação, no todo ou em parte, do objeto.

14.2.3 - Formação de Consórcios

14.2.3.1. Não será permitida formação de Consórcio.

14.2.4 - Alteração Subjetiva

14.2.4.1. É admissível a fusão, cisão ou incorporação da CONTRATADA com/por 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.

14.2.5 - Garantia Contratual

14.2.5.1. Não será exigida a prestação de garantia de execução para celebrar a contratação decorrente deste certame licitatório.

15 - ANEXOS DO TERMO DE REFERÊNCIA

ANEXO_A_Funcionalidades_mínimas_do_antivirus.pdf

Processo nº V-0066/2021

ANEXO A

CARACTERÍSTICAS E FUNCIONALIDADES MÍNIMAS DO SOFTWARE ANTIVÍRUS

ANEXO_A
CARACTERÍSTICAS E FUNCIUONALIDADES MÍNIMAS DO SOFTWARE ANTI-VÍRUS

1. Especificações técnicas da solução para ambiente Windows, Linux e Mobile.

1.1. Compatibilidade:

1.1.2. Microsoft Windows Server 2008 (Todas edições);
1.1.3. Microsoft Windows Server 2008 x64 SP1 (Todas edições);
1.1.4. Microsoft Windows Server 2008 R2 (Todas edições);
1.1.5. Microsoft Windows Server 2012 (Todas edições);
1.1.6. Microsoft Windows Server 2012 R2 (Todas edições);
1.1.7. Microsoft Windows Server 2016 x64
1.1.8. Microsoft Windows Small Business Server 2008 (Todas edições);
1.1.9. Microsoft Windows Small Business Server 2011 (Todas edições);
1.1.10. Microsoft Windows XP Professional SP2 ou superior;
1.1.10.1. Microsoft Windows XP Professional x64 SP2 ou superior;
1.1.11. Microsoft Windows Vista Business / Enterprise / Ultimate SP1 ou posterior;
1.1.12. Microsoft Windows Vista Business / Enterprise / Ultimate SP1 x64 ou posterior;
1.1.13. Microsoft Windows 7 SP1 Professional / Enterprise / Ultimate x32/x64;
1.1.14. Microsoft Windows 7 SP1 Professional / Enterprise / Ultimate x32/x64;
1.1.15. Microsoft Windows 8 SP1 Professional / Enterprise x32/x64;
1.1.16. Microsoft Windows 8 Professional / Enterprise x64;
1.1.17. Microsoft Windows 8.1 Professional / Enterprise x32;
1.1.18. Microsoft Windows 8.1 Professional / Enterprise x64;
1.1.19. Microsoft Windows 10 todas edições x32;
1.1.19.1.1. Microsoft Windows 10 todas edições x64;

Suporta as seguintes plataformas virtuais:

1.1.20. Vmware: Workstation 12.x Pro, vSphere 5.5, vSphere 6
1.1.21. Microsoft Hyper-V: 2008, 2008 R2, 2008 R2 SP1, 2012, 2012 R2;
1.1.22. Microsoft VirtualPC 6.0.156.0;
1.1.23. Parallels Desktop 7 e 11;
1.1.24. Oracle VM VirtualBox 4.0.4-70112 (Somente logon como convidado);
1.1.25. Citrix XenServer 6.2 e 6.5

Características:

1.1.26. A console deve ser acessada via WEB (HTTPS) ou MMC;
1.1.26.1. Console deve ser baseada no modelo cliente/servidor;
1.1.26.2. Compatibilidade com Windows Failover Clustering ou outra solução de alta disponibilidade;
1.1.26.3. Deve permitir a atribuição de perfis para os administradores da Solução de Antivírus;
1.1.27. Deve permitir incluir usuários do AD para logarem na console de administração
1.1.27.1. Console deve ser totalmente integrada com suas funções e módulos caso haja a necessidade no futuro de adicionar novas tecnologias tais como, criptografia, Patch management e MDM;
1.1.28. As licenças deverão ser perpétuas, ou seja, expirado a validade da mesma o produto deverá permanecer funcional para a proteção contra códigos maliciosos utilizando as definições até o momento da expiração da licença;
1.1.28.1. Capacidade de remover remotamente e automaticamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores;
1.1.28.2. Capacidade de instalar remotamente a solução de antivírus nas estações e servidores Windows, através de compartilhamento administrativo, login script e/ou GPO de Active Directory;
1.1.29. Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria;
1.1.30. Deve armazenar histórico das alterações feitas em políticas;
1.1.31. Deve permitir voltar para uma configuração antiga da política de acordo com o histórico de alterações efetuadas pelo administrador apenas selecionando a data em que a política foi alterada;
1.1.32. Deve ter a capacidade de comparar a política atual com a anterior, informando quais configurações foram alteradas;
1.1.33. A solução de gerencia deve permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas;
1.1.34. Através da solução de gerência, deve ser possível verificar qual licença está aplicada para determinado computador;
1.1.35. Capacidade de instalar remotamente a solução de segurança em smartphones e tablets de sistema iOS e Android;
1.1.36. Capacidade de instalar remotamente qualquer “app” em smartphones e tablets de sistema iOS;
1.1.37. A solução de gerência centralizada deve permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle;
1.1.38. Deverá ter a capacidade de criar regras para limitar o tráfego de comunicação cliente/servidor por subrede com os seguintes parâmetros: KB/s e horário;
1.1.38.1. Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux e Mac) protegidos pela solução antivírus;

1.1.38.2. Capacidade de gerenciar smartphones e tablets (Android e iOS) protegidos pela solução de segurança;

1.1.39. Capacidade de instalar atualizações em computadores de teste antes de instalar nos demais computadores da rede;

1.1.40. Capacidade de gerar pacotes customizados (auto executáveis) contendo a licença e configurações do produto;

1.1.41. Capacidade de atualizar os pacotes de instalação com as últimas vacinas;

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

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

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

1.1.44. Deve permitir a realocação de máquinas novas na rede para um determinado grupo sem ter um agente ou endpoint instalado utilizando os seguintes parâmetros:

1.1.44.1. Nome do computador;

1.1.44.2. Nome do domínio;

1.1.44.3. Range de IP;

1.1.44.4. Sistema Operacional;

1.1.44.5. Máquina virtual.

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

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

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

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

1.1.49. Capacidade de, assim que detectar máquinas novas no Active Directory, subnets ou grupos de trabalho, automaticamente importar a máquina para a estrutura de proteção da console e verificar se possui o antivírus instalado. Caso não possuir, deve instalar o antivírus automaticamente;

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

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

1.1.52. Deve fornecer as seguintes informações dos computadores:

1.1.52.1. Se o antivírus está instalado;
1.1.52.2. Se o antivírus está iniciado;
1.1.52.3. Se o antivírus está atualizado;
1.1.52.4. Minutos/horas desde a última conexão da máquina com o servidor administrativo;
1.1.52.5. Minutos/horas desde a última atualização de vacinas;
1.1.52.6. Data e horário da última verificação executada na máquina;
1.1.52.7. Versão do antivírus instalado na máquina;
1.1.52.8. Se é necessário reiniciar o computador para aplicar mudanças;
1.1.52.9. Data e horário de quando a máquina foi ligada;
1.1.52.10. Quantidade de vírus encontrados (contador) na máquina;
1.1.52.11. Nome do computador;
1.1.52.12. Domínio ou grupo de trabalho do computador;
1.1.52.13. Data e horário da última atualização de vacinas;
1.1.52.14. Sistema operacional com Service Pack;
1.1.52.15. Quantidade de processadores;
1.1.52.16. Quantidade de memória RAM;
1.1.52.17. Usuário(s) logado(s) naquele momento, com informações de contato (caso disponíveis no Active Directory);
1.1.52.18. Endereço IP;
1.1.52.19. Aplicativos instalados, inclusive aplicativos de terceiros, com histórico de instalação, contendo data e hora que o software foi instalado ou removido;
1.1.52.20. Atualizações do Windows Updates instaladas;
1.1.52.21. Informação completa de hardware contendo: processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de áudio, adaptadores de rede, monitores, drives de CD/DVD;
1.1.52.22. Vulnerabilidades de aplicativos instalados na máquina;
1.1.53. Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterá-las;
1.1.54. Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como:
1.1.54.1. Alteração de Gateway Padrão;
1.1.54.2. Alteração de subrede;
1.1.54.3. Alteração de domínio;
1.1.54.4. Alteração de servidor DHCP;
1.1.54.5. Alteração de servidor DNS;
1.1.54.6. Alteração de servidor WINS;
1.1.54.7. Alteração de subrede;
1.1.54.8. Resolução de Nome;
1.1.54.9. Disponibilidade de endereço de conexão SSL;
1.1.55. Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet;
1.1.56. Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes;

1.1.57. Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus;
1.1.58. Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos;
1.1.59. Capacidade de eleger qualquer computador cliente como repositório de vacinas e de pacotes de instalação, sem que seja necessária a instalação de um servidor administrativo completo, onde outras máquinas clientes irão atualizar-se e receber pacotes de instalação, a fim de otimizar tráfego da rede;
1.1.60. Capacidade de fazer deste repositório de vacinas um gateway para conexão com o servidor de administração, para que outras máquinas que não consigam conectar-se diretamente ao servidor possam usar este gateway para receber e enviar informações ao servidor administrativo;
1.1.61. Capacidade de exportar relatórios para pelo menos dois dos seguintes tipos de arquivos: PDF, HTML e XML;
1.1.62. Capacidade de gerar traps SNMP para monitoramento de eventos;
1.1.63. Capacidade de enviar e-mails para contas específicas em caso de algum evento;
1.1.64. Listar em um único local, todos os computadores não gerenciados na rede;
1.1.65. Deve encontrar computadores na rede através de no mínimo três formas: Domínio, Active Directory e subredes;
1.1.66. Deve possuir compatibilidade com Microsoft NAP, quando instalado em um Windows 2008 Server;
1.1.67. Capacidade de baixar novas versões do antivírus direto pela console de gerenciamento, sem a necessidade de importá-los manualmente
1.1.68. Capacidade de ligar máquinas via Wake on Lan para realização de tarefas (varredura, atualização, instalação, etc), inclusive de máquinas que estejam em subnets diferentes do servidor;
1.1.69. Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado intervalo de tempo);
1.1.70. Deve através de opções de optimizações fazer com que o computador gerenciado conceda recursos à outras aplicações, mantendo o antivírus ativo porém sem comprometer o desempenho do computador;
1.1.71. Deve permitir a configuração de senha no endpoint e configurar quando que será necessário a utilizá-la, (ex: Solicitar senha quando alguma tarefa de scan for criada localmente no endpoint);
1.1.72. Permitir fazer uma verificação rápida ou detalhada de um dispositivo removível assim que conectado no computador, podendo configurar a capacidade máxima em GB da verificação;
1.1.73. Deve ser capaz de configurar quais eventos serão armazenados localmente, nos eventos do windows ou ainda se serão mostrados na tela para o colaborador, sejam estes eventos informativos, de alertas ou de erros;
1.1.74. Capacidade de realizar atualização incremental de vacinas nos computadores clientes;

1.1.75. Deve armazenar localmente e enviar ao servidor de gerência a ocorrência de vírus com os seguintes dados, no mínimo:
   a) Nome do vírus;
   b) Nome do arquivo infectado;
   c) Data e hora da detecção;
   d) Nome da máquina ou endereço IP;
   e) Ação realizada.

1.1.76. Capacidade de reportar vulnerabilidades de softwares presentes nos computadores;

1.1.77. Capacidade de listar updates nas máquinas com o respectivo link para download

1.1.78. Deve criar um backup de todos arquivos deletados em computadores para que possa ser restaurado através de comando na Console de administração;

1.1.79. Deve ter uma quarentena na própria console de gerenciamento, permitindo baixar um artefato ou enviar direto para análise do fabricante;

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

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

1.1.82. Capacidade de diferenciar máquinas virtuais de máquinas físicas.

Funcionalidades Requeridas para estações Windows

Compatibilidade:

1.1.83. Microsoft Windows 7 Professional/Enterprise/Ultimate x86 / x64 e posterior;

1.1.83.1. Microsoft Windows 8 Professional/Enterprise x86 / x64;

1.1.84. Microsoft Windows 8.1 Pro / Enterprise x86 / x64;

1.1.85. Microsoft Windows 10 Pro / Enterprise x86 / x64;

1.1.86. Microsoft Windows Server 2012 R2 Standard x64;

1.1.87. Microsoft Windows Server 2012 Foundation x64;

1.1.88. Microsoft Windows Server 2012 Standard x64;

1.1.89. Microsoft Small Business Server 2011 Standard x64;

1.1.90. Microsoft Windows Server 2008 R2 Standard/Enterprise x64 SP1;

1.1.91. Microsoft Windows Server 2008 Standard/Enterprise x86/x64 SP2;

1.1.92. Microsoft Windows Server 2016 x64

Características:

1.1.93. Deve prover as seguintes proteções:

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

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

1.1.93.3. Antivírus de E-mail (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos);

1.1.93.4. O Endpoint deve possuir opção para rastreamento por linha de comando, parametrizável, com opção de limpeza;

1.1.93.5. Firewall com IDS;

1.1.93.6. Autoproteção (contra-ataques aos serviços/processos do antivírus);

1.1.93.7. Controle de dispositivos externos;

1.1.93.8. Controle de acesso a sites por categoria, ex: Bloquear conteúdo adulto, sites de jogos, etc;

1.1.93.9. Controle de acesso a sites por horário;

1.1.93.10. Controle de acesso a sites por usuários;

1.1.93.11. Controle de acesso a websites por dados, ex: Bloquear websites com conteúdos de vídeo e áudio;

1.1.93.12. Controle de execução de aplicativos;

1.1.93.13. Controle de vulnerabilidades do Windows e dos aplicativos instalados;

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

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

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

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

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

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

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

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

1.1.102. Ter a capacidade de fazer detecções por comportamento, identificando ameaças avançadas sem a necessidade de assinaturas;

1.1.103. Capacidade de verificar somente arquivos novos e alterados;

1.1.104. Capacidade de verificar objetos usando heurística;

1.1.105. Capacidade de agendar uma pausa na verificação;

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

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

1.1.108. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
1.1.108.1. Perguntar o que fazer, ou;
1.1.108.2. Bloquear acesso ao objeto;
1.1.108.2.1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
1.1.108.2.2. Caso positivo de desinfecção:
1.1.108.2.2.1. Restaurar o objeto para uso;
1.1.108.2.3. Caso negativo de desinfecção:
1.1.108.2.3.1. Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);
1.1.109. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
1.1.110. Capacidade de verificar e-mails recebidos e enviados nos protocolos POP3, IMAP, NNTP, SMTP e MAPI, assim como conexões criptografadas (SSL) para POP3 e IMAP (SSL);
1.1.111. Capacidade de verificar links inseridos em e-mails contra phishings;
1.1.112. Capacidade de verificar tráfego nos browsers: Internet Explorer, Firefox e Opera;
1.1.113. Capacidade de verificação de corpo e anexos de e-mails usando heurística;
1.1.114.
1.1.115. O antivírus de e-mail, ao encontrar um objeto potencialmente perigoso, deve:
1.1.115.1. Perguntar o que fazer, ou;
1.1.115.2. Bloquear o e-mail;
1.1.115.2.1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
1.1.115.2.2. Caso positivo de desinfecção:
1.1.115.2.2.1. Restaurar o e-mail para o usuário;
1.1.115.2.3. Caso negativo de desinfecção:
1.1.115.2.3.1. Mover para quarentena ou apagar o objeto (de acordo com a configuração pré-estabelecida pelo administrador);
1.1.116. Caso o e-mail conter código que parece ser, mas não é definitivamente malicioso, o mesmo deve ser mantido em quarentena;
1.1.117. Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados;
1.1.118. Capacidade de filtrar anexos de e-mail, apagando-os ou renomeando-os de acordo com a configuração feita pelo administrador;
1.1.119. Capacidade de verificação de tráfego HTTP e qualquer script do Windows Script Host (JavaScript, Visual Basic Script, etc), usando heurísticas;
1.1.120. Deve ter suporte total ao protocolo Ipv6;
1.1.121. Capacidade de alterar as portas monitoradas pelos módulos de Web e E-mail;

1.1.122. Na verificação de tráfego web, caso encontrado código malicioso o programa deve:

1.1.122.1. Perguntar o que fazer, ou;

1.1.122.2. Bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio, ou;

1.1.122.3. Permitir acesso ao objeto;

1.1.123. O antivírus de web deve realizar a verificação de, no mínimo, duas maneiras diferentes, sob escolha do administrador:

1.1.123.1. Verificação *on-the-fly*, onde os dados são verificados enquanto são recebidos em tempo-real, ou;

1.1.123.2. Verificação de *buffer*, onde os dados são recebidos e armazenados para posterior verificação;

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

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

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

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

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

1.1.129. Capacidade de distinguir diferentes subnets e conceder opção de ativar ou não o firewall para uma subnet específica;

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

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

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

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

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

1.1.132.1. Discos de armazenamento locais;

1.1.132.2. Armazenamento removível;

1.1.132.3. Impressoras;

1.1.132.4. CD/DVD;

1.1.132.5. Drives de disquete;
1.1.132.6. Modems;
1.1.132.7. Dispositivos de fita;
1.1.132.8. Dispositivos multifuncionais;
1.1.132.9. Leitores de smart card;
1.1.132.10. Dispositivos de sincronização via ActiveSync (Windows CE, Windows Mobile, etc);
1.1.132.11. Wi-Fi;
1.1.132.12. Adaptadores de rede externos;
1.1.132.13. Dispositivos MP3 ou smartphones;
1.1.132.14. Dispositivos Bluetooth;
1.1.132.15. Câmeras e Scanners.

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

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

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

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

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

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

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

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

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

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

Funcionalidades Requeridas para Estações Mac OS X

Compatibilidade:

1.1.143. Mac OS X 10.11 (El Capitan);

1.1.144. Mac OS X 10.10 (Yosemite);
1.1.145. Mac OS X 10.9 (Mavericks);
1.1.146. Mac OS X 10.8 (Mountain Lion);
1.1.147. Mac OS X 10.7 (Lion);
1.1.148. Mac OS Sierra 10.12

Características:

1.1.149. Deve prover proteção residente para arquivos (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
1.1.150. Possuir módulo de web-antivírus para proteger contra ameaças durante navegação na internet com possíbilidade de analisar endereços https;
1.1.151. Possuir módulo de bloqueio á ataques na rede;
1.1.152. Possibilidade de bloquear a comunicação entre a máquina atacante e os demais computadores por tempo definido pelo administrador;
1.1.153. Capacidade de criar exclusões para computadores que não devem ser monitorados pelo módulo de bloqueio à ataques na rede;
1.1.154. Possibilidade de importar uma chave no pacote de instalação;
1.1.155. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
1.1.156. A instalação e primeira execução do produto deve ser feita sem necessidade de reinicialização do computador, de modo que o produto funcione com toda sua capacidade;
1.1.157. Deve possuir suportes a notificações utilizando o Growl;
1.1.158. As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa);
1.1.159. Capacidade de voltar para a base de dados de vacina anterior;
1.1.160. Capacidade de varrer a quarentena automaticamente após cada atualização de vacinas;
1.1.161. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: “Win32.Trojan.banker”) para que qualquer objeto detectado com o veredicto escolhido seja ignorado;
1.1.162. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);
1.1.163. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;
1.1.164. Capacidade de verificar somente arquivos novos e alterados;
1.1.165. Capacidade de verificar objetos usando heurística;

1.1.166. Capacidade de agendar uma pausa na verificação;

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

1.1.167.1. Perguntar o que fazer, ou;

1.1.167.2. Bloquear acesso ao objeto;

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

1.1.167.2.2. Caso positivo de desinfecção:

1.1.167.2.2.1. Restaurar o objeto para uso;

1.1.167.2.3. Caso negativo de desinfecção:

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

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

1.1.169. Capacidade de verificar arquivos de formato de email;

1.1.170. Possibilidade de trabalhar com o produto pela linha de comando, com no mínimo opções para atualizar as vacinas, iniciar uma varredura, para o antivírus e iniciar o antivírus pela linha de comando;

1.1.171. Capacidade de ser instalado, removido e administrado pela mesma console central de gerenciamento.

Funcionalidades Requeridas para Estações de trabalho Linux

Compatibilidade:

1.1.172. Plataforma 32-bits:

1.1.172.1. Red Hat Enterprise Linux 6.7;

1.1.172.2. Red Hat Enterprise Linux 6.8;

1.1.172.3. CentOS-6.7;

1.1.172.4. CentOS-6.8;

1.1.172.5. Ubuntu 14.04 LTS;

1.1.172.6. Ubuntu 16.04 LTS;

1.1.172.7. Ubuntu 16.10 LTS;

1.1.172.8. Debian GNU/Linux 7.10;

1.1.172.9. Debian GNU/Linux 7.11;

1.1.172.10. Debian GNU/Linux 8.6;

1.1.172.11. Debian GNU/Linux 8.7.

1.1.173. Plataforma 64-bits:

1.1.173.1. Red Hat Enterprise Linux 6.7;

1.1.173.2. Red Hat Enterprise Linux 6.8;

1.1.173.3. Red Hat Enterprise Linux 7.2;

1.1.173.4. Red Hat Enterprise Linux 7.3;

1.1.173.5. CentOS-6.7;

1.1.173.6. CentOS-6.8;
1.1.173.7. CentOS-7.2;
1.1.173.8. CentOS-7.3;
1.1.173.9. Ubuntu 14.04 LTS;
1.1.173.10. Ubuntu 16.04 LTS;
1.1.173.11. Ubuntu 16.10 LTS;
1.1.173.12. Debian GNU/Linux 7.10;
1.1.173.13. Debian GNU/Linux 7.11;
1.1.173.14. Debian GNU/Linux 8.6;
1.1.173.15. Debian GNU/Linux 8.7;
1.1.173.16. OpenSUSE 42.2;
1.1.173.17. SUSE Linux Enterprise Server 12;
1.1.173.18. OracleLinux 7.3;
1.1.173.19. Novell Open Enterprise Server 11 SP3;
1.1.173.20. Novell Open Enterprise Server 2015 SP1

Características:

1.1.174. Deve prover as seguintes proteções:
1.1.175. Antivírus de arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
1.1.176. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;
1.1.177. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
1.1.178. Capacidade de criar exclusões por local, máscara e nome da ameaça;
1.1.179. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
1.1.180. Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;
1.1.181. Dectectar aplicações que possam ser utilizadas como vetor de ataque por hackers;
1.1.182. Fazer detecções através de heurística utilizando no mínimo as seguintes opções de nível:
1.1.182.1. Alta;
1.1.182.2. Média;
1.1.182.3. Baixa;
1.1.182.4. Recomendado;
1.1.183. Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;
1.1.184. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados.

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

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

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

1.1.188. Capacidade de verificar objetos usando heurística;

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

1.1.190. Possibilidade de

1.1.191. Deve possuir módulo escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).

Funcionalidades Requeridas para Servidores Windows

Compatibilidade:

1.1.192. Plataforma 32-bits:

1.1.192.1. Windows Server 2008 Standard/Enterprise/Datacenter SP1 e posterior;

1.1.192.2. Windows Server 2008 Core Standard/Enterprise/Datacenter SP1 e posterior

1.1.193. Plataforma 64-bits

1.1.194. Microsoft Windows Server 2008 Standard / Enterprise / DataCenter (SP1 ou posterior);

1.1.195. Microsoft Windows Server 2008 Core Standard / Enterprise / DataCenter (SP1 ou posterior).

1.1.196. Microsoft Windows Server 2008 R2 Standard / Enterprise / DataCenter (SP1 ou posterior);

1.1.197. Microsoft Windows Server 2008 R2 Core Standard / Enterprise / DataCenter (SP1 ou posterior);

1.1.198. Microsoft Windows Storage Server 2008 R2;

1.1.199. Microsoft Windows Storage Server 2008 SP2 Standard Edition;

1.1.200. Microsoft Windows Storage Server SP2 Workgroup Edition;

1.1.201. Microsoft Windows Hyper-V Server 2008 R2 SP1 e posterior;

1.1.202. Microsoft Windows Server 2012 Essentials / Standard / Foundation / Datacenter;

1.1.203. Microsoft Windows Server 2012 R2 Essentials / Standard / Foundation / Datacenter;

1.1.204. Microsoft Windows Server 2012 Core Essentials / Standard / Foundation / Datacenter;
1.1.205. Microsoft Windows Server 2012 R2 Core Essentials / Standard / Foundation / Datacenter;
1.1.206. Microsoft Windows Storage Server 2012 (Todas edições);
1.1.207. Microsoft Windows Storage Server 2012 R2 (Todas edições);
1.1.208. Microsoft Windows Hyper-V Server 2012;
1.1.209. Microsoft Windows Hyper-V Server 2012 R2;
1.1.210. Windows Server 2016 Essentials/Standard/Datacenter/Core;
1.1.211. Windows Storage Server 2016;
1.1.212. Windows Hyper-V Server 2016.

Características:

1.1.213. Deve prover as seguintes proteções:
1.1.213.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
1.1.213.2. Auto-proteção contra-ataques aos serviços/processos do antivírus;
1.1.213.3. Firewall com IDS;
1.1.213.4. Controle de vulnerabilidades do Windows e dos aplicativos instalados;
1.1.214. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
1.1.215. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;
1.1.216. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
1.1.216.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
1.1.216.2. Gerenciamento de tarefa (criar ou excluir tarefas de verificação);
1.1.216.3. Leitura de configurações;
1.1.216.4. Modificação de configurações;
1.1.216.5. Gerenciamento de Backup e Quarentena;
1.1.216.6. Visualização de relatórios;
1.1.216.7. Gerenciamento de relatórios;
1.1.216.8. Gerenciamento de chaves de licença;
1.1.216.9. Gerenciamento de permissões (adicionar/excluir permissões acima);
1.1.217. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:
1.1.217.1. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;
1.1.217.2. Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.

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

1.1.219. Bloquear malwares tais como Cryptlockers mesmo quando o ataque vier de um computador sem antivírus na rede

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

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

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

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

1.1.224. Capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado no servidor;

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

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

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

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

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

1.1.230. Capacidade de verificar somente arquivos novos e alterados;

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

1.1.232. Capacidade de verificar objetos usando heurística;

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

1.1.234. Capacidade de agendar uma pausa na verificação;

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

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

1.1.236.1. Perguntar o que fazer, ou;
1.1.236.2. Bloquear acesso ao objeto;
1.1.236.2.1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
1.1.236.2.2. Caso positivo de desinfecção:
1.1.236.2.2.1. Restaurar o objeto para uso;
1.1.236.2.3. Caso negativo de desinfecção:
1.1.236.2.3.1. Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);

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

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

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

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

Funcionalidades Requeridas para Servidores Linux

Compatibilidade:

Plataforma 32-bits:

1.1.241. Red Hat Enterprise Linux 6.7;
1.1.242. Red Hat Enterprise Linux 6.8;
1.1.243. CentOS-6.7;
1.1.244. CentOS-6.8;
1.1.245. Ubuntu 14.04 LTS;
1.1.246. Ubuntu 16.04 LTS;
1.1.247. Ubuntu 16.10 LTS;
1.1.248. Debian GNU/Linux 7.10;
1.1.249. Debian GNU/Linux 7.11;
1.1.250. Debian GNU/Linux 8.6;
1.1.251. Debian GNU/Linux 8.7.

Plataforma 64-bits:

1.1.252. Red Hat Enterprise Linux 6.7;
1.1.253. Red Hat Enterprise Linux 6.8;
1.1.254. Red Hat Enterprise Linux 7.2;
1.1.255. Red Hat Enterprise Linux 7.3;
1.1.256. CentOS-6.7;
1.1.257. CentOS-6.8;
1.1.258. CentOS-7.2;
1.1.259. CentOS-7.3;

1.1.260. Ubuntu 14.04 LTS;
1.1.261. Ubuntu 16.04 LTS;
1.1.262. Ubuntu 16.10 LTS;
1.1.263. Debian GNU/Linux 7.10;
1.1.264. Debian GNU/Linux 7.11;
1.1.265. Debian GNU/Linux 8.6;
1.1.266. Debian GNU/Linux 8.7;
1.1.267. OpenSUSE 42.2;
1.1.268. SUSE Linux Enterprise Server 12;
1.1.269. OracleLinux 7.3;
1.1.270. Novell Open Enterprise Server 11 SP3;
1.1.271. Novell Open Enterprise Server 2015 SP1;

Características:

1.1.272. Deve prover as seguintes proteções:
1.1.273. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
1.1.274. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;
1.1.275. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
1.1.276. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
1.1.277. Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;
1.1.278. Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;
1.1.279. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados;
1.1.279.1. Em caso erros, deve ter capacidade de criar *logs* automaticamente, sem necessidade de outros softwares;
1.1.280. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
1.1.281. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;
1.1.282. Capacidade de verificar objetos usando heurística;
1.1.283. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;

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

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

Funcionalidades Requeridas para Smartphones e tablets

Compatibilidade:

1.1.285. Apple iOS 9.0-10.3;

1.1.286. Android 4.1 – 7.1.1

Características:

1.1.287. Deve prover as seguintes proteções:

1.1.287.1. Proteção em tempo real do sistema de arquivos do dispositivo – interceptação e verificação de:

1.1.287.2. Proteção contra adware e autodialers;

1.1.287.3. Todos os objetos transmitidos usando conexões wireless (porta de infravermelho, Bluetooth) e mensagens EMS, durante sincronismo com PC e ao realizar download usando o browser;

1.1.287.4. Arquivos abertos no smartphone;

1.1.287.5. Programas instalados usando a interface do smartphone

1.1.287.6. Verificação dos objetos na memória interna do smartphone e nos cartões de expansão sob demanda do usuário e de acordo com um agendamento;

1.1.288. Deverá isolar em área de quarentena os arquivos infectados;

1.1.289. Deverá atualizar as bases de vacinas de modo agendado;

1.1.290. Deverá bloquear spams de SMS através de Black lists;

1.1.291. Deverá ter função de bloqueio do aparelho caso o SIM CARD for trocado para outro não autorizado com mensagem de aviso ao utilizador do dispositivo;

1.1.292. Capacidade de desativar por política:

Wi-fi;

Câmera;

Bluetooth.

1.1.293. Deverá ter função de limpeza de dados pessoais a distância, em caso de roubo, por exemplo;

1.1.294. Capacidade de requerer uma senha para desbloquear o dispositivo e personalizar a quantidade de caracteres para esta senha;

1.1.295. Deverá ter firewall pessoal (Android);

1.1.296. Capacidade de tirar fotos quando a senha for inserida incorretamente;

1.1.297. Possibilidade de instalação remota utilizando o Microsoft System Center Mobile Device Manager 2008 SP1;

1.1.298. Capacidade de enviar comandos remotamente de:

1.1.298.1. Localizar;

1.1.298.2. Bloquear.

1.1.299. Capacidade de detectar Jailbreak em dispositivos iOS;

1.1.300. Capacidade de bloquear o acesso a site por categoria em dispositivos;

1.1.301. Capacidade de bloquear o acesso a sites phishing ou malicioso;

1.1.302. Capacidade de criar containers de aplicativos, separando dados corporativos de dados pessoais;

1.1.303. Capacidade de bloquear o dispositivo quando o cartão "SIM" for substituído;

1.1.304. Capacidade de configurar White e blacklist de aplicativos;

1.1.305. Capacidade de localizar o dispositivo quando necessário;

1.1.306. Permitir atualização das definições quando estiver em "roaming";

1.1.307. Capacidade de selecionar endereço do servidor para buscar a definição de vírus;

1.1.308. Deve permitir verificar somente arquivos executáveis;

1.1.309. Deve ter a capacidade de desinfectar o arquivo se possível;

1.1.310. Capacidade de agendar uma verificação;

1.1.311. Capacidade de enviar URL de instalação por e-mail;

1.1.312. Capacidade de fazer a instalação através de um link QRCode;

1.1.313. Capacidade de executar as seguintes ações caso a desinfecção falhe:

1.1.313.1. Deletar;

1.1.313.2. Ignorar;

1.1.313.3. Quarentenar;

1.1.313.4. Perguntar ao usuário.

Funcionalidades Requeridas para Gerenciamento de dispositivos móveis (MDM)

Compatibilidade:

1.1.314. Dispositivos conectados através do Microsoft Exchange ActiveSync:

1.1.314.1. Apple iOS;

1.1.314.2. Android.

1.1.315. Dispositivos com suporte ao Apple Push Notification (APNs).

1.1.315.1. Apple iOS 3.0 ou superior.

Características:

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

1.1.317. Capacidade de ajustar as configurações de:

1.1.317.1. Sincronização de e-mail;

1.1.317.2. Uso de aplicativos;

1.1.317.3. Senha do usuário;

1.1.317.4. Criptografia de dados;

1.1.317.5. Conexão de mídia removível.

1.1.318. Capacidade de instalar certificados digitais em dispositivos móveis;
1.1.319. Capacidade de, remotamente, resetar a senha de dispositivos iOS;
1.1.320. Capacidade de, remotamente, apagar todos os dados de dispositivos iOS;
1.1.321. Capacidade de, remotamente, bloquear um dispositivo iOS;
1.1.322. Deve permitir configurar horário para sincronização do dispositivo com a console de gerenciamento;
1.1.323. Possibilidade de exigir senha para abrir aplicações instaladas em container;
1.1.324. Deve permitir que o usuário utilize autenticação do Active Directory para abrir aplicações em container;
1.1.325. Deve permitir que uma senha seja digitada a cada x(minutos) para continuar utilizando uma aplicação em container;
1.1.326. Deve permitir a criptografia de dados salvos pelas aplicações em container;
1.1.327. Permitir sincronização com perfil do “Touch Down”;
1.1.328. Capacidade de desinstalar remotamente o antivírus do dispositivo;
1.1.329. Deve permitir fazer o upgrade do antivírus de forma remota sem a necessidade de desinstalar a versão atual;
1.1.330. Capacidade de sincronizar com Samsung Knox;
1.1.331. Deve permitir criar perfis de políticas para out-of-office no caso de BYOD.

Funcionalidades Requeridas de Criptografia

Compatibilidade

1.1.332. Microsoft Windows 7 Ultimate SP1 ou superior x86/x64;
1.1.333. Microsoft Windows 7 Enterprise SP1 ou superior x86/x64;
1.1.334. Microsoft Windows 7 Professional SP1 ou superior x86/x64;
1.1.335. Microsoft Windows 8 Enterprise x86/x64;
1.1.336. Microsoft Windows 8 Pro x86/x64;
1.1.337. Microsoft Windows 8.1 Pro x86/x64;
1.1.338. Microsoft Windows 8.1 Enterprise x86/x64;
1.1.339. Microsoft Windows 10 Enterprise x86/x64;
1.1.340. Microsoft Windows 10 Pro x86/x64;
1.1.341. Microsoft Windows Vista x86/x64 SP2 ou superior;
1.1.342. Microsoft Windows XP Professional x86 SP3 ou superior

Características

1.1.343. O acesso ao recurso criptografado (arquivo, pasta ou disco) deve ser garantido mesmo em caso o usuário tenha esquecido a senha, através de procedimentos de recuperação;

1.1.344. Utilizar, no mínimo, algoritmo AES com chave de 256 bits;

1.1.345. Capacidade de criptografar completamente o disco rígido da máquina, adicionando um ambiente de pré-boot para autenticação do usuário;

1.1.346. Capacidade de utilizar *Single Sign-On* para a autenticação de pré-boot;

1.1.347. Permitir criar vários usuários de autenticação pré-boot;

1.1.348. Capacidade de criar um usuário de autenticação pré-boot comum com uma senha igual para todas as máquinas a partir da console de gerenciamento;

1.1.349. Capacidade de criptografar drives removíveis de acordo com regra criada pelo administrador, com as opções:

1.1.349.1. Criptografar somente os arquivos novos que forem copiados para o disco removível, sem modificar os arquivos já existentes;

1.1.349.2. Criptografar todos os arquivos individualmente;

1.1.349.3. Criptografar o dispositivo inteiro, de maneira que não seja possível listar os arquivos e pastas armazenadas;

1.1.349.4. Criptografar o dispositivo em modo portátil, permitindo acessar os arquivos em máquinas de terceiros através de uma senha;

1.1.350. Capacidade de selecionar pastas e arquivos (por tipo, ou extensão) para serem criptografados automaticamente. Nesta modalidade, os arquivos devem estar acessíveis para todas as máquinas gerenciadas pela mesma console de maneira transparente para os usuários;

1.1.351. Capacidade de criar regras de exclusões para que certos arquivos ou pastas nunca sejam criptografados;

1.1.352. Capacidade de selecionar aplicações que podem ou não ter acesso aos arquivos criptografados;

1.1.353. Verifica compatibilidade de hardware antes de aplicar a criptografia;

1.1.354. Possibilita estabelecer parâmetros para a senha de criptografia;

1.1.355. Bloqueia o reuso de senhas;

1.1.356. Bloqueia a senha após um número de tentativas pré-estabelecidas;

1.1.357. Capacidade de permitir o usuário solicitar permissão a determinado arquivo criptografado para o administrador mediante templates customizados;

1.1.358. Permite criar exclusões para não criptografar determinados “discos rígidos” através de uma busca por nome do computador ou nome do dispositivo

1.1.359. Permite criptografar as seguintes pastas pré-definidas: “meus documentos”, “Favoritos”, “Desktop”, “Arquivos temporários” e “Arquivos do outlook”;

1.1.360. Permite utilizar variáveis de ambiente para criptografar pastas customizadas;

1.1.361. Capacidade de criptografar arquivos por grupos de extensão, tais como: Documentos do office, Document, arquivos de audio, etc;

1.1.362. Permite criar um grupo de extensões de arquivos a serem criptografados;

1.1.363. Capacidade de criar regra de criptografia para arquivos gerados por aplicações;
1.1.364. Permite criptografia de dispositivos móveis mesmo quando o endpoint não possuir comunicação com a console de gerenciamento.
1.1.365. Capacidade de deletar arquivos de forma segura após a criptografia;
1.1.366. Capacidade de criptografar somente o espaço em disco utilizado;
1.1.367. Deve ter a opção de criptografar arquivos criados a partir de aplicações selecionadas pelo administrador;
1.1.368. Capacidade de bloquear aplicações selecionadas pelo administrador de acessarem arquivos criptografados;
1.1.369. Deve permitir criptografar somente o espaço utilizado em dispositivos removíveis tais como pendrives, HD externo, etc;
1.1.370. Capacidade de criptografar discos utilizando a criptografia BitLocker da Microsoft;
1.1.371. Deve ter a opção de utilização de TPM para criptografia através do BitLocker;
1.1.372. Capacidade de fazer “Hardware encryption”;

Funcionalidades Requeridas para Gerenciamento de Sistemas

1.1.373. Capacidade de criar imagens de sistema operacional remotamente e distribuir essas imagens para computadores gerenciados pela solução e para computadores *bare-metal*;
1.1.374. Deve possibilitar a utilização de servidores PXE na rede para deploy de imagens;

1.1.375. Capacidade de detectar softwares de terceiros vulneráveis, criando assim um relatório de softwares vulneráveis;
1.2. Capacidade de corrigir as vulnerabilidades de softwares, fazendo o download centralizado da correção ou atualização e aplicando essa correção ou atualização nas máquinas gerenciadas de maneira transparente para os usuários;
1.3. Capacidade de gerenciar licenças de softwares de terceiros;
1.4. Capacidade de registrar mudanças de hardware nas máquinas gerenciadas;
1.5. Capacidade de gerenciar um inventário de hardware, com a possibilidade de cadastro de dispositivos (ex: router, switch, projetor, acessório, etc), informando data de compra, local onde se encontra, service tag, número de identificação e outros;
1.6. Possibilita fazer distribuição de software de forma manual e agendada;
1.7. Suporta modo de instalação silenciosa;
1.8. Suporte a pacotes MSI, exe, bat, cmd e outros padrões de arquivos executáveis;
1.9. Possibilita fazer a distribuição através de agentes de atualização;
1.10. Utiliza tecnologia multicast para evitar tráfego na rede;
1.11. Possibilita criar um inventário centralizado de imagens;
1.12. Capacidade de atualizar o sistema operacional direto da imagem mantendo os dados do usuário;
1.13. Suporte a WakeOnLan para deploy de imagens;

1.14. Capacidade de atuar como servidor de atualização do Windows podendo fazer deploy de patches;
1.15. Suporta modo de teste, podendo atribuir alguns computadores para receberem as atualizações de forma automática para avaliação de alterações no comportamento;
1.16. Capacidade de gerar relatórios de vulnerabilidades e patches;
1.17. Possibilita criar exclusões para aplicação de patch por tipo de sistema operacional, Estação de trabalho e Servidor ou por grupo de administração;
1.18. Permite iniciar instalação de patch e correções de vulnerabilidades ao reiniciar ou desligar o computador;
1.19. Permite baixar atualizações para o computador sem efetuar a instalação
1.20. Permite o administrador instalar somente atualizações aprovadas, instalar todas as atualizações (exceto as bloqueadas) ou instalar todas as atualizações incluindo as bloqueadas;
1.21. Capacidade de instalar correções de vulnerabilidades de acordo com a severidade;
1.22. Permite selecionar produtos a serem atualizados pela console de gerenciamento;
1.23. Permite selecionar categorias de atualizações para serem baixadas e instaladas, tais como: atualizações de segurança, ferramentas, drivers, etc;
1.24. Capacidade de adicionar caminhos específicos para procura de vulnerabilidades e atualizações em arquivos;
1.25. Capacidade de instalar atualizações ou correções somente em computadores definidos, em grupos definidos ou em uma porcentagem de computadores conforme selecionado pelo administrador;
1.26. Capacidade de configurar o reinicio do computador após a aplicação das atualizações e correções de vulnerabilidades;
1.27. Deve permitir selecionar o idioma das aplicações que serão atualizadas;
1.28. Permitir agendar o sincronismo entre a console de gerenciamento e os sites da Microsoft para baixar atualizações recentes;

SERVIÇO PÚBLICO FEDERAL
CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA DO ESTADO DE SÃO PAULO

CREA-SP

TERMO DE REFERÊNCIA

INTRODUÇÃO

A presente análise tem por objetivo descrever os elementos necessários e suficientes, com nível de precisão adequado, para subsidiar o processo licitatório, demonstrando sua viabilidade e conveniência. Seu conteúdo dependerá da natureza da solução a ser licitada, sendo mais complexo e minucioso na medida em que a contratação assim exigir. Ele será elaborado com base nas informações constantes do Estudo Técnico preliminar.

1 - OBJETO DA CONTRATAÇÃO

1.1. Constitui objeto da presente licitação a contratação de empresa especializada em fornecimento de serviços de atualização das licenças para ao Antivírus Kaspersky, com suporte e capacitação.

2 - JUSTIFICATIVA E FUNDAMENTAÇÃO DA CONTRATAÇÃO

2.1. OBJETIVO DA CONTRATAÇÃO

1. Renovação das Licenças para a atualização de assinaturas de vírus e ameaças utilizadas no antivírus que o CREA-SP atualmente possui instalado em seus computadores, bem como fornecer o suporte adequado e a capacitação para operar o sistema.

2.2. DA JUSTIFICATIVA PARA LOTE ÚNICO

1. A opção por lote único está fundamentada na IN 05/2017-SLTI/MPOG, onde admite-se a aquisição por lote único quando, comprovada e justificadamente, for tecnicamente inviável o parcelamento, por haver inter-relação entre os serviços contratados, gerenciamento centralizado ou implicar em vantagem para a Administração, requisitos que serão comprovados adiante.

2. Quando analisado sob os aspectos técnicos, tem-se configurado o inter-relacionamento e a interdependência entre os serviços a serem contratados, uma vez que não é possível estabelecer os limites, por serem extremamente tênues, de onde se iniciam e terminam as repercussões entre um e outro, especialmente por se ter como meta alcançar a maturidade do ambiente como um todo, a alta disponibilidade e a gestão de riscos da contratação e dos negócios.

3. Além disso, o agrupamento dos itens em Grupo Único é imprescindível, pois em se tratando de gestão contratual torna-se inviável que os serviços associados sejam fornecidos por diferentes fornecedores, dado que traz maior custo de gestão e controle deste Órgão.

4. Em se tratando do viés econômico, o parcelamento dos serviços associados do objeto pode impactar diretamente os custos da contratação, considerando que a execução desses serviços por uma única empresa se traduz em diluição do custo administrativo da empresa possibilitando menor preço global.

5. Neste sentido, o objeto possui características de dependências entre os serviços a serem prestados, sendo certo que seu parcelamento aumentaria os riscos de execução insatisfatória do serviço.

6. A aquisição em lote único embasa-se no Parecer no 2086/00, elaborado no Processo no 194/2000 do TCDF, da lavra do Professor Jorge Ulisses Jacoby Fernandes e outros doutrinadores a seguir citados:

> “a regra do parcelamento deve ser coordenada com o requisito que a própria lei definiu: só se pode falar em parcelamento quando há viabilidade técnica para sua adoção. (...) Um exame atento dos tipos de objeto licitados pela Administração Pública evidência que embora sejam divisíveis, há interesse técnico na manutenção unicidade, da licitação ou do item dela. Não é, pois, a simples divisibilidade, mas a viabilidade técnica que dirige processo decisório. (...) Se um objeto, divisível, sob o aspecto econômico for mais vantajoso, mas houver inviabilidade técnica em que seja licitado em separado, de nada valerá a avaliação econômica. Imagine-se ainda esse elementar exemplo do automóvel: se por exemplo as peças isoladamente custassem mais barato, mesmo assim, seria recomendável o não parcelamento, pois sob o aspecto técnico é a visão do conjunto que iria definir a garantia do fabricante, o ajuste das partes compondo todo único, orgânico e harmônico".
>
> “Segundo Marçal Justen Filho, "a obrigatoriedade do fracionamento respeita limites de ordem técnica econômica. Não se admite o fracionamento quando tecnicamente isso não for viável ou, mesmo, recomendável. O fracionamento em lotes deve respeitar a integridade qualitativa do objeto a ser executado. (...) a unidade do objeto a ser executado não pode ser destruída através do fracionamento" (JUSTEN FILHO, Marçal. Comentários à Lei de Licitações e Contratos Administrativos. 11.ed. Brasília: 2005, Dialética.
>
> “Carvalho Carneiro esclarece acerca do conceito de viabilidade técnica e econômica, informando que a viabilidade técnica diz respeito à integridade do objeto, não se admitindo o parcelamento quando tal medida implicar na sua desnaturação, onde em risco a satisfação do interesse público em questão” (CARNEIRO, Daniel Carvalho. O parcelamento da contratação na lei de licitações. Revista Diálogo Jurídico, ano IV, n.3., setembro/2004, p.85/95).

7. Ao se avaliar tecnicamente há uma intensa correlação dos serviços prestados com a disponibilização do licenciamento da solução, a qual necessita-se de profissionais que trabalhem de forma integrada, que entendam do objeto a ser contratado de forma a se ter treinamento, suporte técnico e manutenções evolutivas e adaptativas com qualidade, bem como explorar melhor forma as capacidades da solução para atendimento às necessidades deste CREA-SP.

8. Assim, os itens que compõem a solução devem ser fornecidos em Grupo Único, pelo mesmo licitante ou fornecedor, pois somente assim haverá melhor prestação dos serviços associados, com melhoria da gestão contratual por parte deste CREA-SP.

9. Nesse sentido, a opção deste Órgão respeita a legislação vigente e busca aliar tecnicamente e economicamente os aspectos da gestão contratual.

10. Pode-se inferir que está contratação é técnica e economicamente viável e que haverá diminuição do custo administrativo das empresas participantes por diluição em serviços agregados. Já para este CREA-SP haverá diminuição no custo de gestão contratual ao gerenciar uma empresa, ao invés de várias empresas.

11. Por fim, avalia-se que também haverá melhor aproveitamento do mercado e ampliação da competitividade.

2.3. DA FUNDAMENTAÇÃO LEGAL

1. A presente licitação, que trata da contratação do objeto deste Termo de Referência e seus anexos será realizada conforme regulamentação da Lei no 8.666/93.

2. O objeto a ser contratado configura serviço de natureza continuada, nos termos da Instrução nº 2.594/2018 do CREA-SP, de 23 de abril de 2018, e será prestado no prazo de 36 (trinta e seis) meses, podendo haver prorrogação do contrato conforme a previsão do artigo 57, Inciso IV da Lei nº 8.666/1993 e se enquadra no conceito de serviço comum, nos termos da Lei 10.520/02, onde os requisitos técnicos são suficientes para determinar o conjunto da solução escolhida, constatando-se, ainda, que a solução é fornecida por mais de uma empresa no mercado.

3. Instrução Normativa SLTI/ME nº 01/2010, que dispõe sobre os critérios de sustentabilidade ambiental na aquisição de bens, contratação de serviços ou obras pela Administração Pública Federal direta;

4. Portaria ME nº 443, de 27 de dezembro de 2018, que dispõe sobre os serviços que deverão ser preferencialmente objeto de execução indireta;

5. Instrução Normativa SGD/ME nº 01, de 4 de abril de 2019, que dispõe sobre as contratações de soluções de TIC;

6. Instrução Normativa SGD/ME nº 73, de 05 de agosto de 2020, que dispõe sobre pesquisa de preços para contratações pela administração pública federal.

3 - DESCRIÇÃO DA SOLUÇÃO

3.1. COMPOSIÇÃO DA SOLUÇÃO

Item	Descrição	Código	Qtde.	Unidade
1	Licenças de Antivírus denominadas pelo fabricante de: "Kaspersky Endpoint Security for Business - Advanced Renewal 3 year Band V: 1000-1499"	KL4867KAVTR	1.369	Licenças
2	Capacitação de implantação, configuração e gerenciamento da solução.	KL 002.11.6	4	Pessoas
3	Capacitação em gerenciamento de vulnerabilidades a atualizações de software e integração com o sistema SIEM	KL 009.12	4	Pessoas
4	Serviço de Suporte 8x5, monitoramento, atualização do servidor e clientes.	N.A.	36	Meses

4 - ESTIMATIVA DAS QUANTIDADES

Estimativa da quantitativo de Licenças

Da quantidade de Estações de Trabalho

A equipe de planejamento, consultou o contrato de locação de computadores e notebooks C-027 / 2018 e verificou que atualmente o CREA-SP conta com um contingente, efetivamente instalado, de:

- 910 Desktops com 8GB de memória
- 170 Desktops com 4GB de memória
- 150 Notebooks com 8GB de memória.

Totalizando 1230 equipamentos.

Da quantidade de Servidores

O CREA-SP possui ativos e funcionando um total de 139 Servidores.

Desta forma, há necessidade de 139 licenças para cobrir todo o parque instalado de servidores.

Da quantidade total de Licenças

Somando-se a quantidade de licenças de estações de trabalho (1230), com as licenças de servidores (139) chegamos a um total de **1369** licenças.

Estimativa de quantitativo de capacitação

Atualmente a equipe de suporte do CREA/SP conta com 4 (quatro) analistas e 2 (dois) técnicos.

A equipe que vai efetivamente trabalhar com o antivírus: dois analistas que pertencem a equipe de atualização/segurança e dois técnicos que pertence a equipe de atendimento ao usuário:

Desta forma há necessidade de contratação de capacitação para 4 (quatro) funcionários efetivos do CREA-SP.

5 - PLANILHA PARA COTAÇÃO DE PREÇO

Item	Descrição	Código	Qtde	Unidade	Valor Unitário	Valor Total
1	Licenças de Antivírus denominadas pelo fabricante de: "Kaspersky Endpoint Security for Business - Advanced Renewal 3 year Band V: 1000-1499"	KL4867KAVTR	1.369	Licenças	R$	R$
2	Capacitação de implantação, configuração e gerenciamento da solução.	KL 002.11.6	4	Pessoas	R$	R$
3	Capacitação em gerenciamento de vulnerabilidades a atualizações de software e integração com o sistema SIEM	KL 009.12	4	Pessoas	R$	R$
4	Serviço de Suporte 8x5, monitoramento, atualização do servidor e clientes.	N.A.	36	Meses	R$	R$
TOTAL GERAL.....						R$

6 - ESPECIFICAÇÃO TÉCNICA

6.1. DESCRIÇÃO DA SOLUÇÃO

1. A Solução contratada constitui-se de produtos e serviços.

2. O produto aqui considerado é a licença que permite a renovação dos bancos de dados de vírus utilizados pelo software da Kaspersky e sua constante atualização durante o prazo da contratação.

3. Os serviços aqui considerados são a capacitação dos profissionais técnicos do CREA-SP e o suporte continuado que a empresa contratada deverá prestar durante a vigência contratual.

6.1.1. DESCRIÇÃO DO PRODUTO - Kaspersky Endpoint Security for Business - Advanced Renewal

Estas Licenças devem possibilitar ao CREA-SP, através do console de gerenciamento e dos softwares clientes instalados nos computadores, usufruir e utilizar as funcionalidades descritas no ANEXO_A_Funcionalidades_mínimas_do_antivirus.pdf.

6.1.2. DESCRIÇÃO DOS SERVIÇOS

1. Este termo de referência descreve dois tipos de serviços que serão contratados:

a. Serviços de Capacitação;

b. Serviços de Suporte;

6.1.2.1. DESCRIÇÃO DOS SERVIÇOS DE SUPORTE

1. O Contrato de suporte consiste no monitoramento pró-ativo e atendimento reativo às solicitações do CREA-SP. A demanda ou solicitação deverá ser realizada através de abertura de chamado pelo CREA-SP, descrevendo a atividade ou suporte necessário, que serão atendidas por profissionais qualificados para o exercício de atividades compatíveis com os tipos de servidores ou dispositivos na rede, levando sempre em consideração as características e limitações dos produtos suportados.

2. O CREA-SP poderá utilizar qualquer combinação dos seguintes Serviços descritos abaixo.

6.1.2.1.1. GERENCIAMENTO DA CONTA DE SUPORTE

1. Os serviços de Gerenciamento de Conta de Suporte são planejados para ajudar na coordenação da relação de suporte e de serviços.

2. A CONTRATADA deverá possuir um representante dos serviços de suporte, o qual chamaremos de Gerente Técnico de Suporte. Este Gerente é o representante do CREA dentro da CONTRATADA, e coordenará a equipe que fornecerá os Serviços de Solução de Problemas.

6.1.2.1.1.1. ATIVIDADES DO GERENTE TÉCNICO DE SUPORTE

1. O Gerente Técnico de Suporte também realizará as seguintes atividades:

a. O Gerente Técnico de Suporte funcionará como canal de comunicação e pode ainda transmitir a percepção do CREA-SP, com relação aos Serviços, para outras instâncias dentro da CONTRATADA.

b. Reunião de Orientação e Planejamento, também denominada reunião inicial do Contrato, ou reunião de “Kick off", a qual está descrita neste termo de referência.

c. Gerenciamento de Escalação. Questões de suporte que requerem o envolvimento de diversos profissionais e níveis hierárquicos podem ser gerenciadas de perto pelo Gerente Técnico de Suporte ou outro representante para acelerar a solução.

6.1.2.1.2. SERVIÇOS DE SUPORTE AO SOFTWARE

1. Nesta modalidade de serviço, no decorrer do período de duração do contrato, a CONTRATADA irá atuar na resolução dos problemas relativos ao Antivírus instalado no CREA-SP, tanto no Servidor, quanto nos clientes, os quais utilizam as licenças contratadas e fornecidas. Conforme os seguintes requisitos:

6.1.2.2 DESCRIÇÃO DOS SERVIÇOS DE CAPACITAÇÃO

1. A CONTRATADA deverá fornecer a capacitação solicitada a quatro membros da equipe de Sustentação de TI do CREA. Através de treinamentos de instalação e operação do ambiente e do sistema de Antivírus atrelado às licenças de software atualizadas, nas versões fornecidas pela CONTRATADA.

2. A CONTRATADA deverá fornecer a transferência de conhecimento sobre o ambiente atualizado do CREA-SP em até 10 dias depois da finalização dos serviços de atualização do Servidor e dos Clientes. Os serviços de transferência de conhecimento devem ser executados remotamente e não devem gerar nenhum ônus financeiro ao CREA-SP.

6.1.2.2.1. DESCRIÇÃO DA CAPACITAÇÃO KL 002.11.6

1. O objetivo principal é fornecer todo o conhecimento necessário para implantar, configurar e gerenciar a solução.

2. O curso deve ensinar como projetar, implantar e manter sistemas de proteção baseados no Kaspersky Endpoint Security e gerenciá-los centralmente por meio do Kaspersky Security Center.

3. A parte teórica do curso e os laboratórios práticos devem fornecer aos alunos conhecimentos e habilidades necessárias para:

3.1. Descrever os recursos do Kaspersky Endpoint Security para Windows e Kaspersky Security Center

3.2. Projetar e implantar uma solução de proteção ideal com base no Kaspersky Endpoint Security em uma rede Windows e gerenciá-la através do Kaspersky Security Center

3.3. Manter o sistema implantado

6.1.2.2.1.1. CONTEÚDO PROGRAMÁTICO MÍNIMO

1. Introdução

1.1. Noções básicas do Kaspersky Endpoint Security for Business

1.2. Como implantar o Kaspersky Endpoint Security for Business

1.3. Como instalar o Kaspersky Security Center

1.3.1. Laboratório 1. Instale o Kaspersky Security Center

1.4. Como instalar o Kaspersky Endpoint Security em computadores

1.4.1. Laboratório 2. Implantar o Kaspersky Endpoint Security

1,5. Como organizar computadores em grupos

1.5.1. Laboratório 3. Crie uma estrutura de computadores gerenciados

2. Gestão de proteção

2.1. Como o Kaspersky Endpoint Security protege os computadores

2.2. Como configurar a proteção de arquivos

2.2.1. Laboratório 4. Testar proteção contra ameaças a arquivos

2.3. Como configurar a proteção contra ameaças de rede

2.3.1. Laboratório 5. Configure a proteção contra ameaças por e-mail

3.5.1. Laboratório 19. Configure o controle adaptativo de anomalias

4. Manutenção

4.1. Como manter a proteção

4.1.1. Laboratório 20. Configure o painel

4.2. O que fazer diariamente

4.3. O que fazer se algo aconteceu

4.3.1. Laboratório 21. Configure as ferramentas de manutenção

4.3.2. Laboratório 22. Colete informações de diagnóstico

4.4. O que fazer periodicamente

6.1.2.2.2. DESCRIÇÃO DA CAPACITAÇÃO KL 009.12

1. Objetivo: Gerenciar vulnerabilidades e atualizações de software nos computadores da rede. Capturar, reconfigurar e instalar imagens do sistema operacional.

Trabalhar com os registros de hardware e software, gerenciar as licenças de aplicativos de terceiros e configure a integração com sistemas SIEM.

6.1.2.2.2.1. CONTEÚDO PROGRAMÁTICO MÍNIMO

1. Introdução

1.1. Vulnerabilidade e gerenciamento de patches no Kaspersky Security Center

1.2. Licenciamento

1.3. Acesso à funcionalidade de gerenciamento de vulnerabilidades e patches na interface do Kaspersky Security Center

2. Vulnerabilidade e gerenciamento de patches

2.1. Declaração do problema

2.2. Procure vulnerabilidades e atualizações necessárias

2.3. Sincronização do Windows Update

3.6.1. Laboratório 10. Como capturar uma imagem do sistema operacional

3.6.2. Laboratório 11. Como implantar uma imagem do sistema operacional em um computador gerenciado

3.6.3. Laboratório 12. Como implantar uma imagem do sistema operacional em um computador "bare metal"

6.2. REQUISITOS

6.2.1. REQUISITOS ESPECÍFICOS DOS SERVIÇOS

6.2.1.1. REQUISITOS DO SERVIÇO DE SUPORTE, MONITORAMENTO E ATUALIZAÇÃO

6.2.1.1.1. REQUISITOS DE ACEITAÇÃO DOS SERVIÇOS PRESTADOS

1. A CONTRATADA deverá apresentar relatório mensal de atendimentos contendo registro de todas as atividades de suporte bem como capacitações realizadas no período mensal de prestação de serviços encerrado.

2. Após a avaliação do relatório apresentado, de acordo com os REQUISITOS DE NÍVEL DE SERVIÇO MÍNIMO (NMS) a CONTRATANTE emitirá um termo de Aceite.

6.2.1.1.1.1. REQUISITOS DE RELATÓRIOS MENSAIS

1. O Relatório deve ser entregue em formato de documento, .pdf, ou docx. Não serão aceitos relatórios na nuvem, ou em outros formatos.

2. O Relatório deve ser encaminhado ao CREA-SP em até 5 (cinco) dias uteis contados a partir do dia seguinte ao fim do período mensal de prestação de serviços.

3. Qualquer gráfico adicionado ao relatório deve conter explicação do significado das informações em ambos os eixos (abscissas e ordenadas) bem como a conclusão do que o mesmo representa, e quais informações úteis tal gráfico fornece para o CREA e para a administração do sistema.

4. O Relatório deve conter no mínimo, mas não se limitando, às seguintes informações:

a. Lista de chamados abertos pelo CREA, e suas respectivas informações sumarizadas:

- Número identificativo do chamado/O.S.
- Descrição do objeto;
- Severidade;

- Data e horário de abertura;

- Tempos de atendimento conforme a tabela de níveis mínimos de serviço abaixo (proatividade, reação, Solução);

b. Assertividade mensal para cada nível de severidade (Sumário do atendimento mensal, contendo totais de chamados por severidade, destacando quais foram solucionados no prazo de atendimento, ou não, e destacando a assertividade mensal);

c. Descrição de atividades realizadas no sistema do Antivírus, solicitadas por via de chamado técnico, ou não. A quais devem conter os respectivos descritivos e conclusões;

d. Análise CONCLUSIVA da situação de segurança do sistema de antivírus (Servidor e estações);

e. Lista de pendências que possam haver entre o CREA-SP e a CONTRATADA, com seus respectivos planos de ações para resolução com responsabilidades claramente definidas (quem faz o que, como e quando);

f. Plano de ações com responsabilidades claramente definidas (quem faz o que, como e quando) para solucionar possíveis anomalias, discrepâncias, ou qualquer situação detectada que possa colocar em risco a segurança do sistema, no que tange a Vírus, ameaças, e todas as funcionalidades do sistema de Segurança oferecido pela Kaspersky;

g. Plano de ações com responsabilidades claramente definidas (quem faz o que, como e quando) para solução de chamados abertos há mais de um mês, que estejam sem solução;

6.2.1.1.2. REQUISITOS DO SERVIÇO DE SUPORTE TÉCNICO

a) O Atendimento e resolução dos chamados do suporte técnico deverá estar disponível, no mínimo, 8 (horas) horas por dia, 05 (cinco) dias por semana, durante o horário comercial, das 9:00 as 18:00, em português ou por meio de um tradutor.

b) A CONTRATADA deverá prestar assistência técnica durante todo o período contratual.

c) Deve haver Abertura ilimitada de chamados de suporte.

d) Não haverá limitante algum, inclusive de quantidade de horas, para o atendimento dos chamados abertos durante a vigência do contrato.

e) O atendimento será preferencialmente remoto. Caso haja necessidade de intervenção presencial "onsite", por qualquer motivo que impeça o atendimento remoto, independente de culpa ou responsabilidade do CREA, ou da CONTRATADA, este deverá ser executada pela CONTRATANTE.

f) Toda e qualquer despesa relacionadas a prestação do serviço de suporte presencial "onsite", inclusive, mas não se limitando a locomoção, estadia, alimentação e despesas trabalhistas são de responsabilidade inteira e exclusiva da CONTRATADA.

g) Qualquer atendimento presencial "onsite" deverá ser executado em uma das sedes do CREA na Capital de São Paulo.

h) Todos os atendimentos, (remotos ou locais), deverão ser executados sempre com acompanhamento e supervisão da equipe técnica da CONTRATANTE.

i) A CONTRATADA deverá oferecer manutenção e suporte técnico conforme o nível de severidade de cada chamado e dentro dos tempos de resposta definidos abaixo:

j) Quando um chamado for aberto pela CONTRATADA, a CONTRATANTE deverá atribuir ao chamado o nível de severidade de acordo com a avaliação do tipo do problema e do impacto/dano.

k) O CREA-SP poderá a qualquer momento, a seu próprio critério solicitar a mudança da severidade do chamado.

No qual deve ser prontamente atendido pela CONTRATADA, que deve passar a atendê-lo de acordo com a nova severidade.

l) A tabela abaixo traz exemplos de tipos de problemas e níveis de severidade.

Nível de Severidade	**Descrição de suporte e operações**
Severidade A (Crítica)	1 - Ambiente sem condições de funcionamento. 2 - Um ou mais serviços não estão acessíveis ou não podem ser usados. A produção, as operações ou as datas limite para implantação são gravemente afetadas, ou há um grave impactos obre a produção ou as atividades da instituição, ou de algum (qualquer) usuário da mesma. 3 - Um único, ou mais usuários, clientes ou serviços é afetado parcial ou totalmente. 4 - Situação que, mesmo não representando problema técnico grave, possa estar impactando na prestação do serviço do CREA-SP. Ex. Máquina do pregoeiro com problema de vírus, impedindo que seja realizado um pregão na data e hora marcados.
Severidade B (Médio)	Problema que gera restrições ao pleno funcionamento do ambiente. O serviço pode ser usado, mas com limitações. A situação tem impacto operacional moderado e é possível lidar com ela durante o horário comercial. Um único usuário, cliente ou serviço é afetado parcial ou totalmente.

Severidade C (Baixo)	Problema que não afeta o funcionamento do ambiente. A situação tem impacto operacional mínimo. O problema é importante, mas não tem impacto expressivo na produtividade e no serviço atual do cliente. Um único usuário experimenta interrupção parcial, mas existe uma solução alternativa aceitável

6.2.1.1.3. REQUISITOS DE NÍVEL DE SERVIÇO MÍNIMO (NMS)

1. Quanto ao tempo de resposta inicial do suporte técnico, deverá ser baseado nos níveis de severidade descritos acima.

A tabela abaixo descreve as metas de tempo de resposta.

Impacto	Tempo de Proatividade	Tempo de Reação	Tempo de Solução	Assertividade
Crítica	Até 5 minutos	Até 30 min.	Até 2 horas	95 %
Médio	Até 10 minutos	Até 1 hora	Até 4 horas	95 %
Baixo	Não se aplica	Até 06 horas	Até 8 horas	95 %

a) Tempo de Proatividade refere-se ao tempo decorrente entre a detecção da falha e a abertura do chamado. O sistema de Monitoramento/proatividade deve ao detectar uma falha, imediatamente abrir um chamado na operadora dentro dos tempos mínimos especificados.

b) Tempo de reação refere-se ao tempo decorrente entre a abertura do chamado e o contato telefônico (não é contabilizado contato por e-mail, SMS ou outro meio de mão única) entre a contratada e o analista do CREA-SP.

c) Tempo de solução é o tempo decorrido da abertura do chamado até a solução de contorno ou definitiva;

d) Solução de contorno entende se por uma solução temporária que restaure a funcionalidade perdida de forma que os efeitos do problema não sejam mais percebidos pelos usuários.

e) Solução definitiva entende-se pela solução que sanará a causa do problema.

f) Nas situações em que for detectado e/ou comprovado um problema de software (bug) na solução ofertada, o prazo de atendimento será fornecido diretamente pela engenharia do fabricante da solução ofertada.

g) Não será aceito fechamento unilateral de qualquer chamado, por qualquer motivo, ou seja, para que algum chamado seja encerrado deverá haver a anuência do CREA-SP.

h) Chamados que dependam de ação do CREA poderão ficar em estado de pausa, em que o tempo para solução não é contato, até que o CREA execute a ação que retire de sua responsabilidade a referida dependência. Nesses Casos, todos os tempos de atendimento e pausa devem ser registrados pela CONTRATADA.

i) Os chamados abertos não poderão, em hipótese alguma, ser fechados e/ou pausados unilateralmente pela CONTRATADA sem anuência por escrito do CREA-SP.

j) Qualquer chamado que seja fechado e/ou pausado sem anuência por escrito do CREA-SP deverá ser imediatamente reaberto pela CONTRATADA, permanecendo assim até que seja dada solução, ou justificativa para o fechamento/pausa. E em quaisquer dos casos devem ser aceitos formalmente, por escrito, pelo CREA-SP.

k) A empresa contratada deverá apresentar mensalmente relatório contendo todos os chamados abertos pelo CREA-SP, os tempos de reação, tempos de atendimento, assertividade, e plano de ação para solucionar problemas recorrentes ou sem solução os quais estejam impactando no funcionamento do ambiente, resguardando o direito do CREA-SP em elaborar seus próprios relatórios de auditoria para confrontá-los ao relatório da contratada.

6.2.1.1.4. REQUISITOS DE CENTRAL DE ATENDIMENTO

1. A CONTRATADA deverá disponibilizar uma Central de Atendimento para que a equipe técnica do CREA-SP faça registros de ocorrências e solicitações de reparo, bem como o acompanhamento da solução dos problemas.

2. O serviço de registro de chamadas deverá estar disponível nas 24 (vinte e quatro) horas do dia e nos 7 (sete) dias da semana.

3. A CONTRATADA deverá disponibilizar um número telefônico para receber as chamadas técnicas do CREA-SP, e realizar a comunicação entre o CREA-SP e a central de Atendimento da Contratada.

4. A Central de Atendimento deverá gerar um identificador de registro de chamadas que deverá ser informado ao CREA-SP no momento da abertura do chamado, e que terá por finalidade identificar a qualquer momento o problema específico, possibilitando o controle de chamados.

5. O CREA-SP poderá também realizar a abertura de chamados técnicos e solicitações de serviços para todos os itens desta especificação técnica diretamente no sistema de atendimento da CONTRATADA através de um Portal de Atendimento com acessos web, para abertura de chamados técnicos e solicitações de serviços e acompanhamento dos mesmos.

6. As informações relativas aos chamados deverão ser atualizadas automaticamente sempre que houver alguma alteração em sua situação. O acompanhamento on-line da resolução de chamados pelo CREA-SP poderá ser feito também através do sistema de atendimento.

7. Os chamados abertos no sistema de atendimento ou na Central de Atendimento serão referentes a todas as atividades de responsabilidade da CONTRATADA.

8. Os registros dos chamados deverão conter todas as informações relativas ao chamado aberto, como tempo de início e fim de atendimento, identificação do elemento (cliente, servidor) afetado, nome, fone e e-mail do contato no CREA-SP que foi posicionado acerca do reparo e restabelecimento do serviço, descrição detalhada da resolução do chamado com um código associado e responsabilidades.

9. A Contratada deverá atender chamados abertos por usuário, não técnicos, previamente cadastrados, relacionados à: Lentidão da rede, Indisponibilidade e Solicitação de Permissão de acesso à sites; (Apenas gestores);

6.2.1.1.5. REQUISITOS DOS SERVIÇOS DE ATUALIZAÇÃO

1. Os Serviços de atualização devem estar atrelados a chamados abertos no sistema da CONTRATADA, que possibilitarão o acompanhamento das atividades por parte da CONTRATANTE.

2. A CONTRATANTE deverá fornecer as senhas e usuários necessários para que os serviços de atualização possam ser executados adequadamente.

6.2.1.1.5.1. REQUISITOS DE LOCALIDADE DOS SERVIÇOS DE ATUALIZAÇÃO

1. Todo o Serviço de atualização poderá ser realizado remotamente, não obstante, caso haja necessidade de visita "on-site" para atendimento dos requisitos ou funcionalidades das atualizações dentro do prazo, todas as despesas de estadia, alimentação, transporte, etc. deverão ser pagas pela CONTRATADA, sem nenhum ônus financeiro para a CONTRATANTE.

2. A visita, caso necessária, se dará no site do CREA-SP situado à Av. Brigadeiro Faria Lima, 1059, Pinheiros, São Paulo, SP.

3. A decisão da solicitação de visita técnica "on-site" para atendimento deste requisito do contrato é de responsabilidade ÚNICA da CONTRATANTE, desde que baseada nas necessidades de cumprimento de prazo de instalação, ou de impossibilidade técnica da realização do serviço de forma remota, não havendo, depois de solicitado oficialmente pela CONTRATANTE, a possibilidade da CONTRATADA negar por qualquer motivo.

4. A Solicitação de Serviço de Atualização "on-site" deve ser realizada através da emissão de um oficio do CREA-SP para a CONTRATADA.

6.2.1.1.5.2 REQUISITOS DE ATUALIZAÇÃO DO SERVIDOR

1. A CONTRATADA deverá atualizar o banco de dados do Servidor de console do Antivírus, sendo de sua responsabilidade todas as atividades necessárias para entregar o servidor gerenciando todas as 1369 máquinas clientes, incluindo, mas não se limitando às seguintes atividades:

a. instalar/atualizar licenças.

b. Atualizar softwares clientes nos computadores dos usuários.

c. Atualizar softwares no Servidor.

d. Configurar parâmetros do Antivírus no servidor de console.

e. Parametrizar, caso necessário, o próprio console de gerenciamento.

6.2.1.1.5.3. REQUISITOS DE ATUALIZAÇÃO DOS CLIENTES

1. É responsabilidade da CONTRATADA atualizar todos os 1369 clientes do antivírus instalados nos computadores da Rede do CREA-SP, incluindo, mas não limitando-se às seguintes atividades:

a. instalar e atualizar licenças.

b. conectar-se remotamente no computador, celular, tablet, ou qualquer que seja o cliente, caso necessário.

c. configurar parâmetros

d. parametrizar, caso necessário o próprio sistema operacional do host cliente.

2. O Serviço de atualização dos clientes deverá ser executado imediatamente após o Serviço de Atualização do Servidor.

6.2.1.2. REQUISITOS DOS SERVIÇOS DE CAPACITAÇÃO

1. Os treinamentos devem ser fornecidos exclusivamente em Português.

2. Os treinamentos devem fornecer a cada participante um certificado reconhecido pela Kaspersky.

3. Os treinamentos devem ser fornecidos preferencialmente através de recursos online.

6.2.2. REQUISITOS GERAIS

6.2.2.1. REQUISITOS TEMPORAIS

1. As licenças dos softwares contratados, bem como suas chaves de ativação, devem ser disponibilizadas em até 15 dias corridos após a assinatura do contrato, podendo ser prorrogado por igual período, desde que justificado pela CONTRATADA e autorizado pela CONTRATANTE.

2. Os documentos pertinentes aos licenciamentos de softwares deverão ser entregues no endereço: Av. Brigadeiro Faria Lima, 1059 - Pinheiros - São Paulo/SP - CEP 01452-920, aos cuidados do Gestor do Contrato.

3. De comum acordo entre o CREA-SP e a CONTRATADA, a entrega da documentação previstas no item anterior poderá ser realizada de forma eletrônica.

4. Os instaladores dos softwares previstos neste termo de referência, assim como suas atualizações, deverão estar disponíveis para download em conta registrada em nome do CREA-SP ou de representante indicado pelo CREA-SP em site oficial designado pelo fabricante.

5. As versões das licenças deverão ser as mais recentes disponibilizadas no mercado pelo fabricante.

6. As atualizações ou correções das versões das licenças serão realizadas durante todo o período de vigência contratual.

6.2.2.2. REQUISITOS GERAIS PARA A EXECUÇÃO DOS SERVIÇOS

1. Serem realizados com base nas boas práticas preconizadas por modelos como ITIL (IT lnfrastructure Library), COBIT e PMBOK (Project Management Body of Knowledge);

2. Serem executados dentro dos parâmetros estabelecidos neste processo de contratação, com observância às recomendações aceitas pela boa técnica, normas e legislação, bem como observar conduta adequada na utilização dos materiais, equipamentos, ferramentas e utensílios, observando sempre os critérios de qualidade;

3. Adequar-se aos padrões normativos orientados pela Política de Segurança do CREA-SP;

4. Realizar os serviços de modo que não prejudiquem o andamento normal das atividades do Órgão em horário de seu expediente;

5. Implantar o planejamento, a execução e a supervisão permanente dos serviços demandados;

6. Responsabilizar-se pela definição da forma, metodologia, processos, local e modelo e execução dos serviços;

6.2.2.3. REQUISITOS DE QUALIFICAÇÕES DOS PROFISSIONAIS

1. Todos os serviços realizados pela CONTRATADA no âmbito desta CONTRATAÇÃO devem ser executados por profissionais qualificados certificados pela fabricante dos Softwares.

6.2.2.4. OUTROS REQUISITOS LEGAIS

1. A CONTRATADA deve executar o objeto do certame em estreita observância dos ditames estabelecido pela Lei no13.709/2018 (Lei Geral de Proteção de Dados Pessoais (LGPD)).

7 - DEVERES E RESPONSABILIDADES DA CONTRATANTE

7.1. OBRIGAÇÕES E RESPONSABILIDADES DA CONTRATANTE

1. Observar e fazer cumprir fielmente o que estabelece este Termo de Referência;

2. Receber o objeto no prazo e condições estabelecidas no Termo de Referência;

3. Prestar as informações e os esclarecimentos que venham a ser solicitados pela CONTRATADA;

4. Comunicará a CONTRATADA toda e qualquer ocorrência relacionada com a execução do Contrato;

5. Acompanhar e fiscalizar o cumprimento das obrigações da CONTRATADA por meio de um fiscal;

6. Colocar à disposição da CONTRATADA os elementos e informações necessárias à consecução do objeto do Contrato;

7. Atestar a entrega do objeto, receber e promover o pagamento das faturas correspondentes, quando apresentadas na forma estabelecida neste Termo;

8. Aplicar à CONTRATADA as penalidades contratuais e regulamentares cabíveis, garantidos o contraditório e a ampla defesa;

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

8 - DEVERES E RESPONSABILIDADES DA CONTRATADA

8.1. OBRIGAÇÕES E RESPONSABILIDADES DA CONTRATADA

1. Executar os serviços conforme especificações deste Termo de Referência e de sua proposta;

2. Reparar, corrigir, remover ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os serviços efetuados em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;

3. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, de acordo com os artigos 14 e 17 a 27, do Código de Defesa do Consumidor (Lei no 8.078, de 1990);

4. Responsabilizar-se por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas em legislação específica, cuja inadimplência não transfere responsabilidade à CONTRATANTE;

5. Relatar à CONTRATANTE toda e qualquer irregularidade verificada no decorrer da prestação dos serviços;

6. Executar o objeto do certame em estrita observância dos ditames estabelecido pela Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais (LGPD)).

7. Prestar as informações e os esclarecimentos que venham a ser solicitados pela CONTRATANTE por intermédio de preposto designado para acompanhamento do contrato) Indicar no prazo máximo de 24 horas úteis após a assinatura do contrato, junto à CONTRATANTE, um preposto para representar a CONTRATADA, principalmente no tocante à eficiência e agilidade da execução dos serviços objeto deste Termo de Referência, e que deverá responder pela fiel execução do contrato; Na hipótese de afastamento do preposto definitivamente ou temporariamente, a CONTRATADA deverá comunicar ao Gestor do Contrato por escrito o nome e a forma de comunicação de seu substituto até o fim do próximo dia útil.

8. Reconhecer o Gestor do Contrato, bem como outros servidores que forem indicados pela CONTRATANTE, para realizar as solicitações relativas ao contrato firmado, tais como manutenção, configuração, entre outras;

9. Apresentar Nota Fiscal/Fatura com a descrição dos serviços prestados, nas condições deste Termo de Referência, como forma de dar início ao processo de pagamento pela CONTRATANTE;

10. Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual;

11. Assumir as responsabilidades pelos encargos fiscais e comerciais resultantes da contratação.

12. Reparar, corrigir, remover ou substituir, às suas expensas, no total ou em parte, no prazo fixado em contrato, os serviços efetuados em que se verificarem vícios, defeitos ou incorreções resultantes da execução;

13. Propiciar todos os meios necessários à fiscalização do contrato pela CONTRATANTE, cujo representante terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, sempre que considerar a medida necessária;

14. Acatar as orientações da CONTRATANTE, sujeitando-se à mais ampla e irrestrita fiscalização, prestando os esclarecimentos solicitados e atendendo as reclamações formuladas;

15. Prestar esclarecimentos à CONTRATANTE sobre eventuais atos ou fatos noticiados que se refiram à CONTRATADA, independente de solicitação;

16. Comunicar à CONTRATANTE, por escrito, qualquer anormalidade nos serviços e prestar os esclarecimentos julgados necessários;

17. Não veicular publicidade ou qualquer outra informação acerca da prestação dos serviços do Contrato, sem prévia autorização da CONTRATANTE;

18. Não fazer uso das informações prestadas pela CONTRATANTE para fins diversos do estrito e absoluto cumprimento do contrato em questão;

9 - MODELO DE EXECUÇÃO DO CONTRATO

9.1 - Rotinas de Execução

9.1.1. FASE INICIAL DA CONTRATAÇÃO

1. A Fase inicial da contratação é definida como sendo os primeiros sessenta dias de contrato, no qual a contratada DEVERÁ realizar a atualização das licenças contratadas no Servidor de Antivírus e nos computadores do CREA-SP e seus respectivos clientes de Antivírus.

2. A Fase de Iniciação compreende as seguintes atividades:

a. A Reunião de Início do contrato

b. Atualização do Servidor de Antivírus

c. Atualização dos computadores/celulares/etc. onde roda o respectivo cliente do Antivírus.

9.1.1.1. DA REUNIÃO INICIAL DO CONTRATO

1. As partes, CONTRANTE e CONTRATADA deverão, em até 05 (cinco) dias úteis após a assinatura do contrato, prorrogáveis uma única vez, a pedido justificado pela CONTRATADA, promover a reunião inicial do Contrato ("kick off") para o estabelecimento e planejamento dos procedimentos relacionados ao updade/atualização das licenças no servidor e clientes.

2. A reunião inicial deve ter como resultado final um documento, que deve ser elaborado pela CONTRATADA e entregue ao CREA-SP para validação até o 10o dia útil após o início da execução dos serviços contratados, contemplando as seguintes premissas/atividades para o prazo de 60 dias:

a. O Plano de atualização do Servidor

b. O Plano de atualização dos clientes

c. Plano de Treinamento dos servidores do CREA-SP;

d. Plano para início dos atendimentos dos chamados de suporte técnico aos usuários do CREA-SP;

e. Entrega dos manuais de procedimentos para abertura de chamados na Central de Serviços para disseminação aos usuários de TIC do CREA-SP.

9.1.2. FASE DE OPERAÇÃO

1. A Fase de operação inicia com o aceite por parte do CREA da atualização das Licenças contratadas, tanto no Servidor quanto nos seus respectivos clientes, conforme os planejamentos efetuados na fase inicial da contratação.

2. A Fase de operação termina com o término do contrato.

3. Durante a Fase de Operação, a CONTRATADA entra em regime de Suporte continuado, conforme requisitos de suporte definidos neste termo de referência.

4. Durante esta fase o CREA-SP solicitará intervenções da CONTRATADA através da abertura de chamados no sistema da CONTRATADA, os quais devem ser atendidos pela CONTRATADA de acordo com o acordo de NMS (Nível Mínimo de Serviço) definido neste Termo de referência.

9.1.3. DA VIGÊNCIA

1. O Contrato terá vigência de 36 (trinta e seis) meses a partir da data de sua assinatura, podendo ser prorrogado até o limite de 48 (quarenta e oito) meses, na forma da Lei nº 8.666/93.

2. O Contratado deverá sujeitar-se aos acréscimos e supressões contratuais estabelecidos na forma do Art. 65 da Lei nº 8.666/93.

9.1.4. DO REAJUSTAMENTO DE PREÇOS

1. Os preços serão fixos e irreajustáveis pelos primeiros 12 (doze) meses da vigência contratual.

2. A cada 12 (doze) meses de execução contratual, o valor vigente do contrato sofrerá reajuste pelo índice IPC-FIPE para fins de atualização dos valores inicialmente contratados, tomando por base a data da apresentação da proposta comercial.

3. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

9.1.5. DA TRANSIÇÃO CONTRATUAL

1. Em casos de interrupção contratual e ocorrendo mudança de fornecedor da solução, todo conhecimento adquirido ou desenvolvido, bem como toda informação produzida pelos atendimentos de chamados de suporte deverão ser disponibilizados à CONTRATANTE ou empresa por ela designada em até 30 (trinta) dias corridos após o encerramento do contrato. As informações disponibilizadas devem ser em formato digital, inteligível para humanos, e na língua portuguesa.

2. A CONTRATADA deverá elaborar o Plano de Transição, no prazo de 60 (sessenta) dias corridos antes do encerramento do contrato, para a transferência integral e irrestrita dos conhecimentos e das competências necessárias e suficientes para promover a continuidade dos serviços.

3. A CONTRATANTE poderá estabelecer prazo inferior caso haja rescisão contratual.

4. Nenhum pagamento será devido à CONTRATADA pela elaboração ou pela execução do Plano de Transição. O fato da empresa CONTRATADA ou seus representantes não cooperarem ou reterem qualquer informação ou dado solicitado pela CONTRATANTE, que venha a prejudicar, de alguma forma, o andamento da transição das tarefas e serviços para um novo prestador, constituirá quebra de contrato, sujeitando-a as obrigações em relação a todos os danos causados à CONTRATANTE.

9.2. - Quantidade Mínima de Bens ou Serviços para Comparação e Controle

9.2.1. SERVIÇO DE SUPORTE CONTINUADO

1. O Serviço será auferido por meio do ACORDO DE NÍVEL DE SERVIÇO - NÍVEIS MÍNIMOS DE SERVIÇOS (NMS).

9.2.1.1. A execução contratual será acompanhada e fiscalizada por representantes da CONTRATANTE, que poderá utilizar-se da contratação de terceiros para assisti-la e subsidiá-la de informações pertinentes a essa atribuição, em consonância com as disposições do art. 67 da Lei no 8.666/1993.

9.2.1.2. A avaliação da qualidade e da adequação dos serviços ocorrerá na entrega do relatório mensal dos serviços prestados e será realizada pelo Fiscal Técnico do Contrato com base nos indicadores definidos no item REQUISITO DE NÍVEL DE SERVIÇO MÍNIMO (NMS) deste termo de referência, aos quais a CONTRATADA deverá atender.

9.2.1.3. A CONTRATADA estará sujeita, garantido o contraditório e a ampla defesa, às sanções administrativas em função dos indicadores obtidos abaixo da faixa de ajuste.

9.2.1.4. A aplicação dos ajustes do pagamento não exclui a aplicação de multas e sanções previstas neste documento.

9.2.2. DEMAIS SERVIÇOS

1. Os serviços serão auferidos mediante recebimento dos itens contratados, nas datas previamente acordadas entre o CREA-SP e a Contratada devidamente atestados pelo gestor do contrato.

9.3. - Mecanismos Formais de Comunicação entre a Contratada e a Administração

9.3.1. São mecanismos formais de comunicação entre a CONTRATADA e a CONTRATANTE:

a) E-mails: forma rápida de comunicação para tratar de informações pouco críticas;

b) Ofícios: Comunicação para tratar de assuntos gerais;

9.3.2. Toda a comunicação entre a CONTRATANTE e a CONTRATADA deverá ser sempre formal como regra, exceto em casos excepcionais que justifiquem outro canal de comunicação.

9.4 - Forma de Pagamento em Função dos Resultados

9.4.1. FORMAS DE PAGAMENTO

9.4.1.1. FORMA DE PAGAMENTO MEDIANTE ENTREGA

1. Os pagamentos dos seguintes itens da TABELA DE COMPOSIÇÃO DA SOLUÇÃO serão realizados mediante a entrega dos mesmos, após atesto do gestor do contrato e emissão da devida nota fiscal.

a. Capacitação código KL 002.11.6.

b. Capacitação código KL 009.12.

c. Licenças código KL4867KAVTR - Licenças, denominadas pela fabricante como: Kaspersky Endpoint Security for Business - Advanced Renewal 3 year.

9.4.1.2. FORMA DE PAGAMENTO DOS SERVIÇOS DE SUPORTE

1. O pagamento do Serviço de Suporte, Serviço de Atendimento 8x5, também chamado de Suporte Continuado, por sua característica de serviço continuado, será pago mensalmente após a emissão da devida nota fiscal e atesto do gestor do contrato.

9.4.2. DA NOTA FISCAL

1. O CREA-SP efetuará o pagamento até o 15º (décimo quinto) dia após a apresentação da nota fiscal/fatura, a qual deverá ser entregue na Sede Faria Lima, na Equipe de Suporte e Sustentação de TI, localizada na Av. Brigadeiro Faria Lima, 1059 – Pinheiros – CEP 01452-920 – São Paulo/SP, ficando a CONTRATADA obrigada a manter durante execução dos serviços os documentos abaixo relacionados acompanhados da nota fiscal/fatura:

2. Comprovante de Regularidade com o Fundo de Garantia do Tempo de Serviço– Certificado de Regularidade do FGTS CRF.

3. Comprovante de regularidade para com a Fazenda Federal- Certidão de débitos relativos a créditos tributários Federais e à Dívida ativa da União.

4. Comprovante de inexistência de débitos inadimplidos perante a Justiçado Trabalho, mediante a apresentação de Certidão

5. A nota fiscal/fatura será analisada, minimamente, quanto aos itens a seguir descritos:

a. Correlação entre os valores indicados na nota fiscal/fatura o da proposta da empresa.

b. Ausência de emendas ou rasuras na nota fiscal/fatura.

c. O correto preenchimento dos dados do CREA-SP (nome, CNPJ, dados contratuais) e da discriminação dos serviços;

d. Pertinência dos cálculos aritméticos da nota fiscal/fatura – o valor total deverá corresponder ao somatório dos valores individuais lançados na mesma,

e. Correlação entre o valor da nota fiscal e os valores empenhados;

f. Correlação entre o CNPJ da CONTRATADA e o constante na proposta e na nota de empenho;

6. O Crea-SP efetuará retenção de impostos eventualmente incidentes sobre o valor do bem/serviço, conforme previsto na Lei Federal nº 9.430, de 27 de dezembro de 1996 e Instrução Normativa RFB nº 1.234, de 11 de janeiro de 2012 e anexo;

7. A CONTRATADA é responsável pelos encargos fiscais, trabalhistas e previdenciários incidentes sobre os serviços contratados;

8. Se a CONTRATADA descumprir qualquer termo ou condição a que se obrigar no presente certame, por sua exclusiva culpa, poderá a Administração reter o pagamento, até que seja sanado o respectivo inadimplemento, não sobrevindo, portanto, qualquer ônus ao Conselho resultante desta situação;

9. Na hipótese do Crea-SP, por sua exclusiva culpa, efetuar com atraso qualquer pagamento previsto no Contrato, ficará sujeito multa de 2% (dois por cento) ao mês sobre o valor devido, calculada proporcionalmente aos dias de atraso.

9.4.3. CRONOGRAMA FÍSICO FINANCEIRO

1. A Tabela a seguir lista os principais marcos e eventos que ocorrerão durante a execução do Contrato:

Item	Descrição	Ano 1	Ano 2	Ano 3
1	Assinatura do contrato	N.A	N.A	N.A
2	Licenças e capacitação, itens 1, 2 e 3 da tabela de composição da solução	- Pagamento total mediante recebimento	N.A	N.A
3	Serviço de Suporte item 4 da tabela de composição da solução	- Pagamento de 1/3 do valor do contrato - Pagamento Mensal	- Pagamento de 1/3 do valor do contrato - Pagamento Mensal	- Pagamento de 1/3 do valor do contrato - Pagamento Mensal

10 - PROCEDIMENTOS DE FISCALIZAÇÃO DA EXECUÇÃO CONTRATUAL

10.1. PAPÉIS E RESPONSABILIDADES

10.1.1. PAPEIS E RESPONSABILIDADES DO CREA NA FISCALIZAÇÃO CONTRATUAL

10.1.1.1. Gestor do Contrato

Servidor com atribuições gerenciais, designado para coordenar e comandar o processo de gestão e fiscalização da execução contratual, indicado por autoridade competente.

10.1.1.2. Fiscal Técnico

Servidor representante da Área de Tecnologia da Informação, indicado pela autoridade competente dessa área para fiscalizar tecnicamente o contrato.

10.1.1.3. Fiscal Administrativo

Servidor representante da Área Administrativa, indicado pela autoridade competente dessa área para fiscalizar o contrato quanto aos aspectos administrativos.

10.1.2. PAPEIS E RESPONSABILIDADES DA CONTRATADA NA FISCALIZAÇÃO CONTRATUAL

10.1.2.1. Preposto

Representante da CONTRATADA, responsável por acompanhar a execução do contrato e atuar como interlocutor principal junto ao Órgão, incumbido de receber, diligenciar, encaminhar e responder às principais questões técnicas, legais e administrativas referentes ao andamento contratual:

1. Fazer a gestão geral do contrato, mantendo o controle de todas os chamados, com o objetivo de garantir a execução dos serviços dentro dos prazos estabelecidos, atendendo a todos os requisitos de qualidade;

2. Realizar a gestão, por parte da CONTRATADA, quanto aos aspectos de caráter administrativo e legal do contrato;

3. Informar ao CREA-SP sobre problemas de qualquer natureza que possam impedir o andamento normal dos serviços;

4. Elaborar e entregar ao Gestor os documentos mensais referentes ao cumprimento dos Níveis mínimos de Serviço (NMS);

5. Garantir a execução dos procedimentos administrativos referentes aos recursos envolvidos na execução dos serviços contratados;

6. Estar apto a prestar tempestivamente todas as informações (por meio de documentos impressos ou digitais) sobre as regularidades fiscais e financeiras da empresa, bem como a manutenção de todos os requisitos contratuais. Irregularidades administrativas ou contratuais poderão ensejar rescisão contratual;

7. Supervisionar todos os processos do trabalho, garantindo a qualidade dos serviços prestados e o cumprimento dos Níveis Mínimos de Serviço estabelecidos;

8. Propor novas rotinas, processos e fluxos de trabalho, visando maior eficácia no serviço prestado;

9. Gerenciar o cumprimento de prazos e prioridades estabelecidos;

10. Gerenciar e acompanhar o desempenho da prestação de serviço.

10.2. CONTROLE E FISCALIZAÇÃO DA EXECUÇÃO

1. O acompanhamento e a fiscalização da execução do contrato consistem na verificação da conformidade da prestação dos serviços e da alocação dos recursos necessários, de forma a assegurar o perfeito cumprimento do ajuste, devendo ser exercidos por um ou mais representantes da CONTRATANTE, especialmente designados, na forma dos arts. 67 e 73 da Lei nº 8.666, de 1993, e do art. 10 do Decreto nº 9.507, de 2018.

2. O representante da CONTRATANTE deverá ter a experiência necessária para o acompanhamento e controle da execução dos serviços e do contrato.

3. A verificação da adequação da prestação do serviço deverá ser realizada com base nos critérios previstos neste Termo de Referência e Anexos.

4. A execução do contrato será acompanhada e fiscalizada por meio de instrumentos de controle, que compreendam a mensuração dos aspectos mencionados no art. 47 e no ANEXO V, item 2.6, i, ambos da IN nº 05/2017.

5. A fiscalização técnica do contrato avaliará constantemente a execução do objeto e utilizará o Instrumento de Medição de Resultado (IMR), conforme previsto na TABELA DE NÍVEIS MÍNIMOS DE SERVIÇOS (NMS) deste Termo de Referência, ou outro instrumento substituto para aferição da qualidade da prestação dos serviços, devendo haver o redimensionamento no pagamento com base nos indicadores estabelecidos, sempre que a CONTRATADA:

- Não produzir os resultados, deixar de executar, ou não executar com a qualidade mínima exigida as atividades contratadas; ou

- Deixar de utilizar materiais e recursos humanos exigidos para a execução do serviço, ou utilizá-los com qualidade ou quantidade inferior à demandada.

6 A utilização da tabela NMS não impede a aplicação concomitante de outros mecanismos para a avaliação da prestação dos serviços.

7. Durante a execução do objeto, o fiscal técnico deverá monitorar constantemente o nível de qualidade dos serviços para evitar a sua degeneração, devendo intervir para requerer à CONTRATADA a correção das faltas, falhas e irregularidades constatadas.

10.3. ENTREGA E CRITÉRIOS DE ACEITAÇÃO DO OBJETO

10.3.1. ACEITAÇÃO DOS SERVIÇOS DE SUPORTE CONTINUADO

Os Serviços de suporte continuado serão aceitos mensalmente pelo gestor do contrato, através do seu Atesto. Os Critérios utilizados para dar aceitação são os definidos no NMS (Nível mínimo de Serviço) deste Termo de Referência.

10.3.1.1. ACEITAÇÃO DOS SERVIÇOS DE ATUALIZAÇÃO DO SERVIDOR

1. A aceitação referente ao primeiro mês da contratação, além dos critérios definidos no NMS (Níveis Mínimos de Serviço), somente será emitida após o término do Serviço de atualização do Servidor, conforme definido nos requisitos de atualização do Servidor (6.2.1.1.5.2)

10.3.1.2. ACEITAÇÃO DOS SERVIÇOS DE ATUALIZAÇÃO DOS CLIENTES

1. A aceitação referente ao segundo mês da contratação, além dos critérios definidos no NMS (Níveis Mínimos de Serviço), somente será emitida após o termino do Serviço de atualização dos Clientes, conforme definido nos requisitos de atualização dos Clientes (6.2.1.1.5.3).

10.3.2. ACEITAÇÃO DOS DEMAIS ITENS DO OBJETO

O Critério de aceitação é o seu recebimento e a verificação de que atendem ao tipo e quantitativo solicitado no objeto da Contratação.

10.4. DA ACEITAÇÃO DO OBJETO

1. A recusa parcial ou total de um relatório de serviços emitido, será oficiada à CONTRATADA pela CONTRATANTE, que deverá prontamente prestar o serviço de acordo com o solicitado e em acordo com os requisitos estabelecidos pelo contrato;

11 - ESTIMATIVA DE PREÇO

Item	Bem/serviço	Qtde	Unidade	Valor unitário	Valor Total
1	Licenças de Antivírus denominadas pelo fabricante de: "Kaspersky Endpoint Security for Business - Advanced Renewal 3 year Band V: 1000-1499"- código KL4867KAVFR	1369	Licenças	R$	R$
2	Capacitação de implantação, configuração e gerenciamento da solução.	4	Pessoas	R$	R$
3	Capacitação em gerenciamento de vulnerabilidades a atualizações de software e integração com o sistema SIEM.	4	Pessoas	R$	R$
4	Serviço de Suporte 8x5, monitoramento, atualização do servidor e clientes	36	Serviço Mensal	R$	R$
TOTAL (R$)					

12 - FONTE DE RECURSOS ORÇAMENTÁRIOS

12.1. DOTAÇÃO ORÇAMENTÁRIA

Os recursos orçamentários para a presente contratação são oriundos:

- Conta Contábil: 6.2.2.1.1.01.04.09.005
- Centro de Custo: 01.03.17.09.01.01

13 - LOCAIS DE ENTREGA

13.1 Endereço: Av. Brigadeiro Faria Lima, 1059 - Pinheiros - São Paulo - SP

- Telefone para informações: (11) 3095 – 6484

14 - CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

REGIME DE EXECUÇÃO	( ) Empreitada	( ) Preço Global	(X) Preço Unitário
ADJUDICAÇÃO DO OBJETO	(X) Global	( ) Por Lote	( ) Por Item

14.1. – Qualificação Técnica

1. Comprovação de aptidão para a para o fornecimento de bens/serviços em características, quantidades e prazos compatíveis com o objeto desta licitação, por meio de apresentação de Atestado fornecido por pessoas jurídicas de direito público ou privado.

2. O(s) atestado(s) deverão ser apresentados em papel timbrado do emitente, conter identificação do signatário, nome, endereço, telefone e se for o caso, correio eletrônico para contato, a fim de possibilitar possíveis diligências.

OBS.: A Licitante Vencedora deverá apresentar obrigatoriamente, na assinatura do Contrato, cópia autenticada da declaração feita pela Kaspersky, declarando que a empresa é revenda autorizada a fornecer o produto adquirido através do certame.

14.2 - Critérios de Seleção
14.2.1 - Critérios Gerais

14.2.1.1. DO TRATAMENTO DIFERENCIADO ÀS MICROEMPRESAS, EMPRESAS DE PEQUENO PORTE E COOPERATIVA

1. As microempresas e empresas de pequeno porte, que se beneficiarem do regime diferenciado e favorecido concedido pela Lei Complementar n. 123 de 2006, por ocasião da participação neste certame licitatório, deverão apresentar toda a documentação exigida para habilitação, inclusive para efeito de comprovação de regularidade fiscal, mesmo que apresente alguma restrição.

2. Está vedada a participação de cooperativas nos termos da seção da vedação à participação de Cooperativas.

14.2.1.2. DA VEDAÇÃO À PARTICIPAÇÃO DE COOPERATIVAS

1. Fica vedada a participação de cooperativas por não atender aos termos do Artigo 10, inciso I da Instrução Normativa nº 05/2017:

> *Art. 10. A contratação de sociedades cooperativas somente poderá ocorrer quando, pela sua natureza, o serviço a ser contratado evidenciar:*

> *I - a possibilidade de ser executado com autonomia pelos cooperados, de modo a não demandar relação de subordinação entre a cooperativa e os cooperados, nem entre a Administração e os cooperados; e*
>
> *II - que a gestão operacional do serviço seja executada de forma compartilhada ou em rodízio, em que as atividades de coordenação e supervisão da execução dos serviços e as de preposto, conforme determina o art. 68 da Lei nº 8.666, de 1993, sejam realizadas pelos cooperados de* forma alternada ou aleatória, para que tantos quanto possíveis venham a assumir tal atribuição.

2. Avalia-se que no contexto do presente objeto há de se ter diversos perfis de conhecimento e funções distintas para o gerenciamento, desenvolvimento, análise, suporte técnico, operacionalização, treinamento, desenvolvimento de manutenções evolutivas e adaptativas, para a execução das atividades relacionadas à prestação de serviço, que guardam correlação técnica entre si, em função de sua interdependência a começar pelo fornecimento do licenciamento.

3. Portanto, neste caso, há falta de atendimento ao inciso I, o que impossibilita a participação de cooperativas.

14.2.1.3. REGIME DE EXECUÇÃO

1. O regime da execução dos contratos é de EMPREITADA POR PREÇO UNITÁRIO.

14.2.1.4. CRITÉRIO DE JULGAMENTO

1. O tipo e critério de julgamento da licitação é o MENOR PREÇO GLOBAL para a seleção da proposta mais vantajosa.

14.2.2 - Subcontratação

14.2.2.1. Não será permitida a subcontratação, no todo ou em parte, do objeto.

14.2.3 - Formação de Consórcios

14.2.3.1. Não será permitida formação de Consórcio.

14.2.4 - Alteração Subjetiva

14.2.4.1. É admissível a fusão, cisão ou incorporação da CONTRATADA com/por 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.

14.2.5 - Garantia Contratual

14.2.5.1. Não será exigida a prestação de garantia de execução para celebrar a contratação decorrente deste certame licitatório.

15 - ANEXOS DO TERMO DE REFERÊNCIA

ANEXO_A_Funcionalidades_mínimas_do_antivirus.pdf

Processo nº V-0066/2021

ANEXO A

CARACTERÍSTICAS E FUNCIONALIDADES MÍNIMAS DO SOFTWARE ANTIVÍRUS

ANEXO_A
CARACTERÍSTICAS E FUNCIUONALIDADES MÍNIMAS DO SOFTWARE ANTI-VÍRUS

1. Especificações técnicas da solução para ambiente Windows, Linux e Mobile.

1.1. Compatibilidade:

1.1.2. Microsoft Windows Server 2008 (Todas edições);
1.1.3. Microsoft Windows Server 2008 x64 SP1 (Todas edições);
1.1.4. Microsoft Windows Server 2008 R2 (Todas edições);
1.1.5. Microsoft Windows Server 2012 (Todas edições);
1.1.6. Microsoft Windows Server 2012 R2 (Todas edições);
1.1.7. Microsoft Windows Server 2016 x64
1.1.8. Microsoft Windows Small Business Server 2008 (Todas edições);
1.1.9. Microsoft Windows Small Business Server 2011 (Todas edições);
1.1.10. Microsoft Windows XP Professional SP2 ou superior;
1.1.10.1. Microsoft Windows XP Professional x64 SP2 ou superior;
1.1.11. Microsoft Windows Vista Business / Enterprise / Ultimate SP1 ou posterior;
1.1.12. Microsoft Windows Vista Business / Enterprise / Ultimate SP1 x64 ou posterior;
1.1.13. Microsoft Windows 7 SP1 Professional / Enterprise / Ultimate x32/x64;
1.1.14. Microsoft Windows 7 SP1 Professional / Enterprise / Ultimate x32/x64;
1.1.15. Microsoft Windows 8 SP1 Professional / Enterprise x32/x64;
1.1.16. Microsoft Windows 8 Professional / Enterprise x64;
1.1.17. Microsoft Windows 8.1 Professional / Enterprise x32;
1.1.18. Microsoft Windows 8.1 Professional / Enterprise x64;
1.1.19. Microsoft Windows 10 todas edições x32;
1.1.19.1.1. Microsoft Windows 10 todas edições x64;

Suporta as seguintes plataformas virtuais:

1.1.20. Vmware: Workstation 12.x Pro, vSphere 5.5, vSphere 6
1.1.21. Microsoft Hyper-V: 2008, 2008 R2, 2008 R2 SP1, 2012, 2012 R2;
1.1.22. Microsoft VirtualPC 6.0.156.0;
1.1.23. Parallels Desktop 7 e 11;
1.1.24. Oracle VM VirtualBox 4.0.4-70112 (Somente logon como convidado);
1.1.25. Citrix XenServer 6.2 e 6.5

Características:

1.1.26. A console deve ser acessada via WEB (HTTPS) ou MMC;
1.1.26.1. Console deve ser baseada no modelo cliente/servidor;
1.1.26.2. Compatibilidade com Windows Failover Clustering ou outra solução de alta disponibilidade;
1.1.26.3. Deve permitir a atribuição de perfis para os administradores da Solução de Antivírus;
1.1.27. Deve permitir incluir usuários do AD para logarem na console de administração
1.1.27.1. Console deve ser totalmente integrada com suas funções e módulos caso haja a necessidade no futuro de adicionar novas tecnologias tais como, criptografia, Patch management e MDM;
1.1.28. As licenças deverão ser perpétuas, ou seja, expirado a validade da mesma o produto deverá permanecer funcional para a proteção contra códigos maliciosos utilizando as definições até o momento da expiração da licença;
1.1.28.1. Capacidade de remover remotamente e automaticamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores;
1.1.28.2. Capacidade de instalar remotamente a solução de antivírus nas estações e servidores Windows, através de compartilhamento administrativo, login script e/ou GPO de Active Directory;
1.1.29. Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria;
1.1.30. Deve armazenar histórico das alterações feitas em políticas;
1.1.31. Deve permitir voltar para uma configuração antiga da política de acordo com o histórico de alterações efetuadas pelo administrador apenas selecionando a data em que a política foi alterada;
1.1.32. Deve ter a capacidade de comparar a política atual com a anterior, informando quais configurações foram alteradas;
1.1.33. A solução de gerencia deve permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas;
1.1.34. Através da solução de gerência, deve ser possível verificar qual licença está aplicada para determinado computador;
1.1.35. Capacidade de instalar remotamente a solução de segurança em smartphones e tablets de sistema iOS e Android;
1.1.36. Capacidade de instalar remotamente qualquer “app” em smartphones e tablets de sistema iOS;
1.1.37. A solução de gerência centralizada deve permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle;
1.1.38. Deverá ter a capacidade de criar regras para limitar o tráfego de comunicação cliente/servidor por subrede com os seguintes parâmetros: KB/s e horário;
1.1.38.1. Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux e Mac) protegidos pela solução antivírus;

1.1.38.2. Capacidade de gerenciar smartphones e tablets (Android e iOS) protegidos pela solução de segurança;

1.1.39. Capacidade de instalar atualizações em computadores de teste antes de instalar nos demais computadores da rede;

1.1.40. Capacidade de gerar pacotes customizados (auto executáveis) contendo a licença e configurações do produto;

1.1.41. Capacidade de atualizar os pacotes de instalação com as últimas vacinas;

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

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

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

1.1.44. Deve permitir a realocação de máquinas novas na rede para um determinado grupo sem ter um agente ou endpoint instalado utilizando os seguintes parâmetros:

1.1.44.1. Nome do computador;

1.1.44.2. Nome do domínio;

1.1.44.3. Range de IP;

1.1.44.4. Sistema Operacional;

1.1.44.5. Máquina virtual.

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

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

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

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

1.1.49. Capacidade de, assim que detectar máquinas novas no Active Directory, subnets ou grupos de trabalho, automaticamente importar a máquina para a estrutura de proteção da console e verificar se possui o antivírus instalado. Caso não possuir, deve instalar o antivírus automaticamente;

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

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

1.1.52. Deve fornecer as seguintes informações dos computadores:

1.1.52.1. Se o antivírus está instalado;
1.1.52.2. Se o antivírus está iniciado;
1.1.52.3. Se o antivírus está atualizado;
1.1.52.4. Minutos/horas desde a última conexão da máquina com o servidor administrativo;
1.1.52.5. Minutos/horas desde a última atualização de vacinas;
1.1.52.6. Data e horário da última verificação executada na máquina;
1.1.52.7. Versão do antivírus instalado na máquina;
1.1.52.8. Se é necessário reiniciar o computador para aplicar mudanças;
1.1.52.9. Data e horário de quando a máquina foi ligada;
1.1.52.10. Quantidade de vírus encontrados (contador) na máquina;
1.1.52.11. Nome do computador;
1.1.52.12. Domínio ou grupo de trabalho do computador;
1.1.52.13. Data e horário da última atualização de vacinas;
1.1.52.14. Sistema operacional com Service Pack;
1.1.52.15. Quantidade de processadores;
1.1.52.16. Quantidade de memória RAM;
1.1.52.17. Usuário(s) logado(s) naquele momento, com informações de contato (caso disponíveis no Active Directory);
1.1.52.18. Endereço IP;
1.1.52.19. Aplicativos instalados, inclusive aplicativos de terceiros, com histórico de instalação, contendo data e hora que o software foi instalado ou removido;
1.1.52.20. Atualizações do Windows Updates instaladas;
1.1.52.21. Informação completa de hardware contendo: processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de áudio, adaptadores de rede, monitores, drives de CD/DVD;
1.1.52.22. Vulnerabilidades de aplicativos instalados na máquina;
1.1.53. Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterá-las;
1.1.54. Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como:
1.1.54.1. Alteração de Gateway Padrão;
1.1.54.2. Alteração de subrede;
1.1.54.3. Alteração de domínio;
1.1.54.4. Alteração de servidor DHCP;
1.1.54.5. Alteração de servidor DNS;
1.1.54.6. Alteração de servidor WINS;
1.1.54.7. Alteração de subrede;
1.1.54.8. Resolução de Nome;
1.1.54.9. Disponibilidade de endereço de conexão SSL;
1.1.55. Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet;
1.1.56. Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes;

1.1.57. Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus;
1.1.58. Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos;
1.1.59. Capacidade de eleger qualquer computador cliente como repositório de vacinas e de pacotes de instalação, sem que seja necessária a instalação de um servidor administrativo completo, onde outras máquinas clientes irão atualizar-se e receber pacotes de instalação, a fim de otimizar tráfego da rede;
1.1.60. Capacidade de fazer deste repositório de vacinas um gateway para conexão com o servidor de administração, para que outras máquinas que não consigam conectar-se diretamente ao servidor possam usar este gateway para receber e enviar informações ao servidor administrativo;
1.1.61. Capacidade de exportar relatórios para pelo menos dois dos seguintes tipos de arquivos: PDF, HTML e XML;
1.1.62. Capacidade de gerar traps SNMP para monitoramento de eventos;
1.1.63. Capacidade de enviar e-mails para contas específicas em caso de algum evento;
1.1.64. Listar em um único local, todos os computadores não gerenciados na rede;
1.1.65. Deve encontrar computadores na rede através de no mínimo três formas: Domínio, Active Directory e subredes;
1.1.66. Deve possuir compatibilidade com Microsoft NAP, quando instalado em um Windows 2008 Server;
1.1.67. Capacidade de baixar novas versões do antivírus direto pela console de gerenciamento, sem a necessidade de importá-los manualmente
1.1.68. Capacidade de ligar máquinas via Wake on Lan para realização de tarefas (varredura, atualização, instalação, etc), inclusive de máquinas que estejam em subnets diferentes do servidor;
1.1.69. Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado intervalo de tempo);
1.1.70. Deve através de opções de optimizações fazer com que o computador gerenciado conceda recursos à outras aplicações, mantendo o antivírus ativo porém sem comprometer o desempenho do computador;
1.1.71. Deve permitir a configuração de senha no endpoint e configurar quando que será necessário a utilizá-la, (ex: Solicitar senha quando alguma tarefa de scan for criada localmente no endpoint);
1.1.72. Permitir fazer uma verificação rápida ou detalhada de um dispositivo removível assim que conectado no computador, podendo configurar a capacidade máxima em GB da verificação;
1.1.73. Deve ser capaz de configurar quais eventos serão armazenados localmente, nos eventos do windows ou ainda se serão mostrados na tela para o colaborador, sejam estes eventos informativos, de alertas ou de erros;
1.1.74. Capacidade de realizar atualização incremental de vacinas nos computadores clientes;

1.1.75. Deve armazenar localmente e enviar ao servidor de gerência a ocorrência de vírus com os seguintes dados, no mínimo:
   a) Nome do vírus;
   b) Nome do arquivo infectado;
   c) Data e hora da detecção;
   d) Nome da máquina ou endereço IP;
   e) Ação realizada.

1.1.76. Capacidade de reportar vulnerabilidades de softwares presentes nos computadores;

1.1.77. Capacidade de listar updates nas máquinas com o respectivo link para download

1.1.78. Deve criar um backup de todos arquivos deletados em computadores para que possa ser restaurado através de comando na Console de administração;

1.1.79. Deve ter uma quarentena na própria console de gerenciamento, permitindo baixar um artefato ou enviar direto para análise do fabricante;

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

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

1.1.82. Capacidade de diferenciar máquinas virtuais de máquinas físicas.

Funcionalidades Requeridas para estações Windows

Compatibilidade:

1.1.83. Microsoft Windows 7 Professional/Enterprise/Ultimate x86 / x64 e posterior;

1.1.83.1. Microsoft Windows 8 Professional/Enterprise x86 / x64;

1.1.84. Microsoft Windows 8.1 Pro / Enterprise x86 / x64;

1.1.85. Microsoft Windows 10 Pro / Enterprise x86 / x64;

1.1.86. Microsoft Windows Server 2012 R2 Standard x64;

1.1.87. Microsoft Windows Server 2012 Foundation x64;

1.1.88. Microsoft Windows Server 2012 Standard x64;

1.1.89. Microsoft Small Business Server 2011 Standard x64;

1.1.90. Microsoft Windows Server 2008 R2 Standard/Enterprise x64 SP1;

1.1.91. Microsoft Windows Server 2008 Standard/Enterprise x86/x64 SP2;

1.1.92. Microsoft Windows Server 2016 x64

Características:

1.1.93. Deve prover as seguintes proteções:

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

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

1.1.93.3. Antivírus de E-mail (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos);

1.1.93.4. O Endpoint deve possuir opção para rastreamento por linha de comando, parametrizável, com opção de limpeza;

1.1.93.5. Firewall com IDS;

1.1.93.6. Autoproteção (contra-ataques aos serviços/processos do antivírus);

1.1.93.7. Controle de dispositivos externos;

1.1.93.8. Controle de acesso a sites por categoria, ex: Bloquear conteúdo adulto, sites de jogos, etc;

1.1.93.9. Controle de acesso a sites por horário;

1.1.93.10. Controle de acesso a sites por usuários;

1.1.93.11. Controle de acesso a websites por dados, ex: Bloquear websites com conteúdos de vídeo e áudio;

1.1.93.12. Controle de execução de aplicativos;

1.1.93.13. Controle de vulnerabilidades do Windows e dos aplicativos instalados;

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

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

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

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

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

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

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

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

1.1.102. Ter a capacidade de fazer detecções por comportamento, identificando ameaças avançadas sem a necessidade de assinaturas;

1.1.103. Capacidade de verificar somente arquivos novos e alterados;

1.1.104. Capacidade de verificar objetos usando heurística;

1.1.105. Capacidade de agendar uma pausa na verificação;

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

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

1.1.108. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
1.1.108.1. Perguntar o que fazer, ou;
1.1.108.2. Bloquear acesso ao objeto;
1.1.108.2.1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
1.1.108.2.2. Caso positivo de desinfecção:
1.1.108.2.2.1. Restaurar o objeto para uso;
1.1.108.2.3. Caso negativo de desinfecção:
1.1.108.2.3.1. Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);
1.1.109. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
1.1.110. Capacidade de verificar e-mails recebidos e enviados nos protocolos POP3, IMAP, NNTP, SMTP e MAPI, assim como conexões criptografadas (SSL) para POP3 e IMAP (SSL);
1.1.111. Capacidade de verificar links inseridos em e-mails contra phishings;
1.1.112. Capacidade de verificar tráfego nos browsers: Internet Explorer, Firefox e Opera;
1.1.113. Capacidade de verificação de corpo e anexos de e-mails usando heurística;
1.1.114.
1.1.115. O antivírus de e-mail, ao encontrar um objeto potencialmente perigoso, deve:
1.1.115.1. Perguntar o que fazer, ou;
1.1.115.2. Bloquear o e-mail;
1.1.115.2.1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
1.1.115.2.2. Caso positivo de desinfecção:
1.1.115.2.2.1. Restaurar o e-mail para o usuário;
1.1.115.2.3. Caso negativo de desinfecção:
1.1.115.2.3.1. Mover para quarentena ou apagar o objeto (de acordo com a configuração pré-estabelecida pelo administrador);
1.1.116. Caso o e-mail conter código que parece ser, mas não é definitivamente malicioso, o mesmo deve ser mantido em quarentena;
1.1.117. Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados;
1.1.118. Capacidade de filtrar anexos de e-mail, apagando-os ou renomeando-os de acordo com a configuração feita pelo administrador;
1.1.119. Capacidade de verificação de tráfego HTTP e qualquer script do Windows Script Host (JavaScript, Visual Basic Script, etc), usando heurísticas;
1.1.120. Deve ter suporte total ao protocolo Ipv6;
1.1.121. Capacidade de alterar as portas monitoradas pelos módulos de Web e E-mail;

1.1.122. Na verificação de tráfego web, caso encontrado código malicioso o programa deve:

1.1.122.1. Perguntar o que fazer, ou;

1.1.122.2. Bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio, ou;

1.1.122.3. Permitir acesso ao objeto;

1.1.123. O antivírus de web deve realizar a verificação de, no mínimo, duas maneiras diferentes, sob escolha do administrador:

1.1.123.1. Verificação *on-the-fly*, onde os dados são verificados enquanto são recebidos em tempo-real, ou;

1.1.123.2. Verificação de *buffer*, onde os dados são recebidos e armazenados para posterior verificação;

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

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

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

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

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

1.1.129. Capacidade de distinguir diferentes subnets e conceder opção de ativar ou não o firewall para uma subnet específica;

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

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

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

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

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

1.1.132.1. Discos de armazenamento locais;

1.1.132.2. Armazenamento removível;

1.1.132.3. Impressoras;

1.1.132.4. CD/DVD;

1.1.132.5. Drives de disquete;
1.1.132.6. Modems;
1.1.132.7. Dispositivos de fita;
1.1.132.8. Dispositivos multifuncionais;
1.1.132.9. Leitores de smart card;
1.1.132.10. Dispositivos de sincronização via ActiveSync (Windows CE, Windows Mobile, etc);
1.1.132.11. Wi-Fi;
1.1.132.12. Adaptadores de rede externos;
1.1.132.13. Dispositivos MP3 ou smartphones;
1.1.132.14. Dispositivos Bluetooth;
1.1.132.15. Câmeras e Scanners.

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

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

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

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

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

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

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

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

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

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

Funcionalidades Requeridas para Estações Mac OS X

Compatibilidade:

1.1.143. Mac OS X 10.11 (El Capitan);

1.1.144. Mac OS X 10.10 (Yosemite);
1.1.145. Mac OS X 10.9 (Mavericks);
1.1.146. Mac OS X 10.8 (Mountain Lion);
1.1.147. Mac OS X 10.7 (Lion);
1.1.148. Mac OS Sierra 10.12

Características:

1.1.149. Deve prover proteção residente para arquivos (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
1.1.150. Possuir módulo de web-antivírus para proteger contra ameaças durante navegação na internet com possíbilidade de analisar endereços https;
1.1.151. Possuir módulo de bloqueio á ataques na rede;
1.1.152. Possibilidade de bloquear a comunicação entre a máquina atacante e os demais computadores por tempo definido pelo administrador;
1.1.153. Capacidade de criar exclusões para computadores que não devem ser monitorados pelo módulo de bloqueio à ataques na rede;
1.1.154. Possibilidade de importar uma chave no pacote de instalação;
1.1.155. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
1.1.156. A instalação e primeira execução do produto deve ser feita sem necessidade de reinicialização do computador, de modo que o produto funcione com toda sua capacidade;
1.1.157. Deve possuir suportes a notificações utilizando o Growl;
1.1.158. As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa);
1.1.159. Capacidade de voltar para a base de dados de vacina anterior;
1.1.160. Capacidade de varrer a quarentena automaticamente após cada atualização de vacinas;
1.1.161. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: “Win32.Trojan.banker”) para que qualquer objeto detectado com o veredicto escolhido seja ignorado;
1.1.162. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);
1.1.163. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;
1.1.164. Capacidade de verificar somente arquivos novos e alterados;
1.1.165. Capacidade de verificar objetos usando heurística;

1.1.166. Capacidade de agendar uma pausa na verificação;

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

1.1.167.1. Perguntar o que fazer, ou;

1.1.167.2. Bloquear acesso ao objeto;

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

1.1.167.2.2. Caso positivo de desinfecção:

1.1.167.2.2.1. Restaurar o objeto para uso;

1.1.167.2.3. Caso negativo de desinfecção:

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

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

1.1.169. Capacidade de verificar arquivos de formato de email;

1.1.170. Possibilidade de trabalhar com o produto pela linha de comando, com no mínimo opções para atualizar as vacinas, iniciar uma varredura, para o antivírus e iniciar o antivírus pela linha de comando;

1.1.171. Capacidade de ser instalado, removido e administrado pela mesma console central de gerenciamento.

Funcionalidades Requeridas para Estações de trabalho Linux

Compatibilidade:

1.1.172. Plataforma 32-bits:

1.1.172.1. Red Hat Enterprise Linux 6.7;

1.1.172.2. Red Hat Enterprise Linux 6.8;

1.1.172.3. CentOS-6.7;

1.1.172.4. CentOS-6.8;

1.1.172.5. Ubuntu 14.04 LTS;

1.1.172.6. Ubuntu 16.04 LTS;

1.1.172.7. Ubuntu 16.10 LTS;

1.1.172.8. Debian GNU/Linux 7.10;

1.1.172.9. Debian GNU/Linux 7.11;

1.1.172.10. Debian GNU/Linux 8.6;

1.1.172.11. Debian GNU/Linux 8.7.

1.1.173. Plataforma 64-bits:

1.1.173.1. Red Hat Enterprise Linux 6.7;

1.1.173.2. Red Hat Enterprise Linux 6.8;

1.1.173.3. Red Hat Enterprise Linux 7.2;

1.1.173.4. Red Hat Enterprise Linux 7.3;

1.1.173.5. CentOS-6.7;

1.1.173.6. CentOS-6.8;
1.1.173.7. CentOS-7.2;
1.1.173.8. CentOS-7.3;
1.1.173.9. Ubuntu 14.04 LTS;
1.1.173.10. Ubuntu 16.04 LTS;
1.1.173.11. Ubuntu 16.10 LTS;
1.1.173.12. Debian GNU/Linux 7.10;
1.1.173.13. Debian GNU/Linux 7.11;
1.1.173.14. Debian GNU/Linux 8.6;
1.1.173.15. Debian GNU/Linux 8.7;
1.1.173.16. OpenSUSE 42.2;
1.1.173.17. SUSE Linux Enterprise Server 12;
1.1.173.18. OracleLinux 7.3;
1.1.173.19. Novell Open Enterprise Server 11 SP3;
1.1.173.20. Novell Open Enterprise Server 2015 SP1

Características:

1.1.174. Deve prover as seguintes proteções:
1.1.175. Antivírus de arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
1.1.176. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;
1.1.177. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
1.1.178. Capacidade de criar exclusões por local, máscara e nome da ameaça;
1.1.179. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
1.1.180. Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;
1.1.181. Dectectar aplicações que possam ser utilizadas como vetor de ataque por hackers;
1.1.182. Fazer detecções através de heurística utilizando no mínimo as seguintes opções de nível:
1.1.182.1. Alta;
1.1.182.2. Média;
1.1.182.3. Baixa;
1.1.182.4. Recomendado;
1.1.183. Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;
1.1.184. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados.

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

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

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

1.1.188. Capacidade de verificar objetos usando heurística;

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

1.1.190. Possibilidade de

1.1.191. Deve possuir módulo escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).

Funcionalidades Requeridas para Servidores Windows

Compatibilidade:

1.1.192. Plataforma 32-bits:

1.1.192.1. Windows Server 2008 Standard/Enterprise/Datacenter SP1 e posterior;

1.1.192.2. Windows Server 2008 Core Standard/Enterprise/Datacenter SP1 e posterior

1.1.193. Plataforma 64-bits

1.1.194. Microsoft Windows Server 2008 Standard / Enterprise / DataCenter (SP1 ou posterior);

1.1.195. Microsoft Windows Server 2008 Core Standard / Enterprise / DataCenter (SP1 ou posterior).

1.1.196. Microsoft Windows Server 2008 R2 Standard / Enterprise / DataCenter (SP1 ou posterior);

1.1.197. Microsoft Windows Server 2008 R2 Core Standard / Enterprise / DataCenter (SP1 ou posterior);

1.1.198. Microsoft Windows Storage Server 2008 R2;

1.1.199. Microsoft Windows Storage Server 2008 SP2 Standard Edition;

1.1.200. Microsoft Windows Storage Server SP2 Workgroup Edition;

1.1.201. Microsoft Windows Hyper-V Server 2008 R2 SP1 e posterior;

1.1.202. Microsoft Windows Server 2012 Essentials / Standard / Foundation / Datacenter;

1.1.203. Microsoft Windows Server 2012 R2 Essentials / Standard / Foundation / Datacenter;

1.1.204. Microsoft Windows Server 2012 Core Essentials / Standard / Foundation / Datacenter;
1.1.205. Microsoft Windows Server 2012 R2 Core Essentials / Standard / Foundation / Datacenter;
1.1.206. Microsoft Windows Storage Server 2012 (Todas edições);
1.1.207. Microsoft Windows Storage Server 2012 R2 (Todas edições);
1.1.208. Microsoft Windows Hyper-V Server 2012;
1.1.209. Microsoft Windows Hyper-V Server 2012 R2;
1.1.210. Windows Server 2016 Essentials/Standard/Datacenter/Core;
1.1.211. Windows Storage Server 2016;
1.1.212. Windows Hyper-V Server 2016.

Características:

1.1.213. Deve prover as seguintes proteções:
1.1.213.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
1.1.213.2. Auto-proteção contra-ataques aos serviços/processos do antivírus;
1.1.213.3. Firewall com IDS;
1.1.213.4. Controle de vulnerabilidades do Windows e dos aplicativos instalados;
1.1.214. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
1.1.215. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;
1.1.216. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
1.1.216.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
1.1.216.2. Gerenciamento de tarefa (criar ou excluir tarefas de verificação);
1.1.216.3. Leitura de configurações;
1.1.216.4. Modificação de configurações;
1.1.216.5. Gerenciamento de Backup e Quarentena;
1.1.216.6. Visualização de relatórios;
1.1.216.7. Gerenciamento de relatórios;
1.1.216.8. Gerenciamento de chaves de licença;
1.1.216.9. Gerenciamento de permissões (adicionar/excluir permissões acima);
1.1.217. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:
1.1.217.1. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;
1.1.217.2. Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.

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

1.1.219. Bloquear malwares tais como Cryptlockers mesmo quando o ataque vier de um computador sem antivírus na rede

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

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

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

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

1.1.224. Capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado no servidor;

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

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

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

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

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

1.1.230. Capacidade de verificar somente arquivos novos e alterados;

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

1.1.232. Capacidade de verificar objetos usando heurística;

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

1.1.234. Capacidade de agendar uma pausa na verificação;

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

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

1.1.236.1. Perguntar o que fazer, ou;
1.1.236.2. Bloquear acesso ao objeto;
1.1.236.2.1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
1.1.236.2.2. Caso positivo de desinfecção:
1.1.236.2.2.1. Restaurar o objeto para uso;
1.1.236.2.3. Caso negativo de desinfecção:
1.1.236.2.3.1. Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);

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

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

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

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

Funcionalidades Requeridas para Servidores Linux

Compatibilidade:

Plataforma 32-bits:

1.1.241. Red Hat Enterprise Linux 6.7;
1.1.242. Red Hat Enterprise Linux 6.8;
1.1.243. CentOS-6.7;
1.1.244. CentOS-6.8;
1.1.245. Ubuntu 14.04 LTS;
1.1.246. Ubuntu 16.04 LTS;
1.1.247. Ubuntu 16.10 LTS;
1.1.248. Debian GNU/Linux 7.10;
1.1.249. Debian GNU/Linux 7.11;
1.1.250. Debian GNU/Linux 8.6;
1.1.251. Debian GNU/Linux 8.7.

Plataforma 64-bits:

1.1.252. Red Hat Enterprise Linux 6.7;
1.1.253. Red Hat Enterprise Linux 6.8;
1.1.254. Red Hat Enterprise Linux 7.2;
1.1.255. Red Hat Enterprise Linux 7.3;
1.1.256. CentOS-6.7;
1.1.257. CentOS-6.8;
1.1.258. CentOS-7.2;
1.1.259. CentOS-7.3;

1.1.260. Ubuntu 14.04 LTS;
1.1.261. Ubuntu 16.04 LTS;
1.1.262. Ubuntu 16.10 LTS;
1.1.263. Debian GNU/Linux 7.10;
1.1.264. Debian GNU/Linux 7.11;
1.1.265. Debian GNU/Linux 8.6;
1.1.266. Debian GNU/Linux 8.7;
1.1.267. OpenSUSE 42.2;
1.1.268. SUSE Linux Enterprise Server 12;
1.1.269. OracleLinux 7.3;
1.1.270. Novell Open Enterprise Server 11 SP3;
1.1.271. Novell Open Enterprise Server 2015 SP1;

Características:

1.1.272. Deve prover as seguintes proteções:
1.1.273. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
1.1.274. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;
1.1.275. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
1.1.276. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
1.1.277. Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;
1.1.278. Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;
1.1.279. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados;
1.1.279.1. Em caso erros, deve ter capacidade de criar *logs* automaticamente, sem necessidade de outros softwares;
1.1.280. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
1.1.281. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;
1.1.282. Capacidade de verificar objetos usando heurística;
1.1.283. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;

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

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

Funcionalidades Requeridas para Smartphones e tablets

Compatibilidade:

1.1.285. Apple iOS 9.0-10.3;

1.1.286. Android 4.1 – 7.1.1

Características:

1.1.287. Deve prover as seguintes proteções:

1.1.287.1. Proteção em tempo real do sistema de arquivos do dispositivo – interceptação e verificação de:

1.1.287.2. Proteção contra adware e autodialers;

1.1.287.3. Todos os objetos transmitidos usando conexões wireless (porta de infravermelho, Bluetooth) e mensagens EMS, durante sincronismo com PC e ao realizar download usando o browser;

1.1.287.4. Arquivos abertos no smartphone;

1.1.287.5. Programas instalados usando a interface do smartphone

1.1.287.6. Verificação dos objetos na memória interna do smartphone e nos cartões de expansão sob demanda do usuário e de acordo com um agendamento;

1.1.288. Deverá isolar em área de quarentena os arquivos infectados;

1.1.289. Deverá atualizar as bases de vacinas de modo agendado;

1.1.290. Deverá bloquear spams de SMS através de Black lists;

1.1.291. Deverá ter função de bloqueio do aparelho caso o SIM CARD for trocado para outro não autorizado com mensagem de aviso ao utilizador do dispositivo;

1.1.292. Capacidade de desativar por política:

Wi-fi;

Câmera;

Bluetooth.

1.1.293. Deverá ter função de limpeza de dados pessoais a distância, em caso de roubo, por exemplo;

1.1.294. Capacidade de requerer uma senha para desbloquear o dispositivo e personalizar a quantidade de caracteres para esta senha;

1.1.295. Deverá ter firewall pessoal (Android);

1.1.296. Capacidade de tirar fotos quando a senha for inserida incorretamente;

1.1.297. Possibilidade de instalação remota utilizando o Microsoft System Center Mobile Device Manager 2008 SP1;

1.1.298. Capacidade de enviar comandos remotamente de:

1.1.298.1. Localizar;

1.1.298.2. Bloquear.

1.1.299. Capacidade de detectar Jailbreak em dispositivos iOS;

1.1.300. Capacidade de bloquear o acesso a site por categoria em dispositivos;

1.1.301. Capacidade de bloquear o acesso a sites phishing ou malicioso;

1.1.302. Capacidade de criar containers de aplicativos, separando dados corporativos de dados pessoais;

1.1.303. Capacidade de bloquear o dispositivo quando o cartão "SIM" for substituído;

1.1.304. Capacidade de configurar White e blacklist de aplicativos;

1.1.305. Capacidade de localizar o dispositivo quando necessário;

1.1.306. Permitir atualização das definições quando estiver em "roaming";

1.1.307. Capacidade de selecionar endereço do servidor para buscar a definição de vírus;

1.1.308. Deve permitir verificar somente arquivos executáveis;

1.1.309. Deve ter a capacidade de desinfectar o arquivo se possível;

1.1.310. Capacidade de agendar uma verificação;

1.1.311. Capacidade de enviar URL de instalação por e-mail;

1.1.312. Capacidade de fazer a instalação através de um link QRCode;

1.1.313. Capacidade de executar as seguintes ações caso a desinfecção falhe:

1.1.313.1. Deletar;

1.1.313.2. Ignorar;

1.1.313.3. Quarentenar;

1.1.313.4. Perguntar ao usuário.

Funcionalidades Requeridas para Gerenciamento de dispositivos móveis (MDM)

Compatibilidade:

1.1.314. Dispositivos conectados através do Microsoft Exchange ActiveSync:

1.1.314.1. Apple iOS;

1.1.314.2. Android.

1.1.315. Dispositivos com suporte ao Apple Push Notification (APNs).

1.1.315.1. Apple iOS 3.0 ou superior.

Características:

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

1.1.317. Capacidade de ajustar as configurações de:

1.1.317.1. Sincronização de e-mail;

1.1.317.2. Uso de aplicativos;

1.1.317.3. Senha do usuário;

1.1.317.4. Criptografia de dados;

1.1.317.5. Conexão de mídia removível.

1.1.318. Capacidade de instalar certificados digitais em dispositivos móveis;
1.1.319. Capacidade de, remotamente, resetar a senha de dispositivos iOS;
1.1.320. Capacidade de, remotamente, apagar todos os dados de dispositivos iOS;
1.1.321. Capacidade de, remotamente, bloquear um dispositivo iOS;
1.1.322. Deve permitir configurar horário para sincronização do dispositivo com a console de gerenciamento;
1.1.323. Possibilidade de exigir senha para abrir aplicações instaladas em container;
1.1.324. Deve permitir que o usuário utilize autenticação do Active Directory para abrir aplicações em container;
1.1.325. Deve permitir que uma senha seja digitada a cada x(minutos) para continuar utilizando uma aplicação em container;
1.1.326. Deve permitir a criptografia de dados salvos pelas aplicações em container;
1.1.327. Permitir sincronização com perfil do “Touch Down”;
1.1.328. Capacidade de desinstalar remotamente o antivírus do dispositivo;
1.1.329. Deve permitir fazer o upgrade do antivírus de forma remota sem a necessidade de desinstalar a versão atual;
1.1.330. Capacidade de sincronizar com Samsung Knox;
1.1.331. Deve permitir criar perfis de políticas para out-of-office no caso de BYOD.

Funcionalidades Requeridas de Criptografia

Compatibilidade

1.1.332. Microsoft Windows 7 Ultimate SP1 ou superior x86/x64;
1.1.333. Microsoft Windows 7 Enterprise SP1 ou superior x86/x64;
1.1.334. Microsoft Windows 7 Professional SP1 ou superior x86/x64;
1.1.335. Microsoft Windows 8 Enterprise x86/x64;
1.1.336. Microsoft Windows 8 Pro x86/x64;
1.1.337. Microsoft Windows 8.1 Pro x86/x64;
1.1.338. Microsoft Windows 8.1 Enterprise x86/x64;
1.1.339. Microsoft Windows 10 Enterprise x86/x64;
1.1.340. Microsoft Windows 10 Pro x86/x64;
1.1.341. Microsoft Windows Vista x86/x64 SP2 ou superior;
1.1.342. Microsoft Windows XP Professional x86 SP3 ou superior

Características

1.1.343. O acesso ao recurso criptografado (arquivo, pasta ou disco) deve ser garantido mesmo em caso o usuário tenha esquecido a senha, através de procedimentos de recuperação;

1.1.344. Utilizar, no mínimo, algoritmo AES com chave de 256 bits;

1.1.345. Capacidade de criptografar completamente o disco rígido da máquina, adicionando um ambiente de pré-boot para autenticação do usuário;

1.1.346. Capacidade de utilizar *Single Sign-On* para a autenticação de pré-boot;

1.1.347. Permitir criar vários usuários de autenticação pré-boot;

1.1.348. Capacidade de criar um usuário de autenticação pré-boot comum com uma senha igual para todas as máquinas a partir da console de gerenciamento;

1.1.349. Capacidade de criptografar drives removíveis de acordo com regra criada pelo administrador, com as opções:

1.1.349.1. Criptografar somente os arquivos novos que forem copiados para o disco removível, sem modificar os arquivos já existentes;

1.1.349.2. Criptografar todos os arquivos individualmente;

1.1.349.3. Criptografar o dispositivo inteiro, de maneira que não seja possível listar os arquivos e pastas armazenadas;

1.1.349.4. Criptografar o dispositivo em modo portátil, permitindo acessar os arquivos em máquinas de terceiros através de uma senha;

1.1.350. Capacidade de selecionar pastas e arquivos (por tipo, ou extensão) para serem criptografados automaticamente. Nesta modalidade, os arquivos devem estar acessíveis para todas as máquinas gerenciadas pela mesma console de maneira transparente para os usuários;

1.1.351. Capacidade de criar regras de exclusões para que certos arquivos ou pastas nunca sejam criptografados;

1.1.352. Capacidade de selecionar aplicações que podem ou não ter acesso aos arquivos criptografados;

1.1.353. Verifica compatibilidade de hardware antes de aplicar a criptografia;

1.1.354. Possibilita estabelecer parâmetros para a senha de criptografia;

1.1.355. Bloqueia o reuso de senhas;

1.1.356. Bloqueia a senha após um número de tentativas pré-estabelecidas;

1.1.357. Capacidade de permitir o usuário solicitar permissão a determinado arquivo criptografado para o administrador mediante templates customizados;

1.1.358. Permite criar exclusões para não criptografar determinados “discos rígidos” através de uma busca por nome do computador ou nome do dispositivo

1.1.359. Permite criptografar as seguintes pastas pré-definidas: “meus documentos”, “Favoritos”, “Desktop”, “Arquivos temporários” e “Arquivos do outlook”;

1.1.360. Permite utilizar variáveis de ambiente para criptografar pastas customizadas;

1.1.361. Capacidade de criptografar arquivos por grupos de extensão, tais como: Documentos do office, Document, arquivos de audio, etc;

1.1.362. Permite criar um grupo de extensões de arquivos a serem criptografados;

1.1.363. Capacidade de criar regra de criptografia para arquivos gerados por aplicações;
1.1.364. Permite criptografia de dispositivos móveis mesmo quando o endpoint não possuir comunicação com a console de gerenciamento.
1.1.365. Capacidade de deletar arquivos de forma segura após a criptografia;
1.1.366. Capacidade de criptografar somente o espaço em disco utilizado;
1.1.367. Deve ter a opção de criptografar arquivos criados a partir de aplicações selecionadas pelo administrador;
1.1.368. Capacidade de bloquear aplicações selecionadas pelo administrador de acessarem arquivos criptografados;
1.1.369. Deve permitir criptografar somente o espaço utilizado em dispositivos removíveis tais como pendrives, HD externo, etc;
1.1.370. Capacidade de criptografar discos utilizando a criptografia BitLocker da Microsoft;
1.1.371. Deve ter a opção de utilização de TPM para criptografia através do BitLocker;
1.1.372. Capacidade de fazer “Hardware encryption”;

Funcionalidades Requeridas para Gerenciamento de Sistemas

1.1.373. Capacidade de criar imagens de sistema operacional remotamente e distribuir essas imagens para computadores gerenciados pela solução e para computadores *bare-metal*;
1.1.374. Deve possibilitar a utilização de servidores PXE na rede para deploy de imagens;

1.1.375. Capacidade de detectar softwares de terceiros vulneráveis, criando assim um relatório de softwares vulneráveis;
1.2. Capacidade de corrigir as vulnerabilidades de softwares, fazendo o download centralizado da correção ou atualização e aplicando essa correção ou atualização nas máquinas gerenciadas de maneira transparente para os usuários;
1.3. Capacidade de gerenciar licenças de softwares de terceiros;
1.4. Capacidade de registrar mudanças de hardware nas máquinas gerenciadas;
1.5. Capacidade de gerenciar um inventário de hardware, com a possibilidade de cadastro de dispositivos (ex: router, switch, projetor, acessório, etc), informando data de compra, local onde se encontra, service tag, número de identificação e outros;
1.6. Possibilita fazer distribuição de software de forma manual e agendada;
1.7. Suporta modo de instalação silenciosa;
1.8. Suporte a pacotes MSI, exe, bat, cmd e outros padrões de arquivos executáveis;
1.9. Possibilita fazer a distribuição através de agentes de atualização;
1.10. Utiliza tecnologia multicast para evitar tráfego na rede;
1.11. Possibilita criar um inventário centralizado de imagens;
1.12. Capacidade de atualizar o sistema operacional direto da imagem mantendo os dados do usuário;
1.13. Suporte a WakeOnLan para deploy de imagens;

1.14. Capacidade de atuar como servidor de atualização do Windows podendo fazer deploy de patches;
1.15. Suporta modo de teste, podendo atribuir alguns computadores para receberem as atualizações de forma automática para avaliação de alterações no comportamento;
1.16. Capacidade de gerar relatórios de vulnerabilidades e patches;
1.17. Possibilita criar exclusões para aplicação de patch por tipo de sistema operacional, Estação de trabalho e Servidor ou por grupo de administração;
1.18. Permite iniciar instalação de patch e correções de vulnerabilidades ao reiniciar ou desligar o computador;
1.19. Permite baixar atualizações para o computador sem efetuar a instalação
1.20. Permite o administrador instalar somente atualizações aprovadas, instalar todas as atualizações (exceto as bloqueadas) ou instalar todas as atualizações incluindo as bloqueadas;
1.21. Capacidade de instalar correções de vulnerabilidades de acordo com a severidade;
1.22. Permite selecionar produtos a serem atualizados pela console de gerenciamento;
1.23. Permite selecionar categorias de atualizações para serem baixadas e instaladas, tais como: atualizações de segurança, ferramentas, drivers, etc;
1.24. Capacidade de adicionar caminhos específicos para procura de vulnerabilidades e atualizações em arquivos;
1.25. Capacidade de instalar atualizações ou correções somente em computadores definidos, em grupos definidos ou em uma porcentagem de computadores conforme selecionado pelo administrador;
1.26. Capacidade de configurar o reinicio do computador após a aplicação das atualizações e correções de vulnerabilidades;
1.27. Deve permitir selecionar o idioma das aplicações que serão atualizadas;
1.28. Permitir agendar o sincronismo entre a console de gerenciamento e os sites da Microsoft para baixar atualizações recentes;