



SERVIÇO PÚBLICO FEDERAL

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

**EDITAL DE PREGÃO ELETRÔNICO Nº 010/2018
PROCESSO ADMINISTRATIVO Nº L-175/2017**

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 Contratos e Licitação - UCL, sediada à Avenida Brigadeiro Faria Lima, 1.059 – Pinheiros – São Paulo – SP, CEP 01452-920, realizará licitação, na modalidade PREGÃO, na forma ELETRÔNICA, do **TIPO MENOR PREÇO**, nos termos da Lei nº 10.520, de 17 de julho de 2002, do Decreto nº 5.450, de 31 de maio de 2005, do Decreto 2.271, de 7 de julho de 1997, do Decreto nº 7.746, de 05 de junho de 2012, das Instruções Normativas SEGES/MPDG nº 05, de 26 de maio de 2017, e nº 02, de 11 de outubro de 2010 e nº 01, de 19 de janeiro de 2010, da Lei Complementar nº 123, de 14 de dezembro de 2006, aplicando-se, subsidiariamente, a Lei nº 8.666, de 21 de junho de 1993, e as exigências estabelecidas neste Edital.

DATA DA SESSÃO: **11/04/2018**

HORÁRIO: 9 horas e 30 minutos - abertura das propostas;

HORÁRIO: 10 horas e 30 minutos - realização do pregão;

LOCAL: ENDEREÇO ELETRÔNICO: www.licitacoes-e.com.br.

1 DO OBJETO

1.1 O objeto desta licitação é a escolha da proposta mais vantajosa para a contratação de empresa para fornecimento de software antivírus para o CREA-SP, incluindo instalação configuração e treinamento do software conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.

2 DOS RECURSOS ORÇAMENTÁRIOS

2.1 As despesas para atender a esta licitação estão programadas em dotação orçamentária própria, oriundo das contas nºs 6.2.2.1.1.02.02.05.001 – Direito de Uso Software e 6.2.2.1.1.01.04.09.005 – Serviços de Informática.

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 2.2 A despesa com a execução dos serviços de que trata o objeto desta licitação é estimada no total de R\$ 206.150,67 (duzentos e seis mil, cento e cinquenta reais e sessenta e sete centavos).

3 DO CREDENCIAMENTO

- 3.1 O Credenciamento é o nível básico de registro junto ao provedor do sistema, que permite a participação dos interessados na modalidade licitatória Pregão, em sua forma eletrônica.
- 3.2 Somente poderá participar deste Pregão Eletrônico o LICITANTE devidamente credenciado junto ao provedor do sistema na página eletrônica do Banco do Brasil www.licitacoes-e.com.br, nos termos do art. 3º do Decreto nº 5.450/05.
- 3.3 O credenciamento dar-se-á pela atribuição de chave de identificação e de senha pessoal e intransferível, para acesso ao sistema eletrônico.
- 3.4 O credenciamento junto ao provedor do sistema implica a responsabilidade legal do LICITANTE ou de seu representante legal e a presunção de sua capacidade técnica para realização das transações inerentes ao Pregão Eletrônico.
- 3.5 O uso da senha de acesso pelo LICITANTE é de sua responsabilidade exclusiva, incluindo qualquer transação efetuada diretamente ou por seu representante, não cabendo ao provedor do sistema ou a este Conselho, responsabilidade por eventuais danos decorrentes do uso indevido da senha, ainda que por terceiros.
- 3.6 A perda da senha ou a quebra de sigilo deverão ser comunicadas imediatamente ao provedor do sistema para imediato bloqueio de acesso.

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 junto ao provedor do sistema na página eletrônica do Banco do Brasil www.licitacoes-e.com.br, nos termos do art. 3º do Decreto nº 5.450/05.
- 4.2 Não poderão participar desta licitação os interessados:

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 4.2.1 proibidos de participar de licitações e celebrar contratos administrativos, na forma da legislação vigente;
- 4.2.2 estrangeiros que não tenham representação legal no Brasil com poderes expressos para receber citação e responder administrativamente ou judicialmente;
- 4.2.3 que se enquadrem nas vedações previstas no artigo 9º da Lei nº 8.666, de 1993;
- 4.2.4 que estejam sob falência, em recuperação judicial ou extrajudicial, concurso de credores ou insolvência, em processo de dissolução ou liquidação;
- 4.2.5 entidades empresariais que estejam reunidas em consórcio;
- 4.2.6 Sociedades Cooperativas.
- 4.3 Como condição para participação no Pregão, o licitante declarará em campo próprio do sistema eletrônico, relativo às seguintes declarações:
 - 4.3.1 que cumpre os requisitos estabelecidos no art. 3º da Lei Complementar nº 123, de 2006, estando apta a usufruir do tratamento favorecido estabelecido em seus arts. 42 a 49.
 - 4.3.1.1 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 Microempresas ou Empresa de Pequeno Porte.
 - 4.3.2 que está ciente e concorda com as condições contidas no Edital e seus anexos, bem como de que cumpre plenamente os requisitos de habilitação definidos no Edital.
 - 4.3.3 que inexistem fatos impeditivos para sua habilitação no certame, ciente da obrigatoriedade de declarar ocorrências posteriores.
 - 4.3.4 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 art. 7º, XXXIII, da Constituição.
 - 4.3.5 que a proposta foi elaborada de forma independente, nos termos da Instrução Normativa SLTI nº 2, de 16 de setembro de 2009.

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP****5 DO ENVIO DA PROPOSTA**

- 5.1 O LICITANTE deverá encaminhar a proposta por meio do sistema eletrônico até a data e horário marcados para abertura da sessão, quando, então, encerrar-se-á automaticamente a fase de recebimento de propostas.
- 5.2 Todas as referências de tempo no Edital, no aviso e durante a sessão pública observarão o horário de Brasília – DF.
- 5.3 O LICITANTE será responsável por todas as transações que forem efetuadas em seu nome no sistema eletrônico, assumindo como firmes e verdadeiras suas propostas e lances.
- 5.4 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.
- 5.5 Até a abertura da sessão, os LICITANTES poderão retirar ou substituir as propostas apresentadas.
- 5.6 O LICITANTE deverá enviar sua proposta mediante o preenchimento, no sistema eletrônico, do campo Valor Total do Lote com o **VALOR TOTAL GERAL DO LOTE** proposto para o objeto desta licitação.
- 5.6.1 O Pregoeiro verificará as propostas inseridas por meio do sistema eletrônico e desclassificará, motivadamente, aquela que não esteja em conformidade com os requisitos estabelecidos neste Edital e seus anexos.
- 5.6.2 **Qualquer elemento que possa identificar o LICITANTE** nas informações adicionais ou em documento que venha a ser anexado no Sistema Eletrônico importa a **desclassificação da proposta**, sem prejuízo das sanções previstas nesse Edital.
- 5.7 Todas as especificações do objeto contidas na proposta vinculam a CONTRATADA.

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 5.8 A proposta comercial, a ser enviada *posteriormente* pelo **Arrematante**, observado o disposto no item “8.7”, deverá ser composta considerando o descrito no Termo de Referência – anexo I deste Edital e conforme segue:

Lote – “1” - (único)

Item	Descrição	Quant.	Valor Unitário	Valor Total
1	Aquisição de Software de Antivírus. A validade da licenças será perpétua, mas as atualizações da solução de antivírus terão validade de 36 (trinta e seis) meses.	1100 (Unidades)	R\$	R\$
2	Instalação, configuração e treinamento do Software.	80 (horas)	R\$	R\$
Valor Total Geral do Lote = Item 1 + Item 2.....				R\$

- 5.9 Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente na prestação dos serviços.
- a) A CONTRATADA deverá arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, tais como os valores providos com o quantitativo de vale transporte, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto da licitação, exceto quando ocorrer algum dos eventos arrolados nos incisos do §1º do art. 57 da Lei nº 8.666, de 1993.
- b) Caso o eventual equívoco no dimensionamento dos quantitativos se revele superior às necessidades da CONTRATANTE, a Administração deverá efetuar o pagamento seguindo estritamente as regras contratuais de faturamento dos serviços demandados e executados, concomitantemente com a realização, se necessário e cabível, de adequação contratual do quantitativo necessário, com base na alínea “b” do inciso I do art. 65 da Lei nº 8.666/93 e nos termos do art. 63, § 2º da IN SEGES/MPDG nº 5/2017.
- 5.10 Prazo de validade da proposta não será inferior a 60 (sessenta) dias, a contar da data de sua apresentação.

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP****6 DA FORMULAÇÃO DE LANCES E JULGAMENTO DAS PROPOSTAS**

- 6.1 A abertura da presente licitação dar-se-á em sessão pública, por meio de sistema eletrônico, na data, horário e local indicados neste Edital.
- 6.2 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 técnicas exigidas no Termo de Referência.
- a) a desclassificação será sempre fundamentada e registrada no sistema.
- b) a não desclassificação da proposta não impede o seu julgamento definitivo em sentido contrário, levado a efeito na fase de aceitação.
- 6.3 O sistema ordenará automaticamente as propostas classificadas, sendo que somente estas participarão da fase de lances.
- 6.4 O sistema disponibilizará campo próprio para troca de mensagem entre o Pregoeiro e os LICITANTES.
- 6.5 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.
- a) o lance deverá ser ofertado pelo **VALOR TOTAL GERAL DO LOTE.**
- b) os LICITANTES poderão oferecer lances sucessivos, observando o horário fixado para abertura da sessão e as regras estabelecidas no Edital.
- 6.6 O LICITANTE somente poderá oferecer lance inferior ao último por ele ofertado e registrado pelo sistema.
- 6.7 Não serão aceitos dois ou mais lances de mesmo valor, prevalecendo aquele que for recebido e registrado em primeiro lugar.

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 6.8 Durante o transcurso da sessão pública, os LICITANTES serão informados, em tempo real, do valor do menor lance registrado, vedada a identificação do LICITANTE.
- 6.9 No caso de desconexão com o Pregoeiro, no decorrer da etapa competitiva do Pregão, o sistema eletrônico poderá permanecer acessível aos licitantes para a recepção dos lances.
- 6.10 Se a desconexão perdurar por tempo superior a 10 (dez) minutos, a sessão será suspensa e terá reinício somente após comunicação expressa do Pregoeiro aos participantes.
- 6.11 O critério de julgamento adotado será o menor preço, conforme definido neste Edital e seus anexos.
- 6.12 A etapa de lances da sessão pública será encerrada por decisão do Pregoeiro. O sistema eletrônico encaminhará aviso de fechamento iminente dos lances, após o que transcorrerá período de tempo de até 30 (trinta) minutos, aleatoriamente determinado pelo sistema, findo o qual será automaticamente encerrada a recepção de lances.
- 6.13 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.
- 6.14 Encerrada a etapa de lances, será efetivada a verificação automática, junto à Receita Federal, do porte de entidade empresarial. O sistema identificará em coluna própria as microempresas e as 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 Lei Complementar nº 123, de 2006, regulamentada pelo Decreto nº 8.538, de 2015.

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 6.15 Nessas condições, as propostas de microempresas e empresas de pequeno porte que se encontrem na faixa de até 5% (cinco por cento) acima da proposta ou lance de menor preço serão consideradas empatadas com a primeira colocada.
- 6.16 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 5 (cinco) minutos controlados pelo sistema, contados após a comunicação automática para tanto.
- 6.17 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.
- 6.18 Só se aplica o sorteio quando houver empate entre as propostas e ausência de lances. Lances equivalentes não serão considerados iguais, vez que a ordem de apresentação pelos licitantes é utilizada como um dos critérios de classificação.

7 DA ACEITABILIDADE DA PROPOSTA VENCEDORA.

- 7.1 Encerrada a etapa de lances e depois da verificação de possível empate, o Pregoeiro examinará a proposta classificada em primeiro lugar quanto ao preço, a sua exequibilidade, bem como quanto ao cumprimento das especificações do objeto.
- 7.2 Será desclassificada a proposta ou o lance vencedor que:
- 7.2.1 contenha vício insanável ou ilegalidade;
- 7.2.2 não apresente as especificações técnicas exigidas pelo Termo de Referência;
- 7.2.3 apresentar preço final superior ao preço máximo fixado, ou que apresentar preço manifestamente inexequível.
- 7.2.3.1 Considera-se inexequível a proposta de preços ou menor lance que:

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- a) comprovadamente, 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.
- b) apresentar um ou mais valores da planilha de custo que sejam inferiores àqueles fixados em instrumentos de caráter normativo obrigatório, tais como leis, medidas provisórias e convenções coletivas de trabalho vigentes.

7.3 Se houver indícios de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, poderão ser efetuadas diligências, na forma do § 3º do art. 43 da Lei nº 8.666, de 1993, para efeito de comprovação de sua exequibilidade, podendo ser adotado, dentre outros, os seguintes procedimentos:

- a) questionamentos junto à proponente para apresentação de justificativas e comprovações em relação aos custos com indícios de inexequibilidade;
- b) verificação de outros contratos que o proponente mantenha com a Administração ou com a iniciativa privada.

7.4 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 planilha de custos, não sendo possível a sua imediata desclassificação, será obrigatória a realização de diligências para aferir a legalidade e exequibilidade da proposta.

7.5 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.

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 7.6 O Pregoeiro poderá convocar o LICITANTE para enviar documento digital, por meio de funcionalidade disponível no sistema, estabelecendo no “chat” prazo mínimo de 30 (trinta) minutos, sob pena de não aceitação da proposta.
- 7.6.1 O prazo estabelecido pelo Pregoeiro poderá ser prorrogado por solicitação escrita e justificada do LICITANTE, formulada antes de findo o prazo estabelecido, e formalmente aceita pelo Pregoeiro.
- 7.6.2 Dentre os documentos passíveis de solicitação pelo Pregoeiro, destacam-se as planilhas de custo readequadas com o valor final ofertado.
- 7.6.3 Todos os dados informados pelo licitante em sua planilha deverão refletir com fidelidade os custos especificados e a margem de lucro pretendida.
- 7.6.4 O Pregoeiro, com apoio da área técnica, analisará a compatibilidade dos preços unitários apresentados na Proposta Comercial com aqueles praticados no mercado em relação aos insumos e também quanto aos salários das categorias envolvidas na contratação.
- 7.6.5 Erros no preenchimento da Proposta Comercial não constituem motivo para a desclassificação da proposta. A proposta comercial poderá ser ajustada pelo LICITANTE, no prazo indicado pelo Pregoeiro, desde que não haja majoração do preço proposto.
- 7.7 Se a proposta ou lance vencedor for desclassificado, o Pregoeiro examinará a proposta ou lance subsequente, e, assim sucessivamente, na ordem de classificação.
- 7.8 Havendo necessidade, o Pregoeiro suspenderá a sessão, informando no “chat” a nova data e horário para a continuidade da mesma.
- 7.9 O Pregoeiro poderá encaminhar, por meio do sistema eletrônico, contraproposta ao LICITANTE que apresentou o lance mais vantajoso, com o fim de negociar a obtenção de melhor preço, vedada a negociação em condições diversas das previstas neste Edital.
- 7.9.1 Também nas hipóteses em que o Pregoeiro não aceitar a proposta e passar à subsequente, poderá negociar com o licitante para que seja obtido preço melhor.

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

7.9.2 A negociação será realizada por meio do sistema, podendo ser acompanhada pelos demais LICITANTES.

8 DA HABILITAÇÃO

8.1 Para habilitação no processo licitatório o **LICITANTE ARREMATANTE DO LANCE** deverá apresentar a documentação em conformidade com o disposto abaixo:

8.1.1 **Para empresa Registrada no Cadastro de Fornecedores do CREA-SP**, a documentação exigida no item “8.2” e alíneas “a”, “c”, “d”, “e” e “f”.

8.1.2 **Para empresa não Registrada no Cadastro de Fornecedores do CREA-SP**, a documentação exigida no item “8.2” e suas alíneas, “b” (b.1.1 a b.2.5)”, “c”, “d”, “e” e “f”.

8.2 Da Documentação**8.2.a Registrada no Cadastro de Fornecedores do CREA-SP**

8.2.a.1 Declaração comprovando que o LICITANTE encontra-se registrado no Registro Cadastral de Fornecedores do CREA-SP, devendo, se for o caso, atualizar seus documentos.

8.2.b Não Registrada no Cadastro de Fornecedores do CREA-SP, que comprove possuir os requisitos de habilitação jurídica e regularidade fiscal constantes das alíneas “b.1” e “b.2” abaixo:

8.2.b.1 Jurídica:

8.2.b.1.1 Registro comercial, no caso de empresa individual;

8.2.b.1.2 Ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado, em se tratando de sociedades comerciais, e, no caso de sociedades por ações, acompanhado de documentos de eleição de seus administradores;

8.2.b.1.3 Inscrição do ato constitutivo, no caso de sociedades civis, acompanhada de prova de diretoria em exercício;

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

8.2.b.1.4 Decreto de autorização, em se tratando de empresa ou sociedade estrangeira em funcionamento no País, e ato de registro ou autorização para funcionamento expedido pelo órgão competente, quando a atividade assim o exigir.

8.2.b.2 Regularidade Fiscal e Trabalhista:

8.2.b.2.1 Prova de regularidade relativa ao Fundo de Garantia do Tempo de Serviços (FGTS);

8.2.b.2.2 Prova de regularidade para com a Fazenda Federal, que abrange também a prova de regularidade relativa à Seguridade Social (conforme Portarias nºs 358, de 5 de setembro de 2014 e 1751, de 2 de outubro de 2014);

8.2.b.2.3 Prova de regularidade para com a Fazenda Estadual, do domicílio ou sede do LICITANTE, ou outra equivalente, na forma da Lei.

8.2.b.2.4 Prova de regularidade para com a Fazenda Municipal, do domicílio ou sede do LICITANTE, ou outra equivalente, na forma da Lei;

8.2.b.2.5 Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de **CNDT** (Certidão Negativa de Débitos Trabalhistas), 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.

8.2.c Qualificação Técnica

8.2.c.1 Comprovação de aptidão para a prestação dos serviços em características, quantidades e prazos compatíveis com o objeto desta licitação, ou com o item pertinente, mediante a apresentação de atestados fornecidos por pessoas jurídicas de direito público ou privado.

8.2.c.1.1 As informações contidas no(s) atestado(s) estarão sujeitas à verificação de sua veracidade por parte do Pregoeiro e equipe de apoio do CREA-SP.

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

8.2.c.2 Os atestados deverão referir-se a serviços prestados no âmbito de sua atividade econômica principal ou secundária especificadas no contrato social vigente;

8.2.c.4 O LICITANTE disponibilizará 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.

8.2.d Qualificação Econômico-Financeira

8.2.d.1 Certidão negativa de falência ou recuperação judicial ou extrajudicial expedida pelo cartório distribuidor da sede da pessoa jurídica, datada de, no máximo, 90 (noventa) dias anteriores à data limite para entrega das propostas.

8.2.d.1.1 Sendo a certidão positiva, deverá ser apresentada "Certidão de Objeto e Pé" atualizada referente à ação judicial existente, para constatação ou não de fator impeditivo de habilitação.

8.2.d.2 No caso de praças com mais de um cartório distribuidor, deverão ser apresentadas as certidões de cada um dos distribuidores.

8.2.d.3 Fica dispensada a apresentação da certidão citada nesta cláusula os LICITANTE que se enquadrar como cooperativa, de acordo com o artigo 4º da Lei nº 5.764, de 16 de dezembro de 1971.

8.2.d.4 Balanço patrimonial e demonstrações contábeis do último exercício social, já exigíveis e apresentados na forma da lei, vedada a sua substituição por balancetes ou balanços provisórios, a saber:

a) sociedades empresariais em geral: registrado ou autenticado na Junta Comercial da sede ou do domicílio do LICITANTE, acompanhado de cópia do termo de abertura e de encerramento do Livro Diário do qual foi extraído (art. 5º, § 2º, do Decreto-Lei nº 486, de 03 de março de 1969);

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- b) sociedades empresárias, especificamente no caso de sociedades anônimas regidas pela Lei nº 6.404, 15 de dezembro de 1976: registrado ou autenticado na Junta Comercial da sede ou domicílio do LICITANTE e publicado em Diário Oficial e em jornal de grande circulação (art. 289, caput e § 5º da mesma Lei);
- c) sociedades simples: registrado no Registro Civil das Pessoas Jurídicas do local de sua sede; caso a sociedade simples adote um dos tipos de sociedade empresária, deverá sujeitar-se às normas fixadas para as sociedades empresariais, inclusive quanto ao registro na Junta Comercial;
- d) sociedades cooperativas: arquivo dos documentos pertinentes na Junta Comercial do Estado onde estiver sediada (Lei nº 5.764, de 16 de dezembro de 1971);

8.2.d.4.1 Sociedades constituídas no exercício em curso ou com menos de 01 (um ano) deverão apresentar balanço conforme abaixo discriminado, com a assinatura do responsável por sua contabilidade e do sócio-gerente, devidamente registrado ou autenticado na Junta Comercial da sede ou do domicílio do LICITANTE:

- a) balanço de abertura – sociedades sem movimentação;
- b) balanço intermediário – sociedades com movimentação.

8.2.d.5 A comprovação da boa situação financeira do LICITANTE será feita por meio da avaliação, conforme o caso:

- a) do balanço referido no item “8.2.d.4”, cujos índices de Liquidez Geral (**LG**), de Solvência Geral (**SG**) e de Liquidez Corrente (**LC**), resultantes da aplicação das fórmulas a seguir, terão de ser maiores que um (>1):

$$\text{LG} = \frac{\text{Ativo Circulante} + \text{Realizável a Longo Prazo}}{\text{Passivo Circulante} + \text{Exigível a Longo Prazo}}$$

$$\text{SG} = \frac{\text{Ativo Total}}{\text{Passivo Circulante} + \text{Exigível a Longo Prazo}}$$

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

$$LC = \frac{\text{Ativo Circulante}}{\text{Passivo Circulante}}$$

- b) do balanço referido no item “8.2.d.4.1”, cujo Índice de Solvência, obtido conforme fórmula a seguir, terá de ser maior que um (> 1):

$$S = \frac{\text{Ativo Total}}{\text{Passivo Circulante + Exigível a Longo Prazo}}$$

8.2.d.6 Os índices de que tratam as alíneas “a” e “b” do subitem “8.2.d.5” serão calculados preferencialmente pelo LICITANTE e confirmados pelo responsável por sua contabilidade, mediante sua assinatura e a indicação do seu nome e do número de registro no Conselho Regional de Contabilidade.

8.2.d.7 O LICITANTE que apresentar resultado igual ou menor que 1 (um) nos cálculos de quaisquer dos índices referidos na alínea “a” ou “b”, ambos do subitem “8.2.d.5”, para ser considerada atendida a referida exigência deverá incluir comprovante de que possui patrimônio líquido mínimo ou capital mínimo equivalente a 10% (dez por cento) do valor total estimado para o(s) respectivo(s) lote(s).

8.2.e Deverá apresentar obrigatoriamente, as seguintes declarações:

8.2.e.1 Declaração expressa do LICITANTE, conforme Decreto nº 4.358, de 05 de setembro de 2002, de que não existe na empresa, trabalhador nas situações previstas no inciso XXXIII do Art. 7º da Constituição Federal, (conforme modelo constante no anexo III);

8.2.e.2 Declaração expressa do LICITANTE de que é Microempresa ou Empresa de Pequeno Porte – Lei Complementar nº 123, de 14 de dezembro de 2006, se for o caso, (conforme modelo constante no anexo V);

8.2.e.3 Declaração de que está ciente e concorda com as condições contidas no ato convocatório e seus anexos, bem como de que cumpre plenamente os requisitos de habilitação definidos no referido documento;

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 8.2.e.4 Declaração, sob as penas da lei, de que até a presente data inexistem fatos impeditivos para a sua habilitação no presente processo licitatório, ciente da obrigatoriedade de declarar ocorrências posteriores;
- 8.2.e.5 Declaração de que a proposta apresentada para essa licitação foi elaborada de maneira independente;
- 8.2.e.6 Declaração de 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;
- 8.2.e.7 Declaração informando se os serviços são produzidos ou 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.
- 8.3 O interessado em obter ou atualizar a declaração do Registro de Cadastro de Fornecedores do CREA-SP solicitada no item “8.2.a.1” deverá preencher o formulário Ficha Cadastral de Fornecedores (anexo IV do Edital) e apresentá-lo devidamente preenchido e assinado, juntamente com os documentos relacionados no mesmo, na Unidade de Contratos e Licitação, na Avenida Brigadeiro Faria Lima, 1059, 7º andar – Pinheiros, São Paulo, SP – das 8h30min às 16h30min.
- 8.4 Não serão aceitos protocolos de entrega ou solicitação de documentos em substituição aos documentos requeridos neste Edital e seus anexos.
- 8.5 Os documentos para habilitação deverão ser entregues nos seus respectivos originais ou por cópia autenticada pelos cartórios competentes, vigentes na data de apresentação da proposta.

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 8.6 Para fins de habilitação o LICITANTE classificado provisoriamente em primeiro lugar deverá enviar, **NO PRAZO DE ATÉ 03 (TRÊS) HORAS, DENTRO DO HORÁRIO DE EXPEDIENTE, APÓS A SOLICITAÇÃO DO PREGOEIRO** a proposta de preço adequada ao último lance, devidamente preenchida conforme o disposto no Edital, bem como a documentação exigida nesta cláusula para o e-mail compras.licitacao@creasp.org.br, devendo o LICITANTE encaminhar posteriormente a proposta de preço e os documentos originais ou cópias autenticadas, no prazo máximo de 03 (três) dias úteis, contados da transmissão do *e-mail* para a Unidade de Contratos e Licitação, na Avenida Brigadeiro Faria Lima, 1059 – 7º andar – Pinheiros - São Paulo, SP, CEP – 01452-920, aos cuidados do Pregoeiro.
- 8.6.1 Em ocorrendo a solicitação após às 16h30min, o prazo de até 03 (três) horas, após a solicitação do pregoeiro, será computado a partir das 8h30min do primeiro dia útil subsequente.
- 8.7 Não serão aceitos documentos com indicação de CNPJ/CPF diferentes, salvo aqueles legalmente permitidos.
- 8.8 Constando o atendimento das exigências previstas no Edital e seus anexos, o LICITANTE será declarado vencedor, sendo-lhe adjudicado o objeto da licitação, na hipótese de inexistência de recursos ou, se o LICITANTE classificado em primeiro lugar desatender às exigências habilitatórias, o Pregoeiro examinará a oferta subsequente na ordem de classificação, verificando a sua aceitabilidade e procedendo a sua habilitação, repetindo esse procedimento sucessivamente, se for necessário, até a apuração de uma proposta que atenda ao Edital, sendo o respectivo LICITANTE declarado vencedor.
- 8.9 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:

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 8.9.1 SICAF;
- 8.9.2 Cadastro Nacional de Empresas Inidôneas e Suspensas – CEIS, mantido pela Controladoria-Geral da União (www.portaldatransparencia.gov.br/ceis);
- 8.9.3 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);
- 8.9.4 Lista de Inidôneos, mantida pelo Tribunal de Contas da União – TCU;
- 8.9.5 A consulta aos cadastros será realizada em nome da empresa LICITANTE e também de seu sócio majoritário, por força do art. 12 da Lei nº 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.
- 8.9.6 Constatada a existência de sanção, o Pregoeiro reputará o LICITANTE inabilitado, por falta de condição de participação.
- 8.10 Caso o Pregoeiro não logre êxito em obter a certidão correspondente através do sítio oficial, ou na hipótese de se encontrar vencida no referido sistema o LICITANTE será convocado a encaminhar, no prazo de 02 (duas) horas, documento válido que comprove o atendimento das exigências deste Edital, sob pena de inabilitação, ressalvado o disposto quanto à comprovação da regularidade fiscal das licitantes qualificadas como microempresas ou empresas de pequeno porte, conforme estatui o art. 43, § 1º da LC nº 123, de 2006.
- 8.11 A existência de restrição relativamente à regularidade fiscal não impede que o LICITANTE qualificada como microempresa ou empresa de pequeno porte seja declarada vencedora, uma vez que atenda a todas as demais exigências do edital.
- 8.11.1 A declaração do vencedor acontecerá em momento posterior à fase de habilitação.

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 8.12 Caso a proposta mais vantajosa seja ofertada por microempresa, empresa de pequeno porte ou sociedade cooperativa equiparada, e uma vez constatada a existência de alguma restrição no que tange à regularidade fiscal, 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.
- 8.13 A não regularização fiscal no prazo previsto no subitem anterior acarretará a inabilitação do LICITANTE, sem prejuízo das sanções previstas neste Edital, com a reabertura da sessão pública.
- 8.14 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.
- 8.15 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.
- 8.16 No caso de 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.
- 8.17 Da sessão pública do Pregão divulgar-se-á Ata no sistema eletrônico.

9 DA REABERTURA DA SESSÃO PÚBLICA

- 9.1 A sessão pública poderá ser reaberta:
- 9.1.1 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.



SERVIÇO PÚBLICO FEDERAL

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

- 9.1.2 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, nos termos do art. 43, §1º da LC nº 123/2006. Nessas hipóteses, serão adotados os procedimentos imediatamente posteriores ao encerramento da etapa de lances.
- 9.2 Todos os LICITANTES remanescentes deverão ser convocados para acompanhar a sessão reaberta.
- 9.2.1 A convocação se dará por meio do sistema eletrônico (chat) ou, *e-mail*, de acordo com a fase do procedimento licitatório.
- 9.2.2 A convocação feita por *e-mail* dar-se-á de acordo com os dados contidos no Sistema eletrônico, sendo responsabilidade do LICITANTE manter seus dados cadastrais atualizados.

10 DO ENCAMINHAMENTO DA PROPOSTA VENCEDORA

- 10.1 A proposta final do LICITANTE declarado vencedor (arrematante) deverá ser encaminhada no **prazo de até 03 (três) horas**, a contar da solicitação do Pregoeiro no sistema eletrônico, conforme item “8.7” deste Edital e, deverá:
- 10.1.1 Ser redigida em língua portuguesa, datilografada ou digitada, em uma via, sem emendas, rasuras, entrelinhas ou ressalvas, devendo a última folha ser assinada e as demais rubricadas pelo LICITANTE ou seu representante legal.
- 10.1.2 Apresentar a formação de preços, devidamente ajustada ao lance vencedor, em conformidade com o modelo anexo a este instrumento convocatório.
- 10.1.3 O valor deverá ser apresentado em moeda corrente nacional, fixo e irrevogável, para o período da contratação.
- 10.1.4 Conter a indicação do banco, número da conta e agência do LICITANTE vencedor, para fins de pagamento.

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 10.1.5 Para fins de assinatura do futuro contrato, informar:
- a) razão Social;
 - b) CNPJ, Inscrição Estadual e Municipal;
 - c) endereço completo da empresa, inclusive CEP;
 - d) nome, número do CPF, número do RG e cargo do Representante Legal da empresa com poderes para assinatura do contrato;
 - e) nome, número do CPF, número do RG do responsável (preposto), que deverá ser mantido, aceito pelo CREA-SP, para representá-la na execução do contrato.
- 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 vinculam a CONTRATADA.
- 11 DOS RECURSOS**
- 11.1 O Pregoeiro declarará o vencedor e, depois de decorrida a fase de regularização fiscal de microempresa ou empresa de pequeno porte, se for o caso, concederá o prazo de até 24 (vinte e quatro) horas corridas contadas da declaração, 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 eletrônico, que abrirá a opção **“acolhimento de recurso”**.
- 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.



SERVIÇO PÚBLICO FEDERAL

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

- 11.2.2 A falta de manifestação motivada do licitante quanto à intenção de recorrer importará a decadência desse direito.
- 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.
- 11.3 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 ADJUDICAÇÃO E HOMOLOGAÇÃO

- 12.1 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.
- 12.2 Após a fase recursal, constatada a regularidade dos atos praticados, a autoridade competente homologará o procedimento licitatório.

13 DO TERMO DE CONTRATO

- 13.1 Após a homologação da licitação, o adjudicatário terá o prazo de 05 (cinco) dias úteis, contados a partir da data de sua convocação, para assinar o Termo de Contrato, cuja vigência será de 12 (doze) meses, conforme disciplinado no contrato.
- 13.2 Previamente à contratação, a Administração realizará consulta “on-line” ao SICAF, bem como ao Cadastro Informativo de Créditos não quitados – CADIN, (<http://www.pgfn.fazenda.gov.br/divida-ativa-da-uniao/fluxo-da-divida/cadin/>), cujos resultados serão anexados aos autos do processo.

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 13.2.1 Na hipótese de irregularidade do registro no SICAF, a CONTRATADA deverá regularizar a sua situação perante o cadastro no prazo de até 05 (cinco) dias, sob pena de aplicação das penalidades previstas no Edital e anexos.
- 13.3 Alternativamente à convocação para comparecer perante o Conselho para a assinatura do Termo de Contrato, a Administração poderá encaminhá-lo para assinatura, mediante correspondência postal com aviso de recebimento (AR) ou meio eletrônico, para que seja assinado no prazo de 05 (cinco) dias úteis, a contar da data de seu recebimento.
- 13.4 O prazo previsto para assinatura ou aceite poderá ser prorrogado, por igual período, por solicitação justificada do adjudicatário e aceita pela Administração.

14 DA ACEITAÇÃO DO OBJETO E DA FISCALIZAÇÃO

- 14.1 Os critérios de aceitação do objeto e de fiscalização estão previstos no Termo de Referência.

15 DAS OBRIGAÇÕES DA CONTRATANTE E DA CONTRATADA

- 15.1 As obrigações da CONTRATANTE e da CONTRATADA são as estabelecidas no Termo de Referência.

16 DO PAGAMENTO

- 16.1 O CREA-SP pagará à CONTRATADA, vencedora do Lote “1” único, após 15 (quinze) dias úteis, contados a partir da apresentação das Notas Fiscais ou Faturas, as quais deverão ser entregues na Unidade de Suporte ao Usuários - USU do CREA-SP, sito à Avenida Brigadeiro Faria Lima, 1059 - Térreo – Pinheiros- São Paulo- SP. A emissão das Notas Fiscais ou Faturas se darão mediante prévia autorização para faturamento emitida pelo Gestor da Unidade de Suporte ao Usuário, após verificação das condições expressas no Edital, acompanhada dos seguintes documentos:
- 16.1.1 Prova de regularidade relativo ao Fundo de Garantia do Tempo de Serviços (FGTS);

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 16.1.2 Prova de regularidade para com a Fazenda Federal, que abrange também a prova de regularidade relativa à Seguridade Social (conforme Portarias n^{os} 358, de 5 de setembro de 2014 e 1751, de 2 de outubro de 2014);
- 16.1.3 Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de **CNDT** (Certidão Negativa de Débitos Trabalhistas), nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei n^o 5.452, de 1^o de maio de 1943;
- 16.2 A emissão da Nota Fiscal/Fatura será precedida do recebimento provisório e definitivo do serviço;
- 16.2 O termo de recebimento provisório será assinado pela Contratante e Contratada, assim que todas as licenças estiverem instaladas e configuradas, como também o treinamento realizado.
- 16.3 Após 10 (dez) dias, realizados os testes de conformidade e também verificações operacionais, será emitido o termo de recebimento definitivo.
- 16.3 Realizar a análise de toda documentação apresentada, verificação da entrega dos serviços de acordo com as cláusulas contratuais, e, se, caso haja irregularidades que impeçam a liquidação e o pagamento da despesa, indicar as cláusulas contratuais pertinentes, solicitando à CONTRATADA, por escrito, as respectivas correções.
- 16.4 Emitir Termo Circunstanciado para efeito de recebimento definitivo dos serviços prestados, com base nos relatórios e documentações apresentadas; e
- 16.5 Comunicar a empresa para que emita a Nota Fiscal ou Fatura, com o valor exato dimensionado pela fiscalização.
- 16.6 Os pagamentos decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 24 da Lei 8.666, de 1993, deverão ser efetuados no prazo de até 5 (cinco) dias úteis, contados da data da apresentação da Nota Fiscal/Fatura, nos termos do art. 5^o, § 3^o, da Lei n^o 8.666, de 1993.

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 16.7 O pagamento somente será autorizado depois de efetuado o “atesto” pelo servidor competente, devidamente acompanhada das comprovações mencionadas no item “2” do Anexo XI da IN SEGES/MPDG n. 5/2017.
- 16.7.1 Quando do recebimento e aceitação do objeto, o Gestor do contrato analisará também os relatórios e documentação referentes ao treinamento.
- 16.8 Caso se constate o descumprimento de obrigações trabalhistas ou da manutenção das condições exigidas para habilitação poderá ser concedido um prazo para que a CONTRATADA regularize suas obrigações, quando não se identificar má-fé ou a incapacidade de corrigir a situação.
- 16.8.1 Não sendo regularizada a situação da Contratada no prazo concedido, ou nos casos em que identificada má-fé, se não for possível a realização desses pagamentos pela própria Administração, os valores retidos cautelarmente serão depositados junto à Justiça do Trabalho, com o objetivo de serem utilizados exclusivamente no pagamento de salários e das demais verbas trabalhistas, bem como das contribuições sociais e FGTS decorrentes.
- 16.9 Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.
- 16.10 Antes de cada pagamento à CONTRATADA, será realizada consulta dos documentos de regularidade fiscal para verificar a manutenção das condições de habilitação exigidas no Edital.
- 16.11 Constatando-se, a situação de irregularidade da CONTRATADA, será providenciada sua advertência, por escrito, para que, no prazo de 5 (cinco) dias, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da CONTRATANTE.
- 16.12 Não havendo regularização ou sendo a defesa considerada improcedente, a CONTRATANTE deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência da CONTRATADA, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.



SERVIÇO PÚBLICO FEDERAL

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

- 16.13 Persistindo a irregularidade, a CONTRATANTE deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada à CONTRATADA a ampla defesa.
- 16.14 Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso a CONTRATADA não regularize sua situação.
- 16.15 Somente por motivo de economicidade, segurança nacional ou outro interesse público de alta relevância, devidamente justificado, em qualquer caso, pela máxima autoridade da CONTRATANTE, não será rescindido o contrato em execução com a CONTRATADA inadimplente.
- 16.16 Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável, nos termos do item 6 do Anexo XI da IN SEGES/MPDG n. 5/2017, quando couber:
- 16.16.1 A CONTRATADA regularmente optante pelo Simples Nacional, exclusivamente para as atividades de prestação de serviços previstas no §5º-C, do art. 18, da LC 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime, observando-se as exceções nele previstas. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

17 DAS SANÇÕES ADMINISTRATIVAS

- 17.1 Comete infração administrativa, nos termos da Lei nº 10.520, de 2002, o LICITANTE/adjudicatário que:
- 17.1.1 não assinar o termo de contrato ou aceitar/retirar o instrumento equivalente, quando convocado dentro do prazo de validade da proposta;
- 17.1.2 apresentar documentação falsa;
- 17.1.3 deixar de entregar os documentos exigidos no certame;

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 17.1.4 ensejar o retardamento da execução do objeto;
- 17.1.5 não mantiver a proposta;
- 17.1.6 cometer fraude fiscal;
- 17.1.7 comportar-se de modo inidôneo;
- 17.2 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.
- 17.3 O LICITANTE/ADJUDICATÁRIO que cometer qualquer das infrações discriminadas nos subitens anteriores ficará sujeito, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:
- 17.3.1 pagar multa moratória no montante de 1% (um por cento), **por dia de atraso injustificado** sobre o valor da parcela inadimplida até o limite de 10% (dez por cento);
- 17.3.2 pagar multa compensatória no montante de 20% (vinte por cento) do valor global do contrato, em se tratando de inadimplemento absoluto.
- 17.3.3 impedimento de licitar e de contratar com a União, durante o prazo da sanção, e será descredenciado no Cadastro de Fornecedores do CREA-SP, pelo prazo de até 05 (cinco) anos.
- 17.4 A penalidade de multa pode ser aplicada cumulativamente com a sanção de impedimento.
- 17.5 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.

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 17.6 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.
- 17.7 As sanções por atos praticados no decorrer da contratação estão previstas no Termo de Referência.

18 A IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

- 18.1 Até 02 (dois) dias úteis antes da data designada para a abertura da sessão pública, qualquer pessoa poderá impugnar este Edital.
- 18.2 A impugnação poderá ser realizada por forma eletrônica, pelo *e-mail* compras.licitacao@creasp.org.br, ou por petição dirigida ou protocolada na Unidade de Contratos e Licitação - UCL, na Avenida Brigadeiro Faria Lima, 1059 – 7º andar – Pinheiros – São Paulo, SP, CEP 01452-920.
- 18.3 Caberá ao Pregoeiro decidir sobre a impugnação no prazo de até 24 (vinte e quatro) horas.
- 18.4 Acolhida a impugnação, será definida e publicada nova data para a realização do certame.
- 18.5 Os pedidos de esclarecimentos referentes a este processo licitatório deverão ser enviados ao Pregoeiro, até 03 (três) dias úteis anteriores à data designada para abertura da sessão pública, exclusivamente por meio eletrônico via internet, no endereço indicado no Edital.
- 18.6 As impugnações e pedidos de esclarecimentos não suspendem os prazos previstos no certame.
- 18.7 As respostas às impugnações e os esclarecimentos prestados pelo Pregoeiro serão entranhados nos autos do processo licitatório e estarão disponíveis para consulta por qualquer interessado, e serão disponibilizadas nos sistemas eletrônicos www.licitacoes-e.com.br e www.creasp.org.br.

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP****19 DAS DISPOSIÇÕES GERAIS**

- 19.1 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.
- 19.2 A homologação do resultado desta licitação não implicará direito à contratação.
- 19.3 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.
- 19.4 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.
- 19.5 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.
- 19.6 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.
- 19.7 O LICITANTE detentor do lance vencedor será convocado pelo Pregoeiro, via sistema, a reapresentar de imediato, a proposta comercial, por meio eletrônico com os respectivos valores readequados ao lance vencedor.
- 19.8 Em caso de divergência entre disposições deste Edital e de seus anexos ou demais peças que compõem o processo, prevalecerá as deste Edital.

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 19.9 O Edital está disponibilizado, na íntegra, nos seguintes endereços eletrônicos: www.licitacoes-e.com.br e compras.licitacao@creasp.org.br, e também poderá ser lido e/ou obtido na sede do CREA-SP, localizada na Avenida Brigadeiro Faria Lima, 1059 – 7º andar, Pinheiros, São Paulo, SP, CEP – 01452-920, nos dias úteis, no horário das 8h30min às 16h30min, mesmo endereço e período no qual os autos do processo administrativo permanecerão com vista franqueada aos interessados.
- 19.9 O LICITANTE detentor do lance vencedor será convocado pelo Pregoeiro, via sistema, a reapresentar de imediato, a proposta comercial, por meio eletrônico com os respectivos valores readequados ao lance vencedor.
- 19.10 É expressamente proibida, por parte da CONTRATADA, durante a execução do objeto desta licitação, a contratação de servidor pertencente ao quadro de pessoal do CREA-SP.
- 19.11 O Pregoeiro se reserva o direito de promover diligência, a seu critério, para verificar e esclarecer a comprovação das informações constantes das propostas e documentos enviados.
- 19.12 Será desclassificada a proposta que não atender às exigências, bem como inabilitada a empresa que não apresentar os documentos estabelecidos, neste Edital.
- 19.13 O pregoeiro, no interesse do Conselho, poderá relevar omissões ou erros puramente formais observados na proposta comercial e documentação, desde que não contrariem a legislação vigente e não comprometa a lisura da licitação, sendo possível a promoção de diligência destinada a esclarecer ou a complementar a instrução do processo, vedada a inclusão de novo documento que deveria constar originalmente da proposta ou habilitação.

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 19.14 A critério do CREA-SP, esta licitação poderá ser:
- a) anulada, por ilegalidade, de ofício ou por provocação de terceiros, mediante parecer escrito e devidamente fundamentado;
 - b) revogada, por razões de interesse público decorrente de fato superveniente devidamente comprovado.
- 19.15 O Edital está disponibilizado, na íntegra, nos endereços eletrônicos www.licitacoes-e.com.br Licitação nº 713295 e www.creasp.org.br, e também poderão ser lidos e/ou obtidos no endereço Av. Brigadeiro Faria Lima, 1054 – 7º andar – Pinheiros - SP, nos dias úteis, no horário das 08h30min às 16h30min, mesmo endereço e período no qual os autos do processo administrativo permanecerão com vista franqueada aos interessados.
- 19.16 Recomenda-se que o LICITANTE consulte o manual do Sistema “Licitações-e” (**Orientações para o Fornecedor**), disponível no endereço: <http://www.licitacoes-e.com.br/aop/documentos/CartilhaFornecedor.pdf>.
- 19.17 As regras estabelecidas neste Edital prevalecem sobre os procedimentos previstos no precitado manual do Sistema quando houver divergências.
- 19.18 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.
- 19.19 Fica eleito o Foro da Justiça Federal de São Paulo, para dirimir qualquer lide oriunda do cumprimento do estabelecido neste Edital e seus anexos.
- 19.20 Integram este Edital, para todos os fins e efeitos, os seguintes anexos:
- 19.20.1 ANEXO I - Termo de Referência;
 - 19.20.2 ANEXO II – Formação de Preços Estimativos;



SERVIÇO PÚBLICO FEDERAL

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

- 19.20.3 ANEXO III - Modelo de declaração conforme Decreto nº 4.358, de 05 de setembro de 2002, de que não existe na empresa, trabalhador nas situações previstas no inciso XXXIII do Art. 7º da Constituição Federal;
- 19.20.4 ANEXO IV - Ficha Cadastral de Fornecedores;
- 19.20.5 ANEXO V Modelo de Declaração para Microempresa e Empresa de Pequeno Porte;
- 19.20.6 ANEXO VI – Minuta de Termo de Contrato;

São Paulo, 26 de março de 2018.

Mauricio Bachert Torres
Superintendente Administrativo
Portaria nº 29/2017

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP****ANEXO I****TERMO DE REFERÊNCIA**

A	OBJETIVO
	Contratação de empresa para fornecimento de software antivírus para o CREA-SP, incluindo instalação configuração e treinamento do software conforme condições, quantidades e exigências constantes deste Termo de Referência.
B	JUSTIFICATIVA
	Impedir a ocorrência de infecções por pragas virtuais nos microcomputadores, notebooks e equipamentos servidores de rede do CREA-SP e permitir a identificação/remoção nativa do tipo de vírus RANSOMWARE, tornando o ambiente computacional mais confiável e seguro.
C	DO CONTRATO
	Será firmado contrato com a vencedora do Lote “1” com vigência adstrita ao efetivo cumprimento das obrigações de ambas as partes, a validade das licenças será perpétua, mas as atualizações da solução de antivírus terão validade de 36 (trinta e seis) meses.
D	VALOR ESTIMADO
	A despesa com a execução dos serviços de que trata o objeto desta licitação é estimada em R\$ 206.150,67 (duzentos e seis mil, cento e cinquenta reais e sessenta e sete centavos).
E	DOTAÇÃO ORÇAMENTÁRIA
	A Dotação Orçamentária para as despesas oriundas da contratação advirá das contas nºs 6.2.2.1.1.02.02.05.001 – Direito de Uso Software e 6.2.2.1.1.01.04.09.005 – Serviços de Informática.
F	RESPONSÁVEL PELO PROJETO
	Unidade de Suporte ao Usuário - USU do Departamento de Informática - IF do CREA-SP.



SERVIÇO PÚBLICO FEDERAL

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

1 DO OBJETO

- 1.1 Contratação de empresa para fornecimento de software antivírus para o CREA-SP, incluindo instalação, configuração e treinamento do software conforme condições, quantidades e exigências estabelecidas.

2 DA CARACTERÍSTICA DO PRODUTO

A solução ofertada deverá fornecer proteção para os nossos servidores de dados, rede, e-mail e internet, protegendo também os microcomputadores conectados ou não ao nosso Active Directory.

- 2 A proteção deve ser de âmbito corporativo, possibilitando o gerenciamento centralizado:

2.1 Servidor de Administração e Console Administrativa

2.1.1 Compatibilidade:

- 2.1.1.1 Microsoft Windows Server 2003 ou superior (Todas edições)
- 2.1.1.2 Microsoft Windows Server 2003 x64 ou superior (Todas edições)
- 2.1.1.3 Microsoft Windows Server 2008 (Todas edições)
- 2.1.1.4 Microsoft Windows Server 2008 Core (Todas edições)
- 2.1.1.5 Microsoft Windows Server 2008 x64 SP1 (Todas edições)
- 2.1.1.6 Microsoft Windows Server 2008 R2 (Todas edições)
- 2.1.1.7 Microsoft Windows Server 2008 R2 Core (Todas edições)
- 2.1.1.8 Microsoft Windows Server 2012 (Todas edições)
- 2.1.1.9 Microsoft Windows Server 2012 R2 (Todas edições)
- 2.1.1.10 Microsoft Windows Server 2016 (Todas edições)
- 2.1.1.11 Microsoft Windows XP Professional SP2 ou superior
- 2.1.1.12 Microsoft Windows XP Professional x64 e superior
- 2.1.1.13 Microsoft Windows Vista SP1
- 2.1.1.14 Microsoft Windows Vista x64 SP1
- 2.1.1.15 Microsoft Windows 7

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 2.1.1.16 Microsoft Windows 7 x64
- 2.1.1.17 Microsoft Windows 8
- 2.1.1.18 Microsoft Windows 8 x64
- 2.1.1.19 Microsoft Windows 10
- 2.1.1.20 Microsoft Windows 10 x64

2.1.2 Suportar as seguintes plataformas virtuais:

- 2.1.2.1 VMware: Workstation 9.x, Workstation 10.x, ESX 4.x, ESXi 4.x, ESXi 5.5, ESXi 6.0 e ESXi 6.5
- 2.1.2.2 KVM integrado com: RHEL 5.4 e 5.x acima, SLES 11 SPx, Ubuntu 10.10 LTS

2.1.3 Características:

- 2.1.3.1 A console deve ser acessada via WEB (HTTPS) ou MMC;
- 2.1.3.2 Console deve ser baseada no modelo cliente/servidor
- 2.1.3.3 Compatibilidade com Windows Failover Clustering ou outra solução de alta disponibilidade
- 2.1.3.4 Deve permitir a atribuição de perfis para os administradores da Solução de Antivírus.
- 2.1.3.5 Console deve ser totalmente integrada com suas funções e módulos caso haja a necessidade no futuro de adicionar novas tecnologias tais como, criptografia, Patch management e MDM
- 2.1.3.6 As licenças deverão ser perpétuas, ou seja, expirado a validade da mesma o produto deverá permanecer funcional para a proteção contra códigos maliciosos;
- 2.1.3.7 Capacidade de remover remotamente e automaticamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores, sem a necessidade da senha de remoção do atual antivírus;
- 2.1.3.8 Capacidade de instalar remotamente a solução de antivírus nas estações e servidores Windows, através de compartilhamento administrativo, login script e/ou GPO de Active Directory;

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 2.1.3.9 Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria
- 2.1.3.10 A solução de gerencia deve permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas
- 2.1.3.11 Através da solução de gerência, deve ser possível verificar qual licença está aplicada para determinado computador
- 2.1.3.12 Capacidade de instalar remotamente a solução de segurança em smartphones e tablets de sistema iOS, Andoid e Windows
- 2.1.3.13 Capacidade de instalar remotamente qualquer “app” em smartphones e tablets de sistema iOS;
- 2.1.3.14 A solução de gerência centralizada deve permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle
- 2.1.3.15 Deverá ter a capacidade de criar regras para limitar o tráfego de comunicação cliente/servidor por sub rede com os seguintes parâmetros: KB/s e horário.
- 2.1.3.16 Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux e Mac) protegidos pela solução antivírus;
- 2.1.3.17 Capacidade de gerenciar smartphones e tablets (Windows Phone , Android e iOS) protegidos pela solução antivírus;
- 2.1.3.18 Capacidade de gerar pacotes customizados (auto executáveis) contendo a licença e configurações do produto;
- 2.1.3.19 Capacidade de atualizar os pacotes de instalação com as últimas vacinas;
- 2.1.3.20 Capacidade de fazer distribuição remota de qualquer software, ou seja, deve ser capaz de remotamente enviar qualquer software pela estrutura de gerenciamento de antivírus para que seja instalado nas máquinas clientes;

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 2.1.3.21 A comunicação entre o cliente e o servidor de administração deve ser criptografada.
- 2.1.3.22 Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes;
- 2.1.3.23 Deve permitir a realocação de máquinas novas na rede para um determinado grupo sem ter um agente ou endpoint instalado através dos seguintes parâmetros:
 - 2.1.3.23.1 Nome do computador
 - 2.1.3.23.2 Nome do domínio
 - 2.1.3.23.3 Range de IP
 - 2.1.3.23.4 Sistema Operacional
 - 2.1.3.23.5 Máquina virtual
- 2.1.3.24 Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas;
- 2.1.3.25 Deve permitir, por meio da console de gerenciamento, extrair um artefato em quarentena de um cliente sem a necessidade de um servidor ou console de quarentena adicional
- 2.1.3.26 Capacidade de monitorar diferentes subnets de rede a fim de encontrar máquinas novas para serem adicionadas a proteção;
- 2.1.3.27 Capacidade de monitorar grupos de trabalhos já existentes e quaisquer grupos de trabalho que forem criados na rede, a fim de encontrar máquinas novas para serem adicionadas a proteção;
- 2.1.3.28 Capacidade de, assim que detectar máquinas novas no Active Directory, subnets ou grupos de trabalho, automaticamente importar a máquina para a estrutura de proteção da console e verificar se possui o antivírus instalado. Caso não possuir, deve instalar o antivírus automaticamente;
- 2.1.3.29 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;

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 2.1.3.30 Capacidade de definir políticas de configurações diferentes por grupos de estações, permitindo que sejam criados subgrupos e com função de herança de políticas entre grupos e subgrupos;
- 2.1.3.31 Deve fornecer as seguintes informações dos computadores:
 - 2.1.3.31.1 Se o antivírus está instalado;
 - 2.1.3.31.2 Se o antivírus está iniciado;
 - 2.1.3.31.3 Se o antivírus está atualizado;
 - 2.1.3.31.4 Minutos/horas desde a última conexão da máquina com o servidor administrativo;
 - 2.1.3.31.5 Minutos/horas desde a última atualização de vacinas
 - 2.1.3.31.6 Data e horário da última verificação executada na máquina;
 - 2.1.3.31.7 Versão do antivírus instalado na máquina;
 - 2.1.3.31.8 Se é necessário reiniciar o computador para aplicar mudanças;
 - 2.1.3.31.9 Data e horário de quando a máquina foi ligada;
 - 2.1.3.31.10 Quantidade de vírus encontrados (contador) na máquina;
 - 2.1.3.31.11 Nome do computador;
 - 2.1.3.31.12 Domínio ou grupo de trabalho do computador;
 - 2.1.3.31.13 Data e horário da última atualização de vacinas;
 - 2.1.3.31.14 Sistema operacional com Service Pack;
 - 2.1.3.31.15 Quantidade de processadores;
 - 2.1.3.31.16 Quantidade de memória RAM;
 - 2.1.3.31.17 Usuário(s) logado(s) naquele momento, com informações de contato (caso disponíveis no Active Directory);
 - 2.1.3.31.18 Endereço IP;

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 2.1.3.31.19 Aplicativos instalados, inclusive aplicativos de terceiros, com histórico de instalação, contendo data e hora que o software foi instalado ou removido.
- 2.1.3.31.20 Atualizações do Windows Updates instaladas
- 2.1.3.31.21 Informação completa de hardware contendo: processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de áudio, adaptadores de rede, monitores, drives de CD/DVD
- 2.1.3.31.22 Vulnerabilidades de aplicativos instalados na máquina
- 2.1.3.32 Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterá-las;
- 2.1.3.33 Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como:
 - 2.1.3.33.1 Mudança de gateway;
 - 2.1.3.33.2 Mudança de subnet DNS;
 - 2.1.3.33.3 Mudança de domínio;
 - 2.1.3.33.4 Mudança de servidor DHCP;
 - 2.1.3.33.5 Mudança de servidor DNS;
 - 2.1.3.33.6 Mudança de servidor WINS;
 - 2.1.3.33.7 Aparecimento de nova subnet;
- 2.1.3.34 Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet;
- 2.1.3.35 Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes;

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 2.1.3.36 Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus;
- 2.1.3.37 Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos;
- 2.1.3.38 Capacidade de eleger qualquer computador cliente como repositório de vacinas e de pacotes de instalação, sem que seja necessária a instalação de um servidor administrativo completo, onde outras máquinas clientes irão atualizar-se e receber pacotes de instalação, a fim de otimizar tráfego da rede;
- 2.1.3.39 Capacidade de fazer deste repositório de vacinas um gateway para conexão com o servidor de administração, para que outras máquinas que não consigam conectar-se diretamente ao servidor possam usar este gateway para receber e enviar informações ao servidor administrativo.
- 2.1.3.40 Capacidade de exportar relatórios para os seguintes tipos de arquivos: PDF, HTML e XML.
- 2.1.3.41 Capacidade de gerar traps SNMP para monitoramento de eventos;
- 2.1.3.42 Capacidade de enviar e-mails para contas específicas em caso de algum evento;
- 2.1.3.43 Deve possuir compatibilidade com Microsoft NAP, quando instalado em um Windows 2008 Server;
- 2.1.3.44 Deve possuir compatibilidade com Cisco Network Admission Control (NAC);
- 2.1.3.45 Deve possuir documentação da estrutura do banco de dados para geração de relatórios a partir de ferramentas específicas de consulta (Crystal Reports, por exemplo).
- 2.1.3.46 Capacidade de ligar máquinas via Wake on Lan para realização de tarefas (varredura, atualização, instalação, etc), inclusive de máquinas que estejam em subnets diferentes do servidor;

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 2.1.3.47 Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado intervalo de tempo);
- 2.1.3.48 Capacidade de realizar atualização incremental de vacinas nos computadores clientes;
- 2.1.3.49 Deve armazenar localmente e enviar ao servidor de gerência a ocorrência de vírus com os seguintes dados, no mínimo:
 - 2.1.3.49.1 Nome do vírus
 - 2.1.3.49.2 Nome do arquivo infectado
 - 2.1.3.49.3 Data e hora da detecção
 - 2.1.3.49.4 Nome da máquina ou endereço IP
 - 2.1.3.49.5 Ação realizada
- 2.1.3.50 Capacidade de reportar vulnerabilidades de softwares presentes nos computadores.
- 2.1.3.51 Capacidade de realizar inventário de aplicativos de todas as máquinas clientes;
- 2.1.3.52 Capacidade de diferenciar máquinas virtuais de máquinas físicas;

2.2 Em relação as estações Windows**2.2.1 Compatibilidade:**

- 2.2.1.1 Microsoft Windows XP Professional SP3 e superior
- 2.2.1.2 Microsoft Windows Vista Business/Enterprise/Ultimate SP2
- 2.2.1.3 Microsoft Windows Vista Business/Enterprise/Ultimate x64 SP2
- 2.2.1.4 Microsoft Windows 7 Professional/Enterprise/Ultimate
- 2.2.1.5 Microsoft Windows 7 Professional/Enterprise/Ultimate x64
- 2.2.1.6 Microsoft Windows 7 Professional/Enterprise/Ultimate SP1 e superior
- 2.2.1.7 Microsoft Windows 7 Professional/Enterprise/Ultimate x64 SP1 e superior
- 2.2.1.8 Microsoft Windows 8 Professional/Enterprise

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 2.2.1.9 Microsoft Windows 8 Professional/Enterprise x64
- 2.2.1.10 Microsoft Windows 8.1 Enterprise x86 / 64
- 2.2.1.11 Microsoft Windows 8.1 Pro x86 /64
- 2.2.1.12 Microsoft Windows 10 Enterprise x86 / 64
- 2.2.1.13 Microsoft Windows 10 Pro x86 / 64

2.2.2 Características:

- 2.2.2.1 Deve prover as seguintes proteções:
 - 2.2.2.1.1 Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
 - 2.2.2.1.2 Antivírus de Web (módulo para verificação de sites e downloads contra vírus)
 - 2.2.2.1.3 Antivírus de E-mail (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos)
 - 2.2.2.1.4 Antivírus de Mensagens Instantâneas (módulo para verificação de mensagens instantâneas, como ICQ, MSN, IRC, etc)
 - 2.2.2.1.5 O Endpoint deve possuir opção para rastreamento por linha de comando, parametrizável, com opção de limpeza
 - 2.2.2.1.6 Firewall com IDS
 - 2.2.2.1.7 Autoproteção (contra-ataques aos serviços/processos do antivírus)
 - 2.2.2.1.8 Controle de dispositivos externos
 - 2.2.2.1.9 Controle de acesso a sites por categoria
 - 2.2.2.1.10 Controle de acesso a sites por horário
 - 2.2.2.1.11 Controle de acesso a sites por usuários
 - 2.2.2.1.12 Controle de execução de aplicativos

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 2.2.2.1.13 Controle de vulnerabilidades do Windows e dos aplicativos instalados
- 2.2.2.1.14 Capacidade de escolher quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
- 2.2.2.1.15 As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa).
- 2.2.2.1.16 Capacidade de automaticamente desabilitar o Firewall do Windows (caso exista) durante a instalação, para evitar incompatibilidade com o Firewall da solução;
- 2.2.2.1.17 Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;
- 2.2.2.1.18 Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: “Win32.Trojan.banker”) para que qualquer objeto detectado com o veredicto escolhido seja ignorado;
- 2.2.2.1.19 Capacidade de adicionar aplicativos a uma lista de “aplicativos confiáveis”, onde as atividades de rede, atividades de disco e acesso ao registro do Windows não serão monitoradas;
- 2.2.2.1.20 Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 2.2.2.1.21 Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
- 2.2.2.1.22 Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomá-la a partir da extensão do arquivo;
- 2.2.2.1.23 Capacidade de verificar somente arquivos novos e alterados;
- 2.2.2.1.24 Capacidade de verificar objetos usando heurística;
- 2.2.2.1.25 Capacidade de agendar uma pausa na verificação;
- 2.2.2.1.26 Deve permitir a filtragem de conteúdo de URL avançada efetuando a classificação dos sites em categorias
- 2.2.2.1.27 Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;
- 2.2.2.1.28 O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
 - 2.2.2.1.28.1 Perguntar o que fazer, ou;
 - 2.2.2.1.28.2 Bloquear acesso ao objeto;
 - 2.2.2.1.28.3 Apagar o objeto ou tentar desinfecção (de acordo com a configuração pré-estabelecida pelo administrador);
 - 2.2.2.1.28.4 Caso positivo de desinfecção:
 - 2.2.2.1.28.4.1 Restaurar o objeto para uso;
 - 2.2.2.1.28.4.2 Caso negativo de desinfecção:
 - 2.2.2.1.28.4.2.1 Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 2.2.2.1.29 Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto.
- 2.2.2.1.30 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);
- 2.2.2.1.31 Capacidade de verificar tráfego de ICQ, MSN, AIM e IRC contra vírus e links phishings;
- 2.2.2.1.32 Capacidade de verificar links inseridos em e-mails contra phishings;
- 2.2.2.1.33 Capacidade de verificar tráfego SSL nos browsers: Internet Explorer, Firefox e Chrome;
- 2.2.2.1.34 Capacidade de verificação de corpo e anexos de e-mails usando heurística;
- 2.2.2.1.35 O antivírus de e-mail, ao encontrar um objeto potencialmente perigoso, deve:
 - 2.2.2.1.35.1 Perguntar o que fazer, ou;
 - 2.2.2.1.35.2 Bloquear o e-mail;
 - 2.2.2.1.35.3 Apagar o objeto ou tentar desinfecção (de acordo com a configuração pré-estabelecida pelo administrador);
 - 2.2.2.1.35.4 Caso positivo de desinfecção:
 - 2.2.2.1.35.4.1 Restaurar o e-mail para o usuário;
 - 2.2.2.1.35.5 Caso negativo de desinfecção:
 - 2.2.2.1.35.5.1 Mover para quarentena ou apagar o objeto (de acordo com a configuração pré-estabelecida pelo administrador);

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 2.2.2.1.36 Caso o e-mail conter código que parece ser, mas não é definitivamente malicioso, o mesmo deve ser mantido em quarentena.
- 2.2.2.1.37 Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados.
- 2.2.2.1.38 Capacidade de filtrar anexos de e-mail, apagando-os ou renomeando-os de acordo com a configuração feita pelo administrador.
- 2.2.2.1.39 Capacidade de verificação de tráfego HTTP e qualquer script do Windows Script Host (JavaScript, Visual Basic Script, etc), usando heurísticas;
- 2.2.2.1.40 Deve ter suporte total ao protocolo IPv6;
- 2.2.2.1.41 Capacidade de alterar as portas monitoradas pelos módulos de Web e E-mail;
- 2.2.2.1.42 Na verificação de tráfego web, caso encontrado código malicioso o programa deve:
 - 2.2.2.1.42.1 Perguntar o que fazer, ou;
 - 2.2.2.1.42.2 Bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio, ou;
 - 2.2.2.1.42.3 Permitir acesso ao objeto;
- 2.2.2.1.43 O antivírus de web deve realizar a verificação de, no mínimo, duas maneiras diferentes, sob escolha do administrador:
 - 2.2.2.1.43.1 Verificação on-the-fly, onde os dados são verificados enquanto são recebidos em tempo real, ou;
 - 2.2.2.1.43.2 Verificação de buffer, onde os dados são recebidos e armazenados para posterior verificação.

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 2.2.2.1.44 Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus de web.
- 2.2.2.1.45 Deve possuir módulo que analise as ações de cada aplicação em execução no computador, gravando as ações executadas e comparando-as com sequências características de atividades perigosas. Tais registros de sequências devem ser atualizados juntamente com as vacinas.
- 2.2.2.1.46 Deve possuir módulo que analise cada macro de VBA executada, procurando por sinais de atividade maliciosa.
- 2.2.2.1.47 Deve possuir módulo que analise qualquer tentativa de edição, exclusão ou gravação do registro, de forma que seja possível escolher chaves específicas para serem monitoradas e/ou bloqueadas.
- 2.2.2.1.48 Deve possuir módulo de bloqueio de Phishing, com atualizações incluídas nas vacinas, obtidas pelo Anti-Phishing Working Group (<http://www.antiphishing.org/>).
- 2.2.2.1.49 Capacidade de distinguir diferentes sub-nets e conceder opção de ativar ou não o firewall para uma sub-net específica;
- 2.2.2.1.50 Deve possuir módulo IDS (Intrusion Detection System) para proteção contra port scans e exploração de vulnerabilidades de softwares. A base de dados de análise deve ser atualizada juntamente com as vacinas.
- 2.2.2.1.51 O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 2.2.2.1.51.1 Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;
- 2.2.2.1.51.2 Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.
- 2.2.2.1.52 Deve possuir módulo que habilite ou não o funcionamento dos seguintes dispositivos externos, no mínimo:
 - 2.2.2.1.52.1 Discos de armazenamento locais
 - 2.2.2.1.52.2 Armazenamento removível
 - 2.2.2.1.52.3 Impressoras
 - 2.2.2.1.52.4 Modems
 - 2.2.2.1.52.5 Dispositivos multifuncionais
 - 2.2.2.1.52.6 Leitores de smart card
 - 2.2.2.1.52.7 Dispositivos de sincronização via ActiveSync (Windows CE, Windows, Mobile, etc)
 - 2.2.2.1.52.8 Wi-Fi
 - 2.2.2.1.52.9 Adaptadores de rede externos
 - 2.2.2.1.52.10 Dispositivos MP3 ou smartphones
 - 2.2.2.1.52.11 Dispositivos Bluetooth

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 2.2.2.1.53 Capacidade de liberar acesso a um dispositivo específico e usuários específico por um período de tempo específico, sem a necessidade de desabilitar a proteção, sem desabilitar o gerenciamento central ou de intervenção local do administrador na máquina do usuário.
- 2.2.2.1.54 Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por usuário.
- 2.2.2.1.55 Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por agendamento.
- 2.2.2.1.56 Capacidade de configurar novos dispositivos por Class ID/Hardware ID
- 2.2.2.1.57 Capacidade de limitar o acesso a sites da internet por categoria, por conteúdo (vídeo, áudio, etc), com possibilidade de configuração por usuário ou grupos de usuários e agendamento.
- 2.2.2.1.58 Capacidade de limitar a execução de aplicativos por hash MD5, nome do arquivo, versão do arquivo, nome do aplicativo, versão do aplicativo, fabricante/desenvolvedor, categoria (ex: navegadores, gerenciador de download, jogos, aplicação de acesso remoto, etc).
- 2.2.2.1.59 Capacidade de bloquear execução de aplicativo que está em armazenamento externo.
- 2.2.2.1.60 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.

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 2.2.2.1.61 Capacidade de, em caso de epidemia, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web.
- 2.2.2.1.62 Capacidade de, caso o computador cliente saia da rede corporativa, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web.
- 2.2.2.1.63 Capacidade nativa de identificar e remover vírus do tipo RANSOMWARE.

2.3 Em relação aos servidores Windows**2.3.1 Compatibilidade:**

- 2.3.1.1 Microsoft Windows Small Business Server 2011 Essentials/Standard x64
- 2.3.1.2 Microsoft Windows Server 2003 Standard/Enterprise SP2 x86/x64
- 2.3.1.3 Microsoft Windows Server 2003 R2 Standard/Enterprise SP2 x86/x64
- 2.3.1.4 Microsoft Windows Server 2008 Standard/Enterprise/Datacenter SP1 x86/x64
- 2.3.1.5 Microsoft Windows Server 2008 Core Standard/Enterprise/Datacenter SP1 x86/x64
- 2.3.1.6 Microsoft Windows Server 2008 R2 Standard/Enterprise/Datacenter SP1
- 2.3.1.7 Microsoft Windows Server 2008 R2 Core Standard/Enterprise/Datacenter SP1
- 2.3.1.8 Microsoft Windows Server 2012 Foundation/Essentials/Standard x64

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 2.3.1.9 Microsoft Windows Server 2016
Foundation/Essentials/Standard x64
- 2.3.1.10 Microsoft Terminal baseado em Windows Server 2003
- 2.3.1.11 Microsoft Terminal baseado em Windows Server 2008
- 2.3.1.12 Microsoft Terminal baseado em Windows Server 2008 R2

2.3.2 Características:

- 2.3.2.1 Deve prover as seguintes proteções:
 - 2.3.2.1.1 Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
 - 2.3.2.1.2 Autoproteção contra ataques aos serviços / processos
 - 2.3.2.1.3 Firewall com IDS
 - 2.3.2.1.4 Controle de vulnerabilidades do Windows e dos aplicativos instalados
- 2.3.2.2 Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
- 2.3.2.3 As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora.
- 2.3.2.4 Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
 - 2.3.2.4.1 Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
 - 2.3.2.4.2 Gerenciamento de tarefa (criar ou excluir tarefas de verificação)
 - 2.3.2.4.3 Leitura de configurações
 - 2.3.2.4.4 Modificação de configurações
 - 2.3.2.4.5 Gerenciamento de Backup e Quarentena
 - 2.3.2.4.6 Visualização de relatórios
 - 2.3.2.4.7 Gerenciamento de relatórios

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 2.3.2.4.8 Gerenciamento de chaves de licença
- 2.3.2.4.9 Gerenciamento de permissões (adicionar/excluir permissões acima)
- 2.3.2.5 O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:
 - 2.3.2.5.1 Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;
 - 2.3.2.5.2 Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.
- 2.3.2.6 Capacidade de separadamente selecionar o número de processos que irão executar funções de varredura em tempo real, o número de processos que executarão a varredura sob demanda e o número máximo de processos que podem ser executados no total.
- 2.3.2.7 Capacidade de resumir automaticamente tarefas de verificação que tenham sido paradas por anormalidades (queda de energia, erros, etc)
- 2.3.2.8 Capacidade de automaticamente pausar e não iniciar tarefas agendadas caso o servidor esteja em rodando com fonte ininterrupta de energia (uninterruptible Power supply – UPS)
- 2.3.2.9 Em caso erros, deve ter capacidade de criar logs e traces automaticamente, sem necessidade de outros softwares;
- 2.3.2.10 Capacidade de configurar níveis de verificação diferentes para cada pasta, grupo de pastas ou arquivos do servidor.

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 2.3.2.11 Capacidade de bloquear comunicação a servidores acessados por estações de trabalho infectadas e quando estações tentarem gravar arquivos infectados nos servidores.
- 2.3.2.12 Capacidade de criar uma lista de máquina que nunca serão bloqueadas mesmo quando infectadas.
- 2.3.2.13 Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;
- 2.3.2.14 Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: “Win32.Trojan.banker”) para que qualquer objeto detectado com o veredicto escolhido seja ignorado;
- 2.3.2.15 Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
- 2.3.2.16 Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomá-la a partir da extensão do arquivo;
- 2.3.2.17 Capacidade de verificar somente arquivos novos e alterados;
- 2.3.2.18 Capacidade de escolher qual tipo de objeto composto será verificado (ex: arquivos comprimidos, arquivos auto descompressores, .PST, arquivos compactados por compactadores binários, etc)
- 2.3.2.19 Capacidade de verificar objetos usando heurística;
- 2.3.2.20 Capacidade de configurar diferentes ações para diferentes tipos de ameaças;
- 2.3.2.21 Capacidade de agendar uma pausa na verificação;

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 2.3.2.22 Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;
- 2.3.2.23 O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
 - 2.3.2.23.1 Perguntar o que fazer, ou;
 - 2.3.2.23.2 Bloquear acesso ao objeto;
 - 2.3.2.23.2.1 Apagar o objeto ou tentar desinfecção (de acordo com a configuração pré-estabelecida pelo administrador);
 - 2.3.2.23.2.2 Caso positivo de desinfecção:
 - 2.3.2.23.2.2.1 Restaurar o objeto para uso;
 - 2.3.2.23.2.3 Caso negativo de desinfecção:
 - 2.3.2.23.3 Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);
- 2.3.2.24 Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto.
- 2.3.2.25 Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena
- 2.3.2.26 Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados
- 2.3.2.27 Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa.
- 2.3.2.28 Capacidade nativa de identificar e remover vírus do tipo RANSOMWARE.

2.4 Em relação aos servidores Linux**2.4.1 Compatibilidade:**

- 2.4.1.1 Plataforma 32-bits:
 - 2.4.1.1.1 Red Hat Enterprise Linux 7.x Server;
 - 2.4.1.1.2 Red Hat Enterprise Linux 6.x Server;
 - 2.4.1.1.3 Red Hat Enterprise Linux 5.x Server;

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 2.4.1.1.4 CentOS-7 e CentOS-6;
 - 2.4.1.1.5 SUSE Linux Enterprise Server 12 SP2;
 - 2.4.1.1.6 openSUSE Linux 12.1;
 - 2.4.1.1.7 openSUSE Linux 12.2;
 - 2.4.1.1.8 Debian GNU/Linux 9.1.
- 2.4.1.2 Plataforma 64-bits:
- 2.4.1.2.1 Red Hat Enterprise Linux 7.x Server;
 - 2.4.1.2.2 Red Hat Enterprise Linux 6.x Server;
 - 2.4.1.2.3 Red Hat Enterprise Linux 5.x Server;
 - 2.4.1.2.4 CentOS-6 e CentOS-7;
 - 2.4.1.2.5 SUSE Linux Enterprise Server 12 SP2;
 - 2.4.1.2.6 openSUSE Linux 12.1;
 - 2.4.1.2.7 openSUSE Linux 12.2;
 - 2.4.1.2.8 Debian GNU/Linux 9.1.

2.4.2 Características:

- 2.4.2.1 Deve prover as seguintes proteções:
- 2.4.2.2 Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
- 2.4.2.3 As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora.
- 2.4.2.4 Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
 - 2.4.2.4.1 Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
 - 2.4.2.4.2 Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfetar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 2.4.2.4.3 Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;
- 2.4.2.4.4 Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados.
- 2.4.2.4.5 Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares;
- 2.4.2.4.6 Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
- 2.4.2.4.7 Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomá-la a partir da extensão do arquivo;
- 2.4.2.4.8 Capacidade de verificar objetos usando heurística;
- 2.4.2.4.9 Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena
- 2.4.2.4.10 Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados
- 2.4.2.4.11 Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux)

2.5 Em relação a Smartphones e tablets**2.5.1 Compatibilidade:**

- 2.5.1.1 Apple iOS 7.0 – 10.3
- 2.5.1.2 Windows Phone 8.1
- 2.5.1.3 Android OS 2.3 – 7.0

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP****2.5.2 Características:**

- 2.5.2.1 Deve prover as seguintes proteções:
 - 2.5.2.1.1 Proteção em tempo real do sistema de arquivos do dispositivo – interceptação e verificação de:
 - 2.5.2.1.1.1 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.
 - 2.5.2.1.1.2 Arquivos abertos no smartphone
 - 2.5.2.1.1.3 Programas instalados usando a interface do smartphone
 - 2.5.2.1.2 Verificação dos objetos na memória interna do smartphone e nos cartões de expansão sob demanda do usuário e de acordo com um agendamento;
- 2.5.2.2 Deverá isolar em área de quarentena os arquivos infectados;
- 2.5.2.3 Deverá atualizar as bases de vacinas de modo agendado;
- 2.5.2.4 Deverá bloquear spams de SMS através de Black lists;
- 2.5.2.5 Deverá ter função de bloqueio do aparelho caso o SIM CARD for trocado para outro não autorizado;
- 2.5.2.6 Capacidade de desativar por política: Wi-fi, Câmera, Bluetooth
- 2.5.2.7 Deverá ter função de limpeza de dados pessoais a distância, em caso de roubo, por exemplo.
- 2.5.2.8 Capacidade de requerer uma senha para desbloquear o dispositivo e personalizar a quantidade de caracteres para esta senha
- 2.5.2.9 Deverá ter firewall pessoal;
- 2.5.2.10 Capacidade de tirar fotos quando a senha for inserida incorretamente (Mugshot)

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 2.5.2.11 Possibilidade de instalação remota utilizando o Microsoft System Center Mobile Device Manager 2008 SP1
- 2.5.2.12 Capacidade de enviar comandos remotamente de:
 - 2.5.2.12.1 Localizar
 - 2.5.2.12.2 Bloquear
- 2.5.2.13 Capacidade de detectar Jailbreak em dispositivos iOS
- 2.5.2.14 Capacidade de bloquear o acesso a site por categoria em dispositivos
- 2.5.2.15 Capacidade de bloquear o acesso a sites phishing ou malicioso
- 2.5.2.16 Capacidade de criar containers de aplicativos, separando dados corporativos de dados pessoais
- 2.5.2.17 Capacidade de bloquear o dispositivo quando o cartão “SIM” for substituído
- 2.5.2.18 Capacidade de configurar White e blacklist de aplicativos
- 2.5.2.19 Capacidade de localizar o dispositivo quando necessário
- 2.5.2.20 Permitir atualização das definições quando estiver em “roaming”
- 2.5.2.21 Capacidade de selecionar endereço do servidor para buscar a definição de vírus
- 2.5.2.22 Capacidade de enviar URL de instalação por e-mail
- 2.5.2.23 Capacidade de executar as seguintes ações caso a desinfecção falhe:
 - 2.5.2.23.1 Deletar
 - 2.5.2.23.2 Ignorar
 - 2.5.2.23.3 Quarentena.
 - 2.5.2.23.4 Perguntar ao usuário

2.6 Gerenciamento de dispositivos móveis (MDM):**2.6.1 Compatibilidade:**

- 2.6.1.1 Dispositivos conectados através do Microsoft Exchange ActiveSync

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 2.6.1.2 Apple iOS
- 2.6.1.3 Windows Phone
- 2.6.1.4 Android
- 2.6.2 Dispositivos com suporte ao Apple Push Notification (APNs) servisse
 - 2.6.2.1 Apple iOS 3.0 ou superior
- 2.6.3 Características:
 - 2.6.3.1 Capacidade de aplicar políticas de ActiveSync através do servidor Microsoft Exchange
 - 2.6.3.2 Capacidade de ajustar as configurações de:
 - 2.6.3.2.1 Sincronização de e-mail
 - 2.6.3.2.2 Uso de aplicativos
 - 2.6.3.2.3 Senha do usuário
 - 2.6.3.2.4 Criptografia de dados
 - 2.6.3.2.5 Conexão de mídia removível
 - 2.6.3.3 Capacidade de instalar certificados digitais em dispositivos móveis
 - 2.6.3.4 Capacidade de, remotamente, resetar a senha de dispositivos iOS
 - 2.6.3.5 Capacidade de, remotamente, apagar todos os dados de dispositivos iOS
 - 2.6.3.6 Capacidade de, remotamente, bloquear um dispositivo iOS
- 2.7 Criptografia:
 - 2.7.1 Compatibilidade:
 - 2.7.1.1 Microsoft Windows XP Professional SP3 ou superior
 - 2.7.1.2 Microsoft Windows Vista Business/Enterprise/Ultimate SP2
 - 2.7.1.3 Microsoft Windows Vista Business/Enterprise/Ultimate x64 SP2
 - 2.7.1.4 Microsoft Windows 7 Professional/Enterprise/Ultimate
 - 2.7.1.5 Microsoft Windows 7 Professional/Enterprise/Ultimate x64
 - 2.7.1.6 Microsoft Windows 8 Professional/Enterprise
 - 2.7.1.7 Microsoft Windows 8 Professional/Enterprise x64

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 2.7.1.8 Microsoft Windows 8.1 Professional / Enterprise
- 2.7.1.9 Microsoft Windows 8.1 Professional / Enterprise x64
- 2.7.1.10 Microsoft Windows 10 Pro x86 / x64
- 2.7.1.11 Microsoft Windows 10 Enterprise x86 /x64

2.7.2 Características:

- 2.7.2.1 O acesso ao recurso criptografado (arquivo, pasta ou disco) deve ser garantido mesmo em caso o usuário tenha esquecido a senha, através de procedimentos de recuperação.
- 2.7.2.2 Utilizar, no mínimo, algoritmo AES com chave de 256 bits.
- 2.7.2.3 Capacidade de criptografar completamente o disco rígido da máquina, adicionando um ambiente de pré-boot para autenticação do usuário.
- 2.7.2.4 Capacidade de utilizar Single Sign-On para a autenticação de pré-boot.
- 2.7.2.5 Permitir criar vários usuários de autenticação pré-boot.
- 2.7.2.6 Capacidade de criar um usuário de autenticação pré-boot comum com uma senha igual para todas as máquinas a partir da console de gerenciamento.
- 2.7.2.7 Capacidade de criptografar drives removíveis de acordo com regra criada pelo administrador, com as opções:
 - 2.7.2.7.1 Criptografar somente os arquivos novos que forem copiados para o disco removível, sem modificar os arquivos já existentes.
 - 2.7.2.7.2 Criptografar todos os arquivos individualmente.
 - 2.7.2.7.3 Criptografar o dispositivo inteiro, de maneira que não seja possível listar os arquivos e pastas armazenadas.
 - 2.7.2.7.4 Criptografar o dispositivo em modo portátil, permitindo acessar os arquivos em máquinas de terceiros através de uma senha.

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 2.7.2.8 Capacidade de selecionar pastas e arquivos (por tipo, ou extensão) para serem criptografados automaticamente. Nesta modalidade, os arquivos devem estar acessíveis para todas as máquinas gerenciadas pela mesma console de maneira transparente para os usuários.
- 2.7.2.9 Capacidade de criar regras de exclusões para que certos arquivos ou pastas nunca sejam criptografados.
- 2.7.2.10 Capacidade de selecionar aplicações que podem ou não ter acesso aos arquivos criptografados.
- 2.7.2.11 Verifica compatibilidade de hardware antes de aplicar a criptografia
- 2.7.2.12 Possibilita estabelecer parâmetros para a senha de criptografia
- 2.7.2.13 Bloqueia o reuso de senhas
- 2.7.2.14 Bloqueia a senha após um número de tentativas pré-estabelecidas
- 2.7.2.15 Capacidade de permitir o usuário solicitar permissão a determinado arquivo criptografado para o administrador mediante templates customizados
- 2.7.2.16 Permite criar exclusões para não criptografar determinados “discos rígidos” através de uma busca por nome do computador ou nome do dispositivo
- 2.7.2.17 Permite criptografar as seguintes pastas pré-definidas: “meus documentos”, “Favoritos”, “Desktop”, “Arquivos temporários” e “Arquivos do outlook”
- 2.7.2.18 Permite utilizar variáveis de ambiente para criptografar pastas customizadas.
- 2.7.2.19 Capacidade de criptografar arquivos por grupos de extensão, tais como: Documentos do office, Document, arquivos de áudio, etc
- 2.7.2.20 Permite criar um grupo de extensões de arquivos a serem criptografados

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

2.7.2.21 Capacidade de criar regra de criptografia para arquivos gerados por aplicações

2.7.2.22 Permite criptografia de dispositivos móveis mesmo quando o endpoint não possuir comunicação com a console de gerenciamento.

2.8 Gerenciamento de Sistemas:

2.8.1 Capacidade de criar imagens de sistema operacional remotamente e distribuir essas imagens para computadores gerenciados pela solução e para computadores bare-metal.

2.8.2 Capacidade de detectar softwares de terceiros vulneráveis, criando assim um relatório de softwares vulneráveis.

2.8.3 Capacidade de corrigir as vulnerabilidades de softwares, fazendo o download centralizado da correção ou atualização e aplicando essa correção ou atualização nas máquinas gerenciadas de maneira transparente para os usuários.

2.8.4 Possuir tecnologia de Controle de Admissão de Rede (NAC), com a possibilidade de criar regras de quais tipos de dispositivos podem ter acessos a recursos da rede.

2.8.5 Capacidade de gerenciar licenças de softwares de terceiros.

2.8.6 Capacidade de registrar mudanças de hardware nas máquinas gerenciadas.

2.8.7 Capacidade de gerenciar um inventário de hardware, com a possibilidade de cadastro de dispositivos (ex: router, switch, projetor, acessório, etc), informando data de compra, local onde se encontra, service tag, número de identificação e outros.

2.8.8 Possibilita fazer distribuição de software de forma manual e agendada

2.8.9 Suporta modo de instalação silenciosa

2.8.10 Suporte a pacotes MSI, exe, bat, cmd e outros padrões de arquivos executáveis

2.8.11 Possibilita fazer a distribuição através de agentes de atualização

2.8.12 Utiliza tecnologia multicast para evitar tráfego na rede

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 2.8.13 Possibilita criar um inventário centralizado de imagens
- 2.8.14 Capacidade de atualizar o sistema operacional direto da imagem mantendo os dados do usuário
- 2.8.15 Suporte a WakeOnLan para deploy de imagens
- 2.8.16 Capacidade de atuar como servidor de atualização do Windows podendo fazer deploy de patches
- 2.8.17 Suporta modo de teste, podendo atribuir alguns computadores para receberem as atualizações de forma automática para avaliação de alterações no comportamento
- 2.8.18 Capacidade de gerar relatórios de vulnerabilidades e patches
- 2.8.19 Possibilita criar exclusões para aplicação de patch por tipo de sistema operacional, Estação de trabalho e Servidor ou por grupo de administração
- 2.8.20 Permite iniciar instalação de patch e correções de vulnerabilidades ao reiniciar ou desligar o computador
- 2.8.21 Permite baixar atualizações para o computador sem efetuar a instalação
- 2.8.22 Permite o administrador instalar somente atualizações aprovadas, instalar todas as atualizações (exceto as bloqueadas) ou instalar todas as atualizações incluindo as bloqueadas
- 2.8.23 Capacidade de instalar correções de vulnerabilidades de acordo com a severidade
- 2.8.24 Permite selecionar produtos a serem atualizados pela console de gerenciamento
- 2.8.25 Permite selecionar categorias de atualizações para serem baixadas e instaladas, tais como: atualizações de segurança, ferramentas, drivers, etc

2.9 Serviços de Instalação, configuração e treinamento do software.

- 2.9.1 Declaração de que todos os serviços serão executados por técnicos certificados pelo Fabricante do software.
- 2.9.2 Na contratação deverá apresentar a certificação dos técnicos mediante certificados emitidos pelo fabricante.

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 2.9.3 Documentação do Plano Técnico do Projeto e a Implementação do mesmo, deverá ser apresentado na entrega das licenças.
- 2.9.4 Instalação e configuração total de todas as licenças do software adquirido no ambiente físico/virtual da CONTRATANTE;
- 2.9.5 Validação das soluções implantadas;
- 2.9.6 Criação das rotinas e teste de Backup/Restore;
- 2.9.7 Treinamento pelo fabricante ou por técnicos homologados pelo fabricante para ministrar treinamento para 4 colaboradores, designados pelo Gestor da Unidade de Suporte ao Usuário – DIF/USU;
 - 2.9.7.1 O treinamento será realizado na sua integridade, nas dependências do CREA-SP, Avenida Brigadeiro Faria Lima, 1.059, Pinheiros – São Paulo/SP;
 - 2.9.7.2 O treinamento ocorrerá de forma concomitante à instalação das licenças de software, ou seja, durante o período de operacionalização das licenças;
- 2.9.8 Entrega dos ambientes em produção;
- 2.9.9 Políticas de segurança definidas;
- 2.9.10 Elaboração do documento técnico final do projeto;
- 2.9.11 Aceite por parte da CONTRATANTE.

3 GARANTIA E VALIDADE DAS LICENÇAS

- 3.1 A validade das licenças será perpétua, mas as atualizações da solução de antivírus terão validade de 36 (trinta e seis) meses.

4 OBRIGAÇÕES DA CONTRATANTE

- 4.1 Acompanhar e fiscalizar todas as etapas da prestação dos serviços, através de seu corpo técnico;
- 4.2 Disponibilizar espaço físico e infraestrutura técnica para que os serviços sejam realizados;
- 4.3 Realizar os pagamentos devidos à CONTRATADA no prazo contratual.

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP****5 OBRIGAÇÕES DA CONTRATADA****5.1 A CONTRATADA deverá:**

- 5.1.1 Contratar, treinar e manter empregados em quantidade e qualificação compatíveis para a execução dos serviços objeto da contratação, sendo considerada neste particular, como única empregadora.
- 5.1.2 Fazer cumprir as normas disciplinares e de segurança. Cumprir as exigências das leis trabalhistas, previdenciárias e sindicais relativamente aos empregados, envolvidos na execução dos serviços, inclusive as determinações emanadas da fiscalização da Prefeitura, fazendo prova dos recolhimentos devidos.
- 5.1.3 Responder por quaisquer acidentes, danos ou prejuízos materiais e/ou pessoais causados ao CREA-SP, seus funcionários e/ou terceiros, por dolo e/ou culpa de seus empregados.
- 5.1.4 Desenvolver boas relações com os funcionários do CREA-SP, acatando quaisquer instruções e o que mais emanar da fiscalização.
- 5.1.5 Informar o Departamento de Informática do CREA-SP quaisquer irregularidades identificadas durante os procedimentos técnicos que possam vir impactar na execução total dos serviços.
- 5.1.6 Comunicar ao CREA-SP, imediatamente, qualquer ocorrência ou anormalidade que venha interferir na execução dos serviços.
- 5.1.7 Arcar com os ônus decorrentes da incidência de todos os tributos federais, estaduais e municipais que possam advir dos serviços contratados, responsabilizando-se pelo cumprimento de todas as exigências das repartições competentes, com total isenção da Prefeitura.

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP****6 DA GESTÃO E FISCALIZAÇÃO DO CONTRATO**

- 6.1 A Gestão do Contrato e a Fiscalização do cumprimento do objeto contratado será de competência da Unidade de Suporte ao Usuário - USU, a quem a **CONTRATADA** deverá reportar-se quanto aos assuntos oriundos da execução do mesmo.
- 6.2 Em hipótese alguma, será admitido que a própria **CONTRATADA** materialize a avaliação de desempenho e qualidade da prestação dos serviços realizada.
- 6.3 Na hipótese de comportamento contínuo de desconformidade da prestação do serviço em relação à qualidade exigida, bem como quando esta ultrapassar os níveis mínimos toleráveis previstos nos indicadores, além dos fatores redutores, devem ser aplicadas as sanções à **CONTRATADA** de acordo com as regras previstas no ato convocatório.
- 6.4 O representante da **CONTRATANTE** deverá promover o registro das ocorrências verificadas, adotando as providências necessárias ao fiel cumprimento das cláusulas contratuais, conforme o disposto nos §§ 1º e 2º do art. 67 da Lei nº 8.666, de 1993.
- 6.5 O descumprimento total ou parcial das obrigações e responsabilidades assumidas pela **CONTRATADA**, incluindo a não manutenção das condições de habilitação, ensejará a aplicação de sanções administrativas, previstas no instrumento convocatório e na legislação vigente, podendo culminar em rescisão contratual, por ato unilateral e escrito da **CONTRATANTE**, conforme disposto nos arts. 77 e 80 Lei nº 8.666, de 1993.

7 DO RECEBIMENTO E ACEITAÇÃO DO OBJETO

- 7.1 O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da Contratada pelos prejuízos resultantes da incorreta execução do contrato.
- 7.2 O recebimento definitivo, ato que concretiza o ateste da execução dos serviços, será realizado pelo gestor do contrato.

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 7.2.1. O gestor do contrato analisará os relatórios e toda documentação apresentada pela fiscalização técnica e administrativa e, caso haja irregularidades que impeçam a liquidação e o pagamento da despesa, indicará as cláusulas contratuais pertinentes, solicitando à CONTRATADA, por escrito, as respectivas correções.
- 7.2.2 O gestor emitirá termo circunstanciado para efeito de recebimento definitivo dos serviços prestados, com base nos relatórios e documentação apresentados, e comunicará a CONTRATADA para que emita a Nota Fiscal ou Fatura com o valor exato.

8 DAS SANÇÕES ADMINISTRATIVAS

- 8.1 Comete infração administrativa nos termos da Lei nº 10.520, de 2002, a CONTRATADA que:
- 8.1.1 inexecutar total ou parcialmente qualquer das obrigações assumidas em decorrência da contratação;
 - 8.1.2 ensejar o retardamento da execução do objeto;
 - 8.1.3 falhar ou fraudar na execução do contrato;
 - 8.1.4 comportar-se de modo inidôneo; ou
 - 8.1.5 cometer fraude fiscal.
- 8.2 Pela inexecução total ou parcial do objeto deste contrato, a Administração pode aplicar à CONTRATADA as seguintes sanções:
- 8.2.1 **Advertência por escrito**, quando do não cumprimento de quaisquer das obrigações contratuais consideradas faltas leves, assim entendidas aquelas que não acarretam prejuízos significativos para o serviço contratado;
 - 8.2.2 **Multa:**
 - 8.2.2.1 pagar multa moratória no montante de 1% (um por cento), **por dia de atraso injustificado** sobre o valor da parcela inadimplida até o limite de 10% (dez por cento);

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 8.2.2.2 pagar multa compensatória no montante de 20% (vinte por cento) do valor global do contrato, em se tratando de inadimplemento absoluto;
- 8.2.2.3 impedimento de licitar e de contratar com a União, durante o prazo da sanção, e será descredenciado no Cadastro de Fornecedores do CREA-SP, pelo prazo de até 05 (cinco) anos.

São Paulo, 26 de março de 2018.

Maurício Bachert Torres
Superintendente Administrativo
Portaria nº 29/2017

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP****ANEXO II
FORMAÇÃO DE PREÇO ESTIMATIVO****Lote – “1” - (único)**

Item	Descrição	Quant.	Valor Unitário\$	Valor Total
1	Aquisição de Software de Antivírus. A validade da licenças será perpétua, mas as atualizações da solução de antivírus terão validade de 36 (trinta e seis) meses.	1100 (Unidades)	R\$ 153,10	R\$ 168,417,34
2	Instalação, configuração e treinamento do Software.	80 (horas)	R\$ 471,66	R\$ 37.733,33
Valor Total Geral do Lote = Item 1 + Item 2.....				R\$ 206.150,67



SERVIÇO PÚBLICO FEDERAL

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

ANEXO III

MODELO “A”: EMPREGADOR PESSOA JURÍDICA

DECLARAÇÃO

CREA-SP

Pregão Eletrônico nº 010/2018

Processo Administrativo nº L-175/2017

Objeto: Contratação de empresa para fornecimento, instalação e treinamento de software de antivírus para o CREA-SP.

_____, inscrito no CNPJ nº _____, por intermédio de seu representante legal o(a) Sr(a). _____, portador(a) da Carteira de Identidade nº _____ e do CPF nº _____, **DECLARA**, para fins do disposto no inciso V do art. 27 da Lei nº 8.666, de 21 de junho de 1993, acrescido pela Lei nº 9.854, de 27 de outubro de 1999, que não emprega menor de dezoito anos em trabalho noturno, perigoso ou insalubre, e não emprega menor de dezesseis anos.

Ressalva: emprega menor, a partir de quatorze anos, na condição de aprendiz ().

(local e data)

(representante legal)

Observação: em caso afirmativo, assinalar a ressalva acima.



SERVIÇO PÚBLICO FEDERAL

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

ANEXO IV

FICHA CADASTRAL DE FORNECEDORES

Razão Social		Telefone (1)	
Telefone (2)	Fac-símile	e-mail	
Endereço		Complemento	
Bairro	CEP	Cidade	Estado

Dados do escritório/filial/representação comercial na Cidade de SÃO PAULO, se houver. <i>(somente para a empresa que possui sua sede em outra Cidade)</i>			
Endereço		Complemento	
Bairro	Cidade	Estado	CEP
Telefone	Fac-símile	e-mail	

Objetivo comercial constante do contrato social

Produtos/Serviços que está apta a fornecer

Capital social	Data da última atualização do contrato social	CNPJ
Tempo de atividade	Inscrição estadual	Inscrição municipal

Diretor responsável (nome)	Gerente de vendas (nome)
----------------------------	--------------------------

Nome do responsável pelas informações	Assinatura	Data
---------------------------------------	------------	------

- VIDE VERSO -

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

verso do Anexo IV – Ficha Cadastral de Fornecedores

**DOCUMENTAÇÃO PARA OBTENÇÃO DE REGISTRO
NO CADASTRO DE FORNECEDOR DO CREA-SP**

- 1) Prova de inscrição no Cadastro Nacional de Pessoa Jurídica - CNPJ.
- 2) Prova de inscrição no cadastro de contribuintes estadual, se houver, relativo ao domicílio ou sede do LICITANTE, pertinente ao seu ramo de atividade e compatível com o objeto contratual.
- 3) Prova de inscrição no cadastro de contribuintes municipal, se houver, relativo ao domicílio ou sede do LICITANTE, pertinente ao seu ramo de atividade e compatível com o objeto contratual.
- 4) Prova de regularidade relativa a Seguridade Social – CND/INSS.
- 5) Prova de regularidade relativo ao Fundo de Garantia do Tempo de Serviços – FGTS.
- 6) Prova de regularidade para com a Fazenda Federal, do domicílio ou sede do LICITANTE, ou outra equivalente, na forma da Lei.
- 7) Prova de regularidade para com a Fazenda Estadual, do domicílio ou sede do LICITANTE, ou outra equivalente, na forma da Lei.
- 8) Prova de regularidade para com a Fazenda Municipal, do domicílio ou sede do LICITANTE, ou outra equivalente, na forma da Lei.
- 9) Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de **CNDT** (Certidão Negativa de Débitos Trabalhistas), 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.
- 10) Ato constitutivo, estatuto ou contrato Social ou Estatuto Social em vigor, devidamente registrado, em se tratando de sociedades comerciais, e, no caso de sociedades por ações, acompanhado de documentos de eleição de seus administradores.

Observações:

- a) *Os documentos deverão ser apresentados nos originais ou em cópias autenticadas, podendo este CREA-SP reconhecer a autenticidade de cópias desde que acompanhadas dos seus respectivos originais.*
- b) *Os documentos que não apresentarem data de validade serão considerados válidos por 90 (noventa) dias a contar da data da emissão do respectivo documento.*
- c) *Este cadastro poderá ser atualizado à medida que a documentação solicitada tenha o seu prazo de validade vencido.*

CREA-SP - Unidade de Contratos e Licitação-UCL

Avenida Brigadeiro Faria Lima, 1059 - 7º andar - Pinheiros

01452-920 - SÃO PAULO, SP

Tel. (11) 3095-4725 – 6411 – 6412 ou 6413



SERVIÇO PÚBLICO FEDERAL

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

ANEXO V
MODELO DE DECLARAÇÃO PARA MICROEMPRESA E
EMPRESA DE PEQUENO PORTE

CREA-SP

Pregão Eletrônico nº 010/2018

Processo Administrativo nº L-175/2017

Objeto: Contratação de empresa para fornecimento, instalação e treinamento de software de antivírus para o CREA-SP.

_____, inscrito no **CNPJ/MF** sob o nº _____,
por intermédio de seu representante legal o(a) Sr(a). _____,
portador(a) da Carteira de Identidade nº _____ e do CPF/MF nº _____,
DECLARA, para fins legais, ser Microempresa/Empresa de Pequeno Porte, nos termos da
legislação vigente, em especial no que tange ao conceito trazido pelo artigo 3º da Lei
Complementar nº 123, de 14 de dezembro de 2006, estando apta a usufruir do tratamento
favorecido estabelecido nos artigos 42 a 49 daquela Lei Complementar.

(local e data)

(representante legal)

Observação: A declaração deverá ser feita em papel timbrado da empresa.

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP****ANEXO VI****MINUTA DE TERMO DE CONTRATO****C-***/2018 - SUPJUR****L - 175/2017****CONTRATO PARA FORNECIMENTO, INSTALAÇÃO E TREINAMENTO DE
SOFTWARE DE ANTIVIRUS PARA O CREA-SP**

O **CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA DO ESTADO DE SÃO PAULO**, instituído pelo Decreto Federal n.º 23.569, de 11 de dezembro de 1933 e mantido pela Lei Federal n.º 5.194, de 24 de dezembro de 1966, com sede e foro na Avenida Brigadeiro Faria Lima n.º 1.059, nesta Capital, inscrito no CNPJ sob n.º 60.985.017/0001-77, neste ato representado por seu Presidente, o Engenheiro de Telecomunicações **VINICIUS MARCHESE MARINELLI**, brasileiro, portador da cédula de identidade RG n.º 34.123.915 X SSP/SP e inscrito no CPF/MF n.º 304.423.178-75, registrado no **CREA-SP** sob n.º **5062051089**, doravante denominado simplesmente **CREA-SP**, e de outro lado a Empresa _____, com sede na Rua _____, _____ - _____ - CEP: _____ - _____/_____, inscrita no CNPJ sob n.º _____, Inscrição Estadual n.º _____, Inscrição Municipal n.º _____ e registrada no CREA-SP sob n.º _____, neste ato representada por seu _____, o (a) Sr.(a) _____, portador(a) da Cédula de Identidade RG. n.º _____ e inscrito(a) CPF sob n.º _____, doravante denominada simplesmente **CONTRATADA**, resolvem de comum acordo firmar o presente Contrato conforme Edital do Pregão Eletrônico n.º ***/2018 e r. despacho de fls. _____, nos termos da Lei n.º 10.520/02, do Decreto 5.450/05, bem como, subsidiariamente, a Lei n.º 8.666/93 e suas atualizações, contidos nos autos do Processo Administrativo n.º L-175/2017, e regido pelas seguintes cláusulas e condições:

CLÁUSULA PRIMEIRA - DO OBJETO

1- Constitui objeto do presente contrato o fornecimento de software antivírus para o **CREA-SP**, incluindo instalação, configuração e treinamento do software conforme condições, quantidades e exigências estabelecidas no Edital de Pregão Eletrônico n.º XXX/2018, que passa a fazer parte integrante deste Contrato como se nele estivesse transcrito.

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP****CLÁUSULA SEGUNDA - DAS CARACTERÍSTICAS DO PRODUTO**

2 - A solução ofertada deverá fornecer proteção para os nossos servidores de dados, rede, e-mail e internet, protegendo também os microcomputadores conectados ou não ao nosso Active Directory. A proteção deve ser de âmbito corporativo, possibilitando o gerenciamento centralizado:

6.1 Servidor de Administração e Console Administrativa**6.1.1 Compatibilidade:**

- 6.1.1.1 Microsoft Windows Server 2003 ou superior (Todas edições)
- 6.1.1.2 Microsoft Windows Server 2003 x64 ou superior (Todas edições)
- 6.1.1.3 Microsoft Windows Server 2008 (Todas edições)
- 6.1.1.4 Microsoft Windows Server 2008 Core (Todas edições)
- 6.1.1.5 Microsoft Windows Server 2008 x64 SP1 (Todas edições)
- 6.1.1.6 Microsoft Windows Server 2008 R2 (Todas edições)
- 6.1.1.7 Microsoft Windows Server 2008 R2 Core (Todas edições)
- 6.1.1.8 Microsoft Windows Server 2012 (Todas edições)
- 6.1.1.9 Microsoft Windows Server 2012 R2 (Todas edições)
- 6.1.1.10 Microsoft Windows Server 2016 (Todas edições)
- 6.1.1.11 Microsoft Windows XP Professional SP2 ou superior
- 6.1.1.12 Microsoft Windows XP Professional x64 e superior
- 6.1.1.13 Microsoft Windows Vista SP1
- 6.1.1.14 Microsoft Windows Vista x64 SP1
- 6.1.1.15 Microsoft Windows 7
- 6.1.1.16 Microsoft Windows 7 x64
- 6.1.1.17 Microsoft Windows 8
- 6.1.1.18 Microsoft Windows 8 x64
- 6.1.1.19 Microsoft Windows 10
- 6.1.1.20 Microsoft Windows 10 x64

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP****6.1.2 Suportar as seguintes plataformas virtuais:**

- 6.1.2.1 VMware: Workstation 9.x, Workstation 10.x, ESX 4.x, ESXi 4.x, ESXi 5.5, ESXi 6.0 e ESXi 6.5
- 6.1.2.2 KVM integrado com: RHEL 5.4 e 5.x acima, SLES 11 SPx, Ubuntu 10.10 LTS

6.1.3 Características:

- 6.1.3.1 A console deve ser acessada via WEB (HTTPS) ou MMC;
- 6.1.3.2 Console deve ser baseada no modelo cliente/servidor
- 6.1.3.3 Compatibilidade com Windows Failover Clustering ou outra solução de alta disponibilidade
- 6.1.3.4 Deve permitir a atribuição de perfis para os administradores da Solução de Antivírus.
- 6.1.3.5 Console deve ser totalmente integrada com suas funções e módulos caso haja a necessidade no futuro de adicionar novas tecnologias tais como, criptografia, Patch management e MDM
- 6.1.3.6 As licenças deverão ser perpétuas, ou seja, expirado a validade da mesma o produto deverá permanecer funcional para a proteção contra códigos maliciosos;
- 6.1.3.7 Capacidade de remover remotamente e automaticamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores, sem a necessidade da senha de remoção do atual antivírus;
- 6.1.3.8 Capacidade de instalar remotamente a solução de antivírus nas estações e servidores Windows, através de compartilhamento administrativo, login script e/ou GPO de Active Directory;
- 6.1.3.9 Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 6.1.3.10 A solução de gerencia deve permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas
- 6.1.3.11 Através da solução de gerência, deve ser possível verificar qual licença está aplicada para determinado computador
- 6.1.3.12 Capacidade de instalar remotamente a solução de segurança em smartphones e tablets de sistema iOS, Andoid e Windows
- 6.1.3.13 Capacidade de instalar remotamente qualquer “app” em smartphones e tablets de sistema iOS;
- 6.1.3.14 A solução de gerência centralizada deve permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle
- 6.1.3.15 Deverá ter a capacidade de criar regras para limitar o tráfego de comunicação cliente/servidor por sub rede com os seguintes parâmetros: KB/s e horário.
- 6.1.3.16 Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux e Mac) protegidos pela solução antivírus;
- 6.1.3.17 Capacidade de gerenciar smartphones e tablets (Windows Phone , Android e iOS) protegidos pela solução antivírus;
- 6.1.3.18 Capacidade de gerar pacotes customizados (auto executáveis) contendo a licença e configurações do produto;
- 6.1.3.19 Capacidade de atualizar os pacotes de instalação com as últimas vacinas;
- 6.1.3.20 Capacidade de fazer distribuição remota de qualquer software, ou seja, deve ser capaz de remotamente enviar qualquer software pela estrutura de gerenciamento de antivírus para que seja instalado nas máquinas clientes;

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 6.1.3.21 A comunicação entre o cliente e o servidor de administração deve ser criptografada.
- 6.1.3.22 Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes;
- 6.1.3.23 Deve permitir a realocação de máquinas novas na rede para um determinado grupo sem ter um agente ou endpoint instalado através dos seguintes parâmetros:
 - 6.1.3.23.1 Nome do computador
 - 6.1.3.23.2 Nome do domínio
 - 6.1.3.23.3 Range de IP
 - 6.1.3.23.4 Sistema Operacional
 - 6.1.3.23.5 Máquina virtual
- 6.1.3.24 Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas;
- 6.1.3.25 Deve permitir, por meio da console de gerenciamento, extrair um artefato em quarentena de um cliente sem a necessidade de um servidor ou console de quarentena adicional
- 6.1.3.26 Capacidade de monitorar diferentes subnets de rede a fim de encontrar máquinas novas para serem adicionadas a proteção;
- 6.1.3.27 Capacidade de monitorar grupos de trabalhos já existentes e quaisquer grupos de trabalho que forem criados na rede, a fim de encontrar máquinas novas para serem adicionadas a proteção;
- 6.1.3.28 Capacidade de, assim que detectar máquinas novas no Active Directory, subnets ou grupos de trabalho, automaticamente importar a máquina para a estrutura de proteção da console e verificar se possui o antivírus instalado. Caso não possuir, deve instalar o antivírus automaticamente;

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 6.1.3.29 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;
- 6.1.3.30 Capacidade de definir políticas de configurações diferentes por grupos de estações, permitindo que sejam criados subgrupos e com função de herança de políticas entre grupos e subgrupos;
- 6.1.3.31 Deve fornecer as seguintes informações dos computadores:
- 6.1.3.31.1 Se o antivírus está instalado;
 - 6.1.3.31.2 Se o antivírus está iniciado;
 - 6.1.3.31.3 Se o antivírus está atualizado;
 - 6.1.3.31.4 Minutos/horas desde a última conexão da máquina com o servidor administrativo;
 - 6.1.3.31.5 Minutos/horas desde a última atualização de vacinas
 - 6.1.3.31.6 Data e horário da última verificação executada na máquina;
 - 6.1.3.31.7 Versão do antivírus instalado na máquina;
 - 6.1.3.31.8 Se é necessário reiniciar o computador para aplicar mudanças;
 - 6.1.3.31.9 Data e horário de quando a máquina foi ligada;
 - 6.1.3.31.10 Quantidade de vírus encontrados (contador) na máquina;
 - 6.1.3.31.11 Nome do computador;
 - 6.1.3.31.12 Domínio ou grupo de trabalho do computador;
 - 6.1.3.31.13 Data e horário da última atualização de vacinas;

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 6.1.3.31.14 Sistema operacional com Service Pack;
- 6.1.3.31.15 Quantidade de processadores;
- 6.1.3.31.16 Quantidade de memória RAM;
- 6.1.3.31.17 Usuário(s) logado(s) naquele momento, com informações de contato (caso disponíveis no Active Directory);
- 6.1.3.31.18 Endereço IP;
- 6.1.3.31.19 Aplicativos instalados, inclusive aplicativos de terceiros, com histórico de instalação, contendo data e hora que o software foi instalado ou removido.
- 6.1.3.31.20 Atualizações do Windows Updates instaladas
- 6.1.3.31.21 Informação completa de hardware contendo: processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de áudio, adaptadores de rede, monitores, drives de CD/DVD
- 6.1.3.31.22 Vulnerabilidades de aplicativos instalados na máquina
- 6.1.3.32 Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterá-las;
- 6.1.3.33 Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como:
 - 6.1.3.33.1 Mudança de gateway;
 - 6.1.3.33.2 Mudança de subnet DNS;
 - 6.1.3.33.3 Mudança de domínio;
 - 6.1.3.33.4 Mudança de servidor DHCP;
 - 6.1.3.33.5 Mudança de servidor DNS;
 - 6.1.3.33.6 Mudança de servidor WINS;
 - 6.1.3.33.7 Aparecimento de nova subnet;

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 6.1.3.34 Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet;
- 6.1.3.35 Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes;
- 6.1.3.36 Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus;
- 6.1.3.37 Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos;
- 6.1.3.38 Capacidade de eleger qualquer computador cliente como repositório de vacinas e de pacotes de instalação, sem que seja necessária a instalação de um servidor administrativo completo, onde outras máquinas clientes irão atualizar-se e receber pacotes de instalação, a fim de otimizar tráfego da rede;
- 6.1.3.39 Capacidade de fazer deste repositório de vacinas um gateway para conexão com o servidor de administração, para que outras máquinas que não consigam conectar-se diretamente ao servidor possam usar este gateway para receber e enviar informações ao servidor administrativo.
- 6.1.3.40 Capacidade de exportar relatórios para os seguintes tipos de arquivos: PDF, HTML e XML.
- 6.1.3.41 Capacidade de gerar traps SNMP para monitoramento de eventos;
- 6.1.3.42 Capacidade de enviar e-mails para contas específicas em caso de algum evento;
- 6.1.3.43 Deve possuir compatibilidade com Microsoft NAP, quando instalado em um Windows 2008 Server;

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 6.1.3.44 Deve possuir compatibilidade com Cisco Network Admission Control (NAC);
- 6.1.3.45 Deve possuir documentação da estrutura do banco de dados para geração de relatórios a partir de ferramentas específicas de consulta (Crystal Reports, por exemplo).
- 6.1.3.46 Capacidade de ligar máquinas via Wake on Lan para realização de tarefas (varredura, atualização, instalação, etc), inclusive de máquinas que estejam em subnets diferentes do servidor;
- 6.1.3.47 Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado intervalo de tempo);
- 6.1.3.48 Capacidade de realizar atualização incremental de vacinas nos computadores clientes;
- 6.1.3.49 Deve armazenar localmente e enviar ao servidor de gerência a ocorrência de vírus com os seguintes dados, no mínimo:
 - 6.1.3.49.1 Nome do vírus
 - 6.1.3.49.2 Nome do arquivo infectado
 - 6.1.3.49.3 Data e hora da detecção
 - 6.1.3.49.4 Nome da máquina ou endereço IP
 - 6.1.3.49.5 Ação realizada
- 6.1.3.50 Capacidade de reportar vulnerabilidades de softwares presentes nos computadores.
- 6.1.3.51 Capacidade de realizar inventário de aplicativos de todas as máquinas clientes;
- 6.1.3.52 Capacidade de diferenciar máquinas virtuais de máquinas físicas;

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP****6.2 Em relação as estações Windows****6.2.1 Compatibilidade:**

- 6.2.1.1 Microsoft Windows XP Professional SP3 e superior
- 6.2.1.2 Microsoft Windows Vista Business/Enterprise/Ultimate SP2
- 6.2.1.3 Microsoft Windows Vista Business/Enterprise/Ultimate x64 SP2
- 6.2.1.4 Microsoft Windows 7 Professional/Enterprise/Ultimate
- 6.2.1.5 Microsoft Windows 7 Professional/Enterprise/Ultimate x64
- 6.2.1.6 Microsoft Windows 7 Professional/Enterprise/Ultimate SP1 e superior
- 6.2.1.7 Microsoft Windows 7 Professional/Enterprise/Ultimate x64 SP1 e superior
- 6.2.1.8 Microsoft Windows 8 Professional/Enterprise
- 6.2.1.9 Microsoft Windows 8 Professional/Enterprise x64
- 6.2.1.10 Microsoft Windows 8.1 Enterprise x86 / 64
- 6.2.1.11 Microsoft Windows 8.1 Pro x86 /64
- 6.2.1.12 Microsoft Windows 10 Enterprise x86 / 64
- 6.2.1.13 Microsoft Windows 10 Pro x86 / 64

6.2.2 Características:

- 6.2.2.1 Deve prover as seguintes proteções:
 - 6.2.2.1.1 Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
 - 6.2.2.1.2 Antivírus de Web (módulo para verificação de sites e downloads contra vírus)
 - 6.2.2.1.3 Antivírus de E-mail (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos)

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 6.2.2.1.4 Antivírus de Mensagens Instantâneas (módulo para verificação de mensagens instantâneas, como ICQ, MSN, IRC, etc)
- 6.2.2.1.5 O Endpoint deve possuir opção para rastreamento por linha de comando, parametrizável, com opção de limpeza
- 6.2.2.1.6 Firewall com IDS
- 6.2.2.1.7 Autoproteção (contra-ataques aos serviços/processos do antivírus)
- 6.2.2.1.8 Controle de dispositivos externos
- 6.2.2.1.9 Controle de acesso a sites por categoria
- 6.2.2.1.10 Controle de acesso a sites por horário
- 6.2.2.1.11 Controle de acesso a sites por usuários
- 6.2.2.1.12 Controle de execução de aplicativos
- 6.2.2.1.13 Controle de vulnerabilidades do Windows e dos aplicativos instalados
- 6.2.2.1.14 Capacidade de escolher quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
- 6.2.2.1.15 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).
- 6.2.2.1.16 Capacidade de automaticamente desabilitar o Firewall do Windows (caso exista) durante a instalação, para evitar incompatibilidade com o Firewall da solução;
- 6.2.2.1.17 Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 6.2.2.1.18 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;
- 6.2.2.1.19 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;
- 6.2.2.1.20 Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);
- 6.2.2.1.21 Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
- 6.2.2.1.22 Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomá-la a partir da extensão do arquivo;
- 6.2.2.1.23 Capacidade de verificar somente arquivos novos e alterados;
- 6.2.2.1.24 Capacidade de verificar objetos usando heurística;

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 6.2.2.1.25 Capacidade de agendar uma pausa na verificação;
- 6.2.2.1.26 Deve permitir a filtragem de conteúdo de URL avançada efetuando a classificação dos sites em categorias
- 6.2.2.1.27 Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;
- 6.2.2.1.28 O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
 - 6.2.2.1.28.1 Perguntar o que fazer, ou;
 - 6.2.2.1.28.2 Bloquear acesso ao objeto;
 - 6.2.2.1.28.3 Apagar o objeto ou tentar desinfecção (de acordo com a configuração pré-estabelecida pelo administrador);
 - 6.2.2.1.28.4 Caso positivo de desinfecção:
 - 6.2.2.1.28.4.1 Restaurar o objeto para uso;
 - 6.2.2.1.28.4.2 Caso negativo de desinfecção:
 - 6.2.2.1.28.4.2.1 Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);
- 6.2.2.1.29 Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto.
- 6.2.2.1.30 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);
- 6.2.2.1.31 Capacidade de verificar tráfego de ICQ, MSN, AIM e IRC contra vírus e links phishings;

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 6.2.2.1.32 Capacidade de verificar links inseridos em e-mails contra phishings;
- 6.2.2.1.33 Capacidade de verificar tráfego SSL nos browsers: Internet Explorer, Firefox e Chrome;
- 6.2.2.1.34 Capacidade de verificação de corpo e anexos de e-mails usando heurística;
- 6.2.2.1.35 O antivírus de e-mail, ao encontrar um objeto potencialmente perigoso, deve:
 - 6.2.2.1.35.1 Perguntar o que fazer, ou;
 - 6.2.2.1.35.2 Bloquear o e-mail;
 - 6.2.2.1.35.3 Apagar o objeto ou tentar desinfecção (de acordo com a configuração pré-estabelecida pelo administrador);
 - 6.2.2.1.35.4 Caso positivo de desinfecção:
 - 6.2.2.1.35.4.1 Restaurar o e-mail para o usuário;
 - 6.2.2.1.35.5 Caso negativo de desinfecção:
 - 6.2.2.1.35.5.1 Mover para quarentena ou apagar o objeto (de acordo com a configuração pré-estabelecida pelo administrador);
- 6.2.2.1.36 Caso o e-mail conter código que parece ser, mas não é definitivamente malicioso, o mesmo deve ser mantido em quarentena.
- 6.2.2.1.37 Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados.

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 6.2.2.1.38 Capacidade de filtrar anexos de e-mail, apagando-os ou renomeando-os de acordo com a configuração feita pelo administrador.
- 6.2.2.1.39 Capacidade de verificação de tráfego HTTP e qualquer script do Windows Script Host (JavaScript, Visual Basic Script, etc), usando heurísticas;
- 6.2.2.1.40 Deve ter suporte total ao protocolo IPv6;
- 6.2.2.1.41 Capacidade de alterar as portas monitoradas pelos módulos de Web e E-mail;
- 6.2.2.1.42 Na verificação de tráfego web, caso encontrado código malicioso o programa deve:
 - 6.2.2.1.42.1 Perguntar o que fazer, ou;
 - 6.2.2.1.42.2 Bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio, ou;
 - 6.2.2.1.42.3 Permitir acesso ao objeto;
- 6.2.2.1.43 O antivírus de web deve realizar a verificação de, no mínimo, duas maneiras diferentes, sob escolha do administrador:
 - 6.2.2.1.43.1 Verificação on-the-fly, onde os dados são verificados enquanto são recebidos em tempo real, ou;
 - 6.2.2.1.43.2 Verificação de buffer, onde os dados são recebidos e armazenados para posterior verificação.
- 6.2.2.1.44 Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus de web.

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 6.2.2.1.45 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.
- 6.2.2.1.46 Deve possuir módulo que analise cada macro de VBA executada, procurando por sinais de atividade maliciosa.
- 6.2.2.1.47 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.
- 6.2.2.1.48 Deve possuir módulo de bloqueio de Phishing, com atualizações incluídas nas vacinas, obtidas pelo Anti-Phishing Working Group (<http://www.antiphishing.org/>).
- 6.2.2.1.49 Capacidade de distinguir diferentes sub-nets e conceder opção de ativar ou não o firewall para uma sub-net específica;
- 6.2.2.1.50 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.
- 6.2.2.1.51 O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:
- 6.2.2.1.51.1 Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 6.2.2.1.51.2 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.
- 6.2.2.1.52 Deve possuir módulo que habilite ou não o funcionamento dos seguintes dispositivos externos, no mínimo:
- 6.2.2.1.52.1 Discos de armazenamento locais
 - 6.2.2.1.52.2 Armazenamento removível
 - 6.2.2.1.52.3 Impressoras
 - 6.2.2.1.52.4 Modems
 - 6.2.2.1.52.5 Dispositivos multifuncionais
 - 6.2.2.1.52.6 Leitores de smart card
 - 6.2.2.1.52.7 Dispositivos de sincronização via ActiveSync (Windows CE, Windows, Mobile, etc)
 - 6.2.2.1.52.8 Wi-Fi
 - 6.2.2.1.52.9 Adaptadores de rede externos
 - 6.2.2.1.52.10 Dispositivos MP3 ou smartphones
 - 6.2.2.1.52.11 Dispositivos Bluetooth
- 6.2.2.1.53 Capacidade de liberar acesso a um dispositivo específico e usuários específico por um período de tempo específico, sem a necessidade de desabilitar a proteção, sem desabilitar o gerenciamento central ou de intervenção local do administrador na máquina do usuário.

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 6.2.2.1.54 Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por usuário.
- 6.2.2.1.55 Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por agendamento.
- 6.2.2.1.56 Capacidade de configurar novos dispositivos por Class ID/Hardware ID
- 6.2.2.1.57 Capacidade de limitar o acesso a sites da internet por categoria, por conteúdo (vídeo, áudio, etc), com possibilidade de configuração por usuário ou grupos de usuários e agendamento.
- 6.2.2.1.58 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).
- 6.2.2.1.59 Capacidade de bloquear execução de aplicativo que está em armazenamento externo.
- 6.2.2.1.60 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.
- 6.2.2.1.61 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.

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

6.2.2.1.62 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.

6.2.2.1.63 Capacidade nativa de identificar e remover vírus do tipo RANSOMWARE.

6.3 Em relação aos servidores Windows**6.3.1 Compatibilidade:**

- 6.3.1.1 Microsoft Windows Small Business Server 2011 Essentials/Standard x64
- 6.3.1.2 Microsoft Windows Server 2003 Standard/Enterprise SP2 x86/x64
- 6.3.1.3 Microsoft Windows Server 2003 R2 Standard/Enterprise SP2 x86/x64
- 6.3.1.4 Microsoft Windows Server 2008 Standard/Enterprise/Datacenter SP1 x86/x64
- 6.3.1.5 Microsoft Windows Server 2008 Core Standard/Enterprise/Datacenter SP1 x86/x64
- 6.3.1.6 Microsoft Windows Server 2008 R2 Standard/Enterprise/Datacenter SP1
- 6.3.1.7 Microsoft Windows Server 2008 R2 Core Standard/Enterprise/Datacenter SP1
- 6.3.1.8 Microsoft Windows Server 2012 Foundation/Essentials/Standard x64
- 6.3.1.9 Microsoft Windows Server 2016 Foundation/Essentials/Standard x64
- 6.3.1.10 Microsoft Terminal baseado em Windows Server 2003
- 6.3.1.11 Microsoft Terminal baseado em Windows Server 2008
- 6.3.1.12 Microsoft Terminal baseado em Windows Server 2008 R2

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP****6.3.2 Características:**

- 6.3.2.1 Deve prover as seguintes proteções:
 - 6.3.2.1.1 Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
 - 6.3.2.1.2 Autoproteção contra ataques aos serviços / processos
 - 6.3.2.1.3 Firewall com IDS
 - 6.3.2.1.4 Controle de vulnerabilidades do Windows e dos aplicativos instalados
- 6.3.2.2 Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
- 6.3.2.3 As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora.
- 6.3.2.4 Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
 - 6.3.2.4.1 Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
 - 6.3.2.4.2 Gerenciamento de tarefa (criar ou excluir tarefas de verificação)
 - 6.3.2.4.3 Leitura de configurações
 - 6.3.2.4.4 Modificação de configurações
 - 6.3.2.4.5 Gerenciamento de Backup e Quarentena
 - 6.3.2.4.6 Visualização de relatórios
 - 6.3.2.4.7 Gerenciamento de relatórios
 - 6.3.2.4.8 Gerenciamento de chaves de licença
 - 6.3.2.4.9 Gerenciamento de permissões (adicionar/excluir permissões acima)
- 6.3.2.5 O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 6.3.2.5.1 Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;
- 6.3.2.5.2 Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.
- 6.3.2.6 Capacidade de separadamente selecionar o número de processos que irão executar funções de varredura em tempo real, o número de processos que executarão a varredura sob demanda e o número máximo de processos que podem ser executados no total.
- 6.3.2.7 Capacidade de resumir automaticamente tarefas de verificação que tenham sido paradas por anormalidades (queda de energia, erros, etc)
- 6.3.2.8 Capacidade de automaticamente pausar e não iniciar tarefas agendadas caso o servidor esteja em rodando com fonte ininterrupta de energia (uninterruptible Power supply – UPS)
- 6.3.2.9 Em caso erros, deve ter capacidade de criar logs e traces automaticamente, sem necessidade de outros softwares;
- 6.3.2.10 Capacidade de configurar níveis de verificação diferentes para cada pasta, grupo de pastas ou arquivos do servidor.
- 6.3.2.11 Capacidade de bloquear comunicação a servidores acessados por estações de trabalho infectadas e quando estações tentarem gravar arquivos infectados nos servidores.
- 6.3.2.12 Capacidade de criar uma lista de máquina que nunca serão bloqueadas mesmo quando infectadas.

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 6.3.2.13 Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;
- 6.3.2.14 Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: "Win32.Trojan.banker") para que qualquer objeto detectado com o veredicto escolhido seja ignorado;
- 6.3.2.15 Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
- 6.3.2.16 Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomá-la a partir da extensão do arquivo;
- 6.3.2.17 Capacidade de verificar somente arquivos novos e alterados;
- 6.3.2.18 Capacidade de escolher qual tipo de objeto composto será verificado (ex: arquivos comprimidos, arquivos auto descompressores, .PST, arquivos compactados por compactadores binários, etc)
- 6.3.2.19 Capacidade de verificar objetos usando heurística;
- 6.3.2.20 Capacidade de configurar diferentes ações para diferentes tipos de ameaças;
- 6.3.2.21 Capacidade de agendar uma pausa na verificação;
- 6.3.2.22 Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;
- 6.3.2.23 O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 6.3.2.23.1 Perguntar o que fazer, ou;
- 6.3.2.23.2 Bloquear acesso ao objeto;
- 6.3.2.23.2.1 Apagar o objeto ou tentar desinfecção (de acordo com a configuração pré-estabelecida pelo administrador);
- 6.3.2.23.2.2 Caso positivo de desinfecção:
 - 6.3.2.23.2.2.1 Restaurar o objeto para uso;
 - 6.3.2.23.2.2.3 Caso negativo de desinfecção:
- 6.3.2.23.3 Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);
- 6.3.2.24 Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto.
- 6.3.2.25 Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena
- 6.3.2.26 Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados
- 6.3.2.27 Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa.
- 6.3.2.28 Capacidade nativa de identificar e remover vírus do tipo RANSOMWARE.

6.4 Em relação aos servidores Linux**6.4.1 Compatibilidade:****6.4.1.1 Plataforma 32-bits:**

- 6.4.1.1.1 Red Hat Enterprise Linux 7.x Server;
- 6.4.1.1.2 Red Hat Enterprise Linux 6.x Server;
- 6.4.1.1.3 Red Hat Enterprise Linux 5.x Server;
- 6.4.1.1.4 CentOS-7 e CentOS-6;
- 6.4.1.1.5 SUSE Linux Enterprise Server 12 SP2;

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 6.4.1.1.6 openSUSE Linux 12.1;
 - 6.4.1.1.7 openSUSE Linux 12.2;
 - 6.4.1.1.8 Debian GNU/Linux 9.1.
- 6.4.1.2 Plataforma 64-bits:
- 6.4.1.2.1 Red Hat Enterprise Linux 7.x Server;
 - 6.4.1.2.2 Red Hat Enterprise Linux 6.x Server;
 - 6.4.1.2.3 Red Hat Enterprise Linux 5.x Server;
 - 6.4.1.2.4 CentOS-6 e CentOS-7;
 - 6.4.1.2.5 SUSE Linux Enterprise Server 12 SP2;
 - 6.4.1.2.6 openSUSE Linux 12.1;
 - 6.4.1.2.7 openSUSE Linux 12.2;
 - 6.4.1.2.8 Debian GNU/Linux 9.1.

6.4.2 Características:

- 6.4.2.1 Deve prover as seguintes proteções:
- 6.4.2.2 Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
- 6.4.2.3 As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora.
- 6.4.2.4 Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
 - 6.4.2.4.1 Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
 - 6.4.2.4.2 Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfetar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 6.4.2.4.3 Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;
- 6.4.2.4.4 Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados.
- 6.4.2.4.5 Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares;
- 6.4.2.4.6 Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
- 6.4.2.4.7 Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomá-la a partir da extensão do arquivo;
- 6.4.2.4.8 Capacidade de verificar objetos usando heurística;
- 6.4.2.4.9 Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena
- 6.4.2.4.10 Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

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

6.5 Em relação a Smartphones e tablets**6.5.1 Compatibilidade:**

6.5.1.1 Apple iOS 7.0 – 10.3

6.5.1.2 Windows Phone 8.1

6.5.1.3 Android OS 2.3 – 7.0

6.5.2 Características:

6.5.2.1 Deve prover as seguintes proteções:

6.5.2.1.1 Proteção em tempo real do sistema de arquivos do dispositivo – interceptação e verificação de:

6.5.2.1.1.1 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.

6.5.2.1.1.2 Arquivos abertos no smartphone

6.5.2.1.1.3 Programas instalados usando a interface do smartphone

6.5.2.1.2 Verificação dos objetos na memória interna do smartphone e nos cartões de expansão sob demanda do usuário e de acordo com um agendamento;

6.5.2.2 Deverá isolar em área de quarentena os arquivos infectados;

6.5.2.3 Deverá atualizar as bases de vacinas de modo agendado;

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 6.5.2.4 Deverá bloquear spams de SMS através de Black lists;
- 6.5.2.5 Deverá ter função de bloqueio do aparelho caso o SIM CARD for trocado para outro não autorizado;
- 6.5.2.6 Capacidade de desativar por política: Wi-fi, Câmera, Bluetooth
- 6.5.2.7 Deverá ter função de limpeza de dados pessoais a distância, em caso de roubo, por exemplo.
- 6.5.2.8 Capacidade de requerer uma senha para desbloquear o dispositivo e personalizar a quantidade de caracteres para esta senha
- 6.5.2.9 Deverá ter firewall pessoal;
- 6.5.2.10 Capacidade de tirar fotos quando a senha for inserida incorretamente (Mugshot)
- 6.5.2.11 Possibilidade de instalação remota utilizando o Microsoft System Center Mobile Device Manager 2008 SP1
- 6.5.2.12 Capacidade de enviar comandos remotamente de:
 - 6.5.2.12.1 Localizar
 - 6.5.2.12.2 Bloquear
- 6.5.2.13 Capacidade de detectar Jailbreak em dispositivos iOS
- 6.5.2.14 Capacidade de bloquear o acesso a site por categoria em dispositivos
- 6.5.2.15 Capacidade de bloquear o acesso a sites phishing ou malicioso
- 6.5.2.16 Capacidade de criar containers de aplicativos, separando dados corporativos de dados pessoais
- 6.5.2.17 Capacidade de bloquear o dispositivo quando o cartão “SIM” for substituído
- 6.5.2.18 Capacidade de configurar White e blacklist de aplicativos
- 6.5.2.19 Capacidade de localizar o dispositivo quando necessário
- 6.5.2.20 Permitir atualização das definições quando estiver em “roaming”

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 6.5.2.21 Capacidade de selecionar endereço do servidor para buscar a definição de vírus
- 6.5.2.22 Capacidade de enviar URL de instalação por e-mail
- 6.5.2.23 Capacidade de executar as seguintes ações caso a desinfecção falhe:
 - 6.5.2.23.1 Deletar
 - 6.5.2.23.2 Ignorar
 - 6.5.2.23.3 Quarentena.
 - 6.5.2.23.4 Perguntar ao usuário

6.6 Gerenciamento de dispositivos móveis (MDM):**6.6.1 Compatibilidade:**

- 6.6.1.1 Dispositivos conectados através do Microsoft Exchange ActiveSync
- 6.6.1.2 Apple iOS
- 6.6.1.3 Windows Phone
- 6.6.1.4 Android

6.6.2 Dispositivos com suporte ao Apple Push Notification (APNs) servisse

- 6.6.2.1 Apple iOS 3.0 ou superior

6.6.3 Características:

- 6.6.3.1 Capacidade de aplicar políticas de ActiveSync através do servidor Microsoft Exchange
- 6.6.3.2 Capacidade de ajustar as configurações de:
 - 6.6.3.2.1 Sincronização de e-mail
 - 6.6.3.2.2 Uso de aplicativos
 - 6.6.3.2.3 Senha do usuário
 - 6.6.3.2.4 Criptografia de dados
 - 6.6.3.2.5 Conexão de mídia removível

- 6.6.3.3 Capacidade de instalar certificados digitais em dispositivos móveis

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 6.6.3.4 Capacidade de, remotamente, resetar a senha de dispositivos iOS
- 6.6.3.5 Capacidade de, remotamente, apagar todos os dados de dispositivos iOS
- 6.6.3.6 Capacidade de, remotamente, bloquear um dispositivo iOS

6.7 Criptografia:**6.7.1 Compatibilidade:**

- 6.7.1.1 Microsoft Windows XP Professional SP3 ou superior
- 6.7.1.2 Microsoft Windows Vista Business/Enterprise/Ultimate SP2
- 6.7.1.3 Microsoft Windows Vista Business/Enterprise/Ultimate x64 SP2
- 6.7.1.4 Microsoft Windows 7 Professional/Enterprise/Ultimate
- 6.7.1.5 Microsoft Windows 7 Professional/Enterprise/Ultimate x64
- 6.7.1.6 Microsoft Windows 8 Professional/Enterprise
- 6.7.1.7 Microsoft Windows 8 Professional/Enterprise x64
- 6.7.1.8 Microsoft Windows 8.1 Professional / Enterprise
- 6.7.1.9 Microsoft Windows 8.1 Professional / Enterprise x64
- 6.7.1.10 Microsoft Windows 10 Pro x86 / x64
- 6.7.1.11 Microsoft Windows 10 Enterprise x86 /x64

6.7.2 Características:

- 6.7.2.1 O acesso ao recurso criptografado (arquivo, pasta ou disco) deve ser garantido mesmo em caso o usuário tenha esquecido a senha, através de procedimentos de recuperação.
- 6.7.2.2 Utilizar, no mínimo, algoritmo AES com chave de 256 bits.
- 6.7.2.3 Capacidade de criptografar completamente o disco rígido da máquina, adicionando um ambiente de pré-boot para autenticação do usuário.

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 6.7.2.4 Capacidade de utilizar Single Sign-On para a autenticação de pré-boot.
- 6.7.2.5 Permitir criar vários usuários de autenticação pré-boot.
- 6.7.2.6 Capacidade de criar um usuário de autenticação pré-boot comum com uma senha igual para todas as máquinas a partir da console de gerenciamento.
- 6.7.2.7 Capacidade de criptografar drives removíveis de acordo com regra criada pelo administrador, com as opções:
 - 6.7.2.7.1 Criptografar somente os arquivos novos que forem copiados para o disco removível, sem modificar os arquivos já existentes.
 - 6.7.2.7.2 Criptografar todos os arquivos individualmente.
 - 6.7.2.7.3 Criptografar o dispositivo inteiro, de maneira que não seja possível listar os arquivos e pastas armazenadas.
 - 6.7.2.7.4 Criptografar o dispositivo em modo portátil, permitindo acessar os arquivos em máquinas de terceiros através de uma senha.
- 6.7.2.8 Capacidade de selecionar pastas e arquivos (por tipo, ou extensão) para serem criptografados automaticamente. Nesta modalidade, os arquivos devem estar acessíveis para todas as máquinas gerenciadas pela mesma console de maneira transparente para os usuários.
- 6.7.2.9 Capacidade de criar regras de exclusões para que certos arquivos ou pastas nunca sejam criptografados.
- 6.7.2.10 Capacidade de selecionar aplicações que podem ou não ter acesso aos arquivos criptografados.
- 6.7.2.11 Verifica compatibilidade de hardware antes de aplicar a criptografia

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 6.7.2.12 Possibilita estabelecer parâmetros para a senha de criptografia
- 6.7.2.13 Bloqueia o reuso de senhas
- 6.7.2.14 Bloqueia a senha após um número de tentativas pré-estabelecidas
- 6.7.2.15 Capacidade de permitir o usuário solicitar permissão a determinado arquivo criptografado para o administrador mediante templates customizados
- 6.7.2.16 Permite criar exclusões para não criptografar determinados “discos rígidos” através de uma busca por nome do computador ou nome do dispositivo
- 6.7.2.17 Permite criptografar as seguintes pastas pré-definidas: “meus documentos”, “Favoritos”, “Desktop”, “Arquivos temporários” e “Arquivos do outlook”
- 6.7.2.18 Permite utilizar variáveis de ambiente para criptografar pastas customizadas.
- 6.7.2.19 Capacidade de criptografar arquivos por grupos de extensão, tais como: Documentos do office, Document, arquivos de áudio, etc
- 6.7.2.20 Permite criar um grupo de extensões de arquivos a serem criptografados
- 6.7.2.21 Capacidade de criar regra de criptografia para arquivos gerados por aplicações
- 6.7.2.22 Permite criptografia de dispositivos móveis mesmo quando o endpoint não possuir comunicação com a console de gerenciamento.

6.8 Gerenciamento de Sistemas:

- 6.8.1 Capacidade de criar imagens de sistema operacional remotamente e distribuir essas imagens para computadores gerenciados pela solução e para computadores bare-metal.

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 6.8.2 Capacidade de detectar softwares de terceiros vulneráveis, criando assim um relatório de softwares vulneráveis.
- 6.8.3 Capacidade de corrigir as vulnerabilidades de softwares, fazendo o download centralizado da correção ou atualização e aplicando essa correção ou atualização nas máquinas gerenciadas de maneira transparente para os usuários.
- 6.8.4 Possuir tecnologia de Controle de Admissão de Rede (NAC), com a possibilidade de criar regras de quais tipos de dispositivos podem ter acessos a recursos da rede.
- 6.8.5 Capacidade de gerenciar licenças de softwares de terceiros.
- 6.8.6 Capacidade de registrar mudanças de hardware nas máquinas gerenciadas.
- 6.8.7 Capacidade de gerenciar um inventário de hardware, com a possibilidade de cadastro de dispositivos (ex: router, switch, projetor, acessório, etc), informando data de compra, local onde se encontra, service tag, número de identificação e outros.
- 6.8.8 Possibilita fazer distribuição de software de forma manual e agendada
- 6.8.9 Suporta modo de instalação silenciosa
- 6.8.10 Suporte a pacotes MSI, exe, bat, cmd e outros padrões de arquivos executáveis
- 6.8.11 Possibilita fazer a distribuição através de agentes de atualização
- 6.8.12 Utiliza tecnologia multicast para evitar tráfego na rede
- 6.8.13 Possibilita criar um inventário centralizado de imagens
- 6.8.14 Capacidade de atualizar o sistema operacional direto da imagem mantendo os dados do usuário
- 6.8.15 Suporte a WakeOnLan para deploy de imagens
- 6.8.16 Capacidade de atuar como servidor de atualização do Windows podendo fazer deploy de patches

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 6.8.17 Suporta modo de teste, podendo atribuir alguns computadores para receberem as atualizações de forma automática para avaliação de alterações no comportamento
- 6.8.18 Capacidade de gerar relatórios de vulnerabilidades e patches
- 6.8.19 Possibilita criar exclusões para aplicação de patch por tipo de sistema operacional, Estação de trabalho e Servidor ou por grupo de administração
- 6.8.20 Permite iniciar instalação de patch e correções de vulnerabilidades ao reiniciar ou desligar o computador
- 6.8.21 Permite baixar atualizações para o computador sem efetuar a instalação
- 6.8.22 Permite o administrador instalar somente atualizações aprovadas, instalar todas as atualizações (exceto as bloqueadas) ou instalar todas as atualizações incluindo as bloqueadas
- 6.8.23 Capacidade de instalar correções de vulnerabilidades de acordo com a severidade
- 6.8.24 Permite selecionar produtos a serem atualizados pela console de gerenciamento
- 6.8.25 Permite selecionar categorias de atualizações para serem baixadas e instaladas, tais como: atualizações de segurança, ferramentas, drivers, etc

6.9 Serviços de Instalação, configuração e treinamento do software.

- 6.9.1 Declaração de que todos os serviços serão executados por técnicos certificados pelo Fabricante do software.
- 6.9.2 Na contratação deverá apresentar a certificação dos técnicos mediante certificados emitidos pelo fabricante.
- 6.9.3 Documentação do Plano Técnico do Projeto e a Implementação do mesmo, deverá ser apresentado na entrega das licenças.

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

- 6.9.4 Instalação e configuração total de todas as licenças do software adquirido no ambiente físico/virtual da CONTRATANTE;
- 6.9.5 Validação das soluções implantadas;
- 6.9.6 Criação das rotinas e teste de Backup/Restore;
- 6.9.7 Treinamento pelo fabricante ou por técnicos homologados pelo fabricante para ministrar treinamento para 4 colaboradores, designados pelo Gestor da Unidade de Suporte ao Usuário - DIF/USU;
- 2.9.7.a - O treinamento será realizado na sua integridade, nas dependências do CREA-SP, Avenida Brigadeiro Faria Lima, 1059 - Pinheiros, São Paulo/SP;
- 2.9.7.b - O treinamento ocorrerá de forma concomitante à instalação das licenças de software, ou seja, durante o período de operacionalização das licenças;
- 6.9.8 Entrega dos ambientes em produção;
- 6.9.9 Políticas de segurança definidas;
- 6.9.10 Elaboração do documento técnico final do projeto;
- 6.9.11 Aceite por parte da CONTRATANTE.

CLÁUSULA TERCEIRA - DO RECEBIMENTO E ACEITAÇÃO DO OBJETO

3 - O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da Contratada pelos prejuízos resultantes da incorreta execução do contrato.

3.1 - O recebimento definitivo, ato que concretiza o ateste da execução dos serviços, será realizado pelo gestor do contrato.

3.2 - O gestor do contrato analisará os relatórios e toda documentação apresentada pela fiscalização técnica e administrativa e, caso haja irregularidades que impeçam a liquidação e o pagamento da despesa, indicará as

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

cláusulas contratuais pertinentes, solicitando à **CONTRATADA**, por escrito, as respectivas correções.

3.3 - O gestor emitirá termo circunstanciado para efeito de recebimento definitivo dos serviços prestados, com base nos relatórios e documentação apresentados, e comunicará a **CONTRATADA** para que emita a Nota Fiscal ou Fatura com o valor exato.

CLÁUSULA QUARTA - VIGÊNCIA, GARANTIA E VALIDADE DAS LICENÇAS

4 - A vigência do contrato fica restrita ao efetivo cumprimento das obrigações de ambas as partes, ressalvada a validade das licenças e atualizações da solução de antivírus, na forma estabelecida no item seguinte.

4.1 - A validade das licenças será perpétua, mas as atualizações da solução de antivírus terão validade de 36 (trinta e seis) meses.

CLÁUSULA QUINTA - OBRIGAÇÕES DO CREA-SP

5 - Acompanhar e fiscalizar todas as etapas da prestação dos serviços, através de seu corpo técnico;

5.1 - Disponibilizar espaço físico e infraestrutura técnica para que os serviços sejam realizados;

5.2 - Realizar os pagamentos devidos à **CONTRATADA** no prazo contratual.

CLÁUSULA - SEXTA - OBRIGAÇÕES DA CONTRATADA

6 - A **CONTRATADA** deverá:

6.1 - Contratar, treinar e manter empregados em quantidade e qualificação compatíveis para a execução dos serviços objeto da contratação, sendo considerada neste particular, como única empregadora.

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

6.2 - Fazer cumprir as normas disciplinares e de segurança. Cumprir as exigências das leis trabalhistas, previdenciárias e sindicais relativamente aos empregados, envolvidos na execução dos serviços, inclusive as determinações emanadas da fiscalização da Prefeitura, fazendo prova dos recolhimentos devidos.

6.3 - Responder por quaisquer acidentes, danos ou prejuízos materiais e/ou pessoais causados ao **CREA-SP**, seus funcionários e/ou terceiros, por dolo e/ou culpa de seus empregados.

6.4 - Desenvolver boas relações com os funcionários do CREA-SP, acatando quaisquer instruções e o que mais emanar da fiscalização.

6.5 - Informar o Departamento de Informática do **CREA-SP** quaisquer irregularidades identificadas durante os procedimentos técnicos que possam vir impactar na execução total dos serviços.

6.6 - Comunicar ao **CREA-SP**, imediatamente, qualquer ocorrência ou anormalidade que venha interferir na execução dos serviços.

6.7 - Arcar com os ônus decorrentes da incidência de todos os tributos federais, estaduais e municipais que possam advir dos serviços contratados, responsabilizando-se pelo cumprimento de todas as exigências das repartições competentes, com total isenção da Prefeitura.

CLÁUSULA SÉTIMA – DO PREÇO E DA CONDIÇÃO DE PAGAMENTO

7- Pelo fornecimento, instalação, configuração e treinamento do software objeto do presente Contrato, o **CREA-SP** pagará à CONTRATADA os seguintes valores, conforme quadro abaixo:

Lote – “1” - (único)

Item	Descrição	Quant.	Valor Unitário	Valor Total
1	Aquisição de Software de Antivírus. A validade das licenças será perpétua, mas as atualizações da solução de antivírus terão validade de 36 (trinta e seis) meses.	1100 (Unidades)	R\$	R\$
2	Instalação, configuração e treinamento do Software.	80 (horas)	R\$	R\$
Total Geral do Lote = Item 1 + Item 2.....				



SERVIÇO PÚBLICO FEDERAL

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

7.1 - O CREA-SP pagará à **CONTRATADA**, vencedora do Lote “1” único, após 15 (quinze) dias úteis, contados a partir da apresentação das Notas Fiscais ou Faturas, as quais deverão ser entregues na Unidade de Suporte ao Usuários - USU do **CREA-SP**, sito à Avenida Brigadeiro Faria Lima, 1059 - Térreo – Pinheiros- São Paulo- SP. A emissão das Notas Fiscais ou Faturas se darão mediante prévia autorização para faturamento emitida pelo Gestor da Unidade de Suporte ao Usuário, após verificação das condições expressas no Edital, acompanhada dos seguintes documentos:

7.2 - Prova de regularidade relativo ao Fundo de Garantia do Tempo de Serviços (FGTS);

7.3 - Prova de regularidade para com a Fazenda Federal, que abrange também a prova de regularidade relativa à Seguridade Social (conforme Portarias nºs 358, de 5 de setembro de 2014 e 1751, de 2 de outubro de 2014);

7.4 - Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de CNDT (Certidão Negativa de Débitos Trabalhistas), 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;

7.5 - A emissão da Nota Fiscal/Fatura será precedida do recebimento provisório e definitivo do serviço, nos seguintes termos:

7.5.a - O termo de recebimento provisório será assinado pelo CREA-SP e CONTRATADA, assim que todas as licenças estiverem instaladas e configuradas, como também o treinamento realizado.

7.5.b - Após 10(dez) dias, realizados os testes de conformidade e também verificações operacionais, será emitido o termo de recebimento definitivo.

7.6 - Realizar a análise de toda documentação apresentada, verificação da entrega dos serviços de acordo com as cláusulas contratuais, e, se, caso haja irregularidades que impeçam a liquidação e o pagamento da despesa, indicar as cláusulas contratuais pertinentes, solicitando à CONTRATADA, por escrito, as respectivas correções.

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

7.7 - Emitir Termo Circunstanciado para efeito de recebimento definitivo dos serviços prestados, com base nos relatórios e documentações apresentadas; e

7.8 - Comunicar a empresa para que emita a Nota Fiscal ou Fatura, com o valor exato dimensionado pela fiscalização.

7.9 - Os pagamentos decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 24 da Lei 8.666, de 1993, deverão ser efetuados no prazo de até 5 (cinco) dias úteis, contados da data da apresentação da Nota Fiscal/Fatura, nos termos do art. 5º, § 3º, da Lei nº 8.666, de 1993.

7.10 - O pagamento somente será autorizado depois de efetuado o “atesto” pelo servidor competente, devidamente acompanhada das comprovações mencionadas no item “2” do Anexo XI da IN SEGES/MPDG n. 5/2017.

7.10.a - Quando do recebimento e aceitação do objeto, o Gestor do contrato analisará também os relatórios e documentação referentes ao treinamento.

7.11 - Caso se constate o descumprimento de obrigações trabalhistas ou da manutenção das condições exigidas para habilitação poderá ser concedido um prazo para que a **CONTRATADA** regularize suas obrigações, quando não se identificar má-fé ou a incapacidade de corrigir a situação.

7.12 - Não sendo regularizada a situação da **CONTRATADA** no prazo concedido, ou nos casos em que identificada má-fé, se não for possível a realização desses pagamentos pela própria Administração, os valores retidos cautelarmente serão depositados junto à Justiça do Trabalho, com o objetivo de serem utilizados exclusivamente no pagamento de salários e das demais verbas trabalhistas, bem como das contribuições sociais e FGTS decorrentes.

7.13 - Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.



SERVIÇO PÚBLICO FEDERAL

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

7.14 - Antes de cada pagamento à **CONTRATADA**, será realizada consulta dos documentos de regularidade fiscal para verificar a manutenção das condições de habilitação exigidas no Edital.

7.15 - Constatando-se, a situação de irregularidade da **CONTRATADA**, será providenciada sua advertência, por escrito, para que, no prazo de 5 (cinco) dias, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério do CREA-SP.

7.16 - Não havendo regularização ou sendo a defesa considerada improcedente, o **CREA-SP** deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência da **CONTRATADA**, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

7.17 - Persistindo a irregularidade, o **CREA-SP** deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada à **CONTRATADA** a ampla defesa.

7.18 - Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso a **CONTRATADA** não regularize sua situação.

7.19 - Somente por motivo de economicidade, segurança nacional ou outro interesse público de alta relevância, devidamente justificado, em qualquer caso, pela máxima autoridade do **CREA-SP**, não será rescindido o contrato em execução com a **CONTRATADA** inadimplente.

7.20 - Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável, nos termos do item 6 do Anexo XI da IN SEGES/MPDG n. 5/2017, quando couber:

7.21 - A **CONTRATADA** regularmente optante pelo Simples Nacional, exclusivamente para as atividades de prestação de serviços previstas no §5º-C, do art. 18, da LC 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime, observando-se as exceções nele

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

previstas. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

CLÁUSULA OITAVA - DA GESTÃO E FISCALIZAÇÃO DO CONTRATO

8 - A Gestão do Contrato e a Fiscalização do cumprimento do objeto contratado será de competência da Unidade de Suporte ao Usuário - USU, a quem a **CONTRATADA** deverá reportar-se quanto aos assuntos oriundos da execução do mesmo.

8.1 - Em hipótese alguma, será admitido que a própria **CONTRATADA** materialize a avaliação de desempenho e qualidade da prestação dos serviços realizada.

8.2 - Na hipótese de comportamento contínuo de desconformidade da prestação do serviço em relação à qualidade exigida, bem como quando esta ultrapassar os níveis mínimos toleráveis previstos nos indicadores, além dos fatores redutores, devem ser aplicadas as sanções à **CONTRATADA** de acordo com as regras previstas no ato convocatório.

8.3 - O representante do **CREA-SP** deverá promover o registro das ocorrências verificadas, adotando as providências necessárias ao fiel cumprimento das cláusulas contratuais, conforme o disposto nos §§ 1º e 2º do art. 67 da Lei nº 8.666, de 1993.

8.4 - O descumprimento total ou parcial das obrigações e responsabilidades assumidas pela **CONTRATADA**, incluindo a não manutenção das condições de habilitação, ensejará a aplicação de sanções administrativas, previstas no instrumento convocatório e na legislação vigente, podendo culminar em rescisão contratual, por ato unilateral e escrito do **CREA-SP**, conforme disposto nos arts. 77 e 80 Lei nº 8.666, de 1993.

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP****CLÁUSULA NONA - DAS SANÇÕES ADMINISTRATIVAS**

9 - Comete infração administrativa nos termos da Lei nº 10.520, de 2002, a **CONTRATADA** que:

- a) inexecutar total ou parcialmente qualquer das obrigações assumidas em decorrência da contratação;
- b) ensejar o retardamento da execução do objeto;
- c) falhar ou fraudar na execução do contrato;
- d) comportar-se de modo inidôneo; ou
- e) cometer fraude fiscal.

9.1 - Pela inexecução total ou parcial do objeto deste contrato, a Administração pode aplicar à **CONTRATADA** as seguintes sanções:

a) Advertência por escrito, quando do não cumprimento de quaisquer das obrigações contratuais consideradas faltas leves, assim entendidas aquelas que não acarretam prejuízos significativos para o serviço contratado;

b) Multa:

b.1) pagar multa moratória no montante de 1% (um por cento), **por dia de atraso injustificado** sobre o valor da parcela inadimplida até o limite de 10% (dez por cento);

b.2) pagar multa compensatória no montante de 20% (vinte por cento) do valor global do contrato, em se tratando de inadimplemento absoluto;

b.3) impedimento de licitar e de contratar com a União, durante o prazo da sanção, e será descredenciado no Cadastro de Fornecedores do CREA-SP, pelo prazo de até 05 (cinco) anos.

CLÁUSULA DÉCIMA - DA DOTAÇÃO ORÇAMENTÁRIA

10- A Dotação Orçamentária para as despesas oriundas da presente contratação advirá das contas nº 6.2.2.1.1.02.02.05.001 – Direito de Uso de Software e 6.2.2.1.1.01.04.09.005 - Serviços de Informática.



SERVIÇO PÚBLICO FEDERAL

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

CLÁUSULA DÉCIMA PRIMEIRA - DO AUMENTO OU SUPRESSÃO

11- A **CONTRATADA** ficará obrigada a aceitar, nas mesmas condições contratuais, os acréscimos e supressões que se fizerem necessários no objeto deste contrato durante a vigência contratual, até o limite de 25% (vinte e cinco por cento), conforme disposto no artigo 65, § 1º, da Lei nº 8.666/93, e suas atualizações.

11.1- Nenhum acréscimo ou supressão poderá exceder os limites estabelecidos no item anterior, salvo para as supressões resultantes de acordo celebrado entre as partes.

CLÁUSULA DÉCIMA SEGUNDA - DO EXERCÍCIO DOS DIREITOS

12- Qualquer omissão ou tolerância das partes em exigir o estrito cumprimento dos termos e condições do presente Contrato, ou em exercer uma prerrogativa dele decorrente, não constituirá renúncia, nem afetará o direito da parte de exercê-lo a qualquer tempo.

CLÁUSULA DÉCIMA TERCEIRA – DO PREPOSTO DA CONTRATADA

13- Fica estabelecido que o Preposto da **CONTRATADA** para representá-la perante o **CREA-SP** na execução do presente Contrato é o Senhor (a) _____.

CLÁUSULA DÉCIMA QUARTA – DAS CONSIDERAÇÕES GERAIS

14- É expressamente proibida, por parte da **CONTRATADA**, durante a execução do objeto deste Contrato, a contratação de servidor pertencente ao quadro de pessoal do **CREA-SP**.

14.1- 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.

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

14.2- A **CONTRATADA** se compromete a manter durante a execução do presente Contrato, todas as condições de habilitação e qualificação exigidas no Edital de Pregão Eletrônico n.º ***/2018.

14.3- Integra o presente Contrato como se nele estivesse transcrito o Edital de Pregão Eletrônico n.º ***/2018, seus anexos e a Proposta Comercial apresentada pela **CONTRATADA**, anexados no processo administrativo L-175/2017.

14.4- O presente Contrato não autoriza, nem a **CONTRATADA** tem direito nem poderes e nem deverá comprometer ou vincular a Administração Pública Contratante 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.

14.5- Caso qualquer das Cláusulas deste Contrato seja ou se torne legalmente ineficaz a validade do documento como um todo não deverá ser afetada.

14.6- As eventuais omissões existentes no presente Contrato serão supridas pelas disposições da Lei n.º 10.520/02, Decreto n.º 5.450/05 e Lei n.º 8666/93 e suas atualizações e demais normas aplicáveis ao objeto do presente Contrato.

CLÁUSULA DÉCIMA QUINTA – DO FORO DE ELEIÇÃO

15- As partes de comum acordo elegem o Foro da Capital, para dirimir qualquer lide oriunda do presente Contrato, com renúncia expressa de qualquer outro por mais privilegiado que seja.

**SERVIÇO PÚBLICO FEDERAL****CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA
DO ESTADO DE SÃO PAULO – CREA-SP**

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

São Paulo, de de 2018.

Engenheiro *VINICIUS MARCHESE MARINELLI*
CREA-SP nº 5062051089
PRESIDENTE DO CREA-SP

CONTRATADA

TESTEMUNHAS:

1) _____ 2) _____
Nome: Nome:
RG: RG: