PREFEITURA MUNICIPAL DE SANTO ANDRÉ
SECRETARIA DE ASSUNTOS JURÍDICOS
DEPARTAMENTO DE LICITAÇÕES

PREGÃO PRESENCIAL
Processo Administrativo nº 31833/2018
Pregão nº 068/19 (reprogramado)

1. PREÂMBULO

1.1. Tornamos público que por autorização do(a) Senhor(a) Secretário(a) de Assuntos Jurídicos, em cumprimento à Programação da(s) Secretaria(s) mencionada(s) no Anexo I deste Edital, acha-se aberta nesta Prefeitura, LICITAÇÃO NA MODALIDADE **PREGÃO PRESENCIAL**, a qual será regida pela Lei Federal nº 10.520/02 e, subsidiariamente, pela Lei Federal nº 8.666/93, Lei Complementar nº 123/06 e Leis Municipais nºs 9.487/13 e 9.940/17 e pelos Decretos Municipais nºs 15.926/09, 15.929/09, 16.653/15 e 17.030/18 e processada em conformidade com as disposições deste Edital e de seus Anexos.

1.2. Os envelopes intitulados de "A – Proposta Comercial" e "B – Documentos de Habilitação", bem como o credenciamento deverão ser apresentados na Prefeitura Municipal de Santo André (PMSA), na data, hora e endereço indicados no Anexo I, quando serão recebidos e abertos na forma prevista neste Edital e em seus Anexos.

2. OBJETO

2.1. Conforme descrito no Anexo I.

3. PRAZOS, CONDIÇÕES E LOCAL DE ENTREGA DO(S) MATERIAL(IS) OU DA REALIZAÇÃO DO(S) SERVIÇO(S) E VIGÊNCIA DO CONTRATO

3.1. Conforme descrito no Anexo I.

4. CONDIÇÕES DE PAGAMENTO E REAJUSTES

4.1. Conforme descrito no Anexo I.

5. CONDIÇÕES DE RECEBIMENTO DOS MATERIAIS OU SERVIÇOS

5.1. A Contratada ficará obrigada a entregar o(s) material(is) e/ou executar o(s) serviço(s) conforme estabelecido neste Edital e em seus Anexos.

6. CONDIÇÕES DE PARTICIPAÇÃO

6.1. Poderão participar da licitação as interessadas, doravante denominadas Licitantes, que pertencerem ao ramo de atividade pertinente com o objeto desta licitação e que atenderem a todas as exigências deste Edital e de seus Anexos.

6.2. Além das vedações estabelecidas pelo artigo 9º da Lei Federal nº 8.666/93, não será permitida a participação de empresas e/ou pessoas físicas:

6.2.1. Estrangeiras que não funcionem no País;

6.2.2. Reunidas sob a forma de consórcio, qualquer que seja sua forma de constituição;

6.2.3. Sob processo de concordata, falência, concurso de credores, insolvência, recuperação extrajudicial, dissolução ou liquidação;

6.2.3.1. As empresas em recuperação judicial poderão participar, desde que a licitante apresente o correspondente plano de recuperação homologado pelo juízo competente e em pleno vigor.

6.2.4. Suspensas temporariamente para licitar e impedidas de contratar com o Município de Santo André, nos termos do inciso III do artigo 87 da Lei Federal nº 8.666/93 e suas alterações;

6.2.5. Impedidas de licitar e contratar nos termos do artigo 7º da Lei nº 10.520/02;

6.2.6. Impedidas de licitar e contratar nos termos do artigo 10 da Lei nº 9.605/98;

6.2.7. Declaradas inidôneas pelo Poder Público e não reabilitadas por qualquer ente federativo.

7. PROPOSTA COMERCIAL

7.1. Conforme descrito no Anexo IV.

8. DOCUMENTOS DE HABILITAÇÃO

8.1. Conforme descrito no Anexo III.

9. CREDENCIAMENTO, RECEBIMENTO E ABERTURA DOS ENVELOPES DE PROPOSTAS

9.1. A sessão para recebimento dos envelopes das Licitantes será pública e realizada em conformidade com a legislação citada no item 1 deste Edital, suas cláusulas e Anexos. A fase de abertura da licitação observará, seqüencialmente, as etapas estabelecidas a seguir.

9.2. No dia, hora e local estipulados no Anexo I, as Licitantes deverão estar representadas por agentes credenciados, com poderes específicos para formular lances verbais, bem como para a prática de todos os atos inerentes à sessão pública, portando documento pessoal de identificação, documentação comprobatória dos poderes do credenciante, mediante a apresentação dos elementos a que se referem os subitens 9.2.4 e 9.2.5, para credenciamento junto ao Pregoeiro.

9.2.1. As microempresas ou empresas de pequeno porte (ME ou EPP), ora denominadas "pequenas empresas", deverão estar devidamente representadas em todas as fases da sessão pública com amplos poderes para fim do exercício dos direitos previstos na Lei Complementar nº 123/06 e alterações posteriores e na Lei Municipal nº 9.487/13.

9.2.2. Juntamente com o credenciamento as Licitantes deverão entregar a Declaração de Cumprimento dos Requisitos Habilitatórios, objeto do Anexo VI, bem como, se for o caso, declaração de que se encontra enquadrada na condição de pequena empresa nos termos da legislação fiscal e societária, conforme modelo constante no Anexo VII.

9.2.2.1. As pequenas empresas deverão apresentar declaração, conforme modelo indicado no Anexo VII deste Edital.

9.2.3. O documento de credenciamento e os documentos previstos nos subitens 9.2.2 e 9.2.2.1 deverão ser entregues ao Pregoeiro juntamente com a respectiva cédula de identidade ou equivalente, em separado dos envelopes "PROPOSTA COMERCIAL" e "DOCUMENTOS DE HABILITAÇÃO".

9.2.4. O credenciamento será feito por meio de instrumento público de procuração ou instrumento particular, devendo obrigatoriamente apresentar os dados constantes do Anexo V.

9.2.4.1. O documento de credenciamento deverá vir acompanhado de contrato social ou documento equivalente, que comprove os poderes de quem o está constituindo.

9.2.5. Se a Licitante estiver representada por proprietário, sócio, dirigente ou pessoa de condição assemelhada, quaisquer destes deverá apresentar documento comprobatório da sua condição, no qual estejam expressos os seus poderes para exercer direitos e assumir obrigações em nome daquela, também acompanhado de documento pessoal de identificação, estando neste caso dispensado da apresentação do Termo de Credenciamento, objeto do Anexo V.

9.2.6. O não credenciamento do representante o impedirá de se manifestar e responder pela Licitante.

9.2.7. Nenhum interessado poderá representar mais de uma Licitante.

9.2.8. A não apresentação da Declaração de Cumprimento dos Requisitos Habilitatórios não será fator de impedimento à participação da Licitante, desde que, presente o representante credenciado, faça-o, de próprio punho, antes do início dos trabalhos.

9.3. Finalizada a etapa de credenciamento, o Pregoeiro declarará encerrada esta fase e procederá ao recebimento dos envelopes que deverão conter as Propostas Comerciais e os Documentos de Habilitação, em invólucros separados, indevassáveis, e devidamente lacrados, contendo os seguintes dizeres em suas faces externas:

ENVELOPE “A”
EDITAL DE PREGÃO Nº .....
PROPOSTA COMERCIAL
RAZÃO SOCIAL DA LICITANTE E RESPECTIVO CNPJ

ENVELOPE “B”
EDITAL DE PREGÃO Nº .....
DOCUMENTOS DE HABILITAÇÃO
RAZÃO SOCIAL DA LICITANTE E RESPECTIVO CNPJ

9.4. A Proposta Comercial, conforme definida no Anexo IV, preferencialmente deverá ser apresentada em 1 (uma) via, impressa, com escrita numa só das faces de cada folha, sem emendas, nem rasuras, de forma LEGÍVEL, assinada por seu representante legal, na qual deverão constar de forma clara e precisa os elementos e requisitos mencionados no Anexo II.

9.5. Nos preços unitários ou globais, conforme definido no Anexo I, expressos em Reais e com duas casas decimais, deverão estar inclusos, entre outros, tributos, prêmios de seguro, taxas, inclusive de administração, emolumentos, transporte, quaisquer despesas operacionais, todos os encargos trabalhistas, sociais, previdenciários, fiscais e comerciais, despesas e obrigações financeiras de qualquer natureza, frete, carga e descarga, transporte, enfim, todos os componentes de custos, necessários à perfeita execução do objeto deste Edital e de seus Anexos.

9.5.1. Em casos específicos e devidamente descritos no Anexo I do Edital, serão admitidos preços unitários expressos com até três casas decimais, entretanto, o valor total de cada item, bem como o valor final da proposta comercial deverá ser expresso com duas casas decimais. Caso sejam ofertados valores unitários expressos com mais de três casas decimais, estas serão meramente desconsideradas.

9.6. Serão desclassificadas as propostas comerciais que não atenderem as exigências essenciais deste Edital e de seus Anexos, que estejam em desconformidade com o critério indicado no Anexo I, bem como as omissas e as que apresentarem irregularidades ou defeitos capazes de dificultar o julgamento.

9.6.1. Consideram-se exigências essenciais aquelas que não possam ser atendidas, no ato, por simples manifestação de vontade do representante, e aquelas cujo desatendimento, nesse momento, possam representar desrespeito aos princípios da licitação.

9.6.2. Havendo falhas possíveis de serem sanadas, deverá o detentor da proposta ou seu representante credenciado assim fazê-lo, desde que não atrapalhe o andamento dos trabalhos ou atrase o julgamento das propostas.

10. PROCEDIMENTO

10.1. Recebidos os envelopes, serão abertos os de Proposta Comercial. O Pregoeiro, juntamente com a equipe de apoio, procederá à análise da conformidade das propostas com os requisitos estabelecidos neste Edital e em seus Anexos, com exceção do preço, desclassificando as incompatíveis.

10.2. No curso da sessão, das propostas que satisfizerem os requisitos do item anterior, o Pregoeiro classificará para a etapa de lances verbais, o autor da oferta de menor preço, observado o disposto no Anexo I, e aqueles que tenham apresentado propostas em valores sucessivos e superiores em até 10 % (dez por cento), relativamente à de menor preço.

10.2.1. Quando não houver, no mínimo, 3 (três) propostas nas condições definidas no subitem anterior, serão consideradas classificadas, para essa fase competitiva, as melhores propostas subseqüentes, até o máximo de 3 (três).

10.2.2. No caso de empate entre duas ou mais propostas escritas será realizado sorteio para determinação da ordem de oferta de lances.

10.3. A oferta dos lances deverá ser efetuada, de forma sucessiva, em valores distintos, decrescentes e inferiores ao menor valor ofertado, sempre que o Pregoeiro convidar individualmente, de forma seqüencial, o representante para fazê-lo, a partir da proposta de maior preço até o menor.

10.3.1. A definição sobre quais valores deverão incidir os lances, se globais ou unitários, consta do Anexo I.

10.4. A desistência em apresentar lance verbal, quando convocado pelo Pregoeiro, implicará na exclusão da Licitante da fase de lances e na manutenção de seu último preço apresentado, para efeito de ordenação das propostas.

10.5. O encerramento da fase competitiva se dará quando, indagados pelo Pregoeiro, as Licitantes manifestarem seu desinteresse em apresentar novos lances, oportunidade em que serão classificadas as propostas.

10.6. Neste momento, deverá o Pregoeiro verificar se há Licitante na condição de pequena empresa e, em caso positivo, indagar a mesma sobre a intenção do exercício das prerrogativas trazidas pela Lei Complementar nº 123/06 e alterações posteriores e pela Lei Municipal nº 9.487/13.

10.7. Será assegurada às pequenas empresas, como critério de desempate, a preferência de contratação de acordo com o estabelecido no artigo 44 da Lei Complementar nº 123/06 e alterações posteriores, bem como no artigo 27 I da Lei Municipal nº 9.487/13.

10.7.1. Entendem-se por empate, situações em que as propostas apresentadas pelas pequenas empresas sejam iguais ou até 5% (cinco por cento) superiores à melhor proposta classificada nos termos do subitem 10.5.

10.8. Na hipótese de empate, nos termos da Lei Complementar nº 123/06 e alterações posteriores e da Lei Municipal nº 9.487/13, será procedido o seguinte:

10.8.1. A pequena empresa mais bem classificada poderá apresentar proposta comercial com valor inferior àquela considerada vencedora da sessão pública, situação em que será adjudicado em seu favor o objeto licitado.

10.8.1.1. A pequena empresa mais bem classificada será convocada para apresentar a nova proposta verbal no prazo máximo de 5 (cinco) minutos após o encerramento dos lances, sob pena de preclusão, aplicando-se a regra aos demais licitantes que se enquadrarem na hipótese do subitem 10.7.1.

10.9. Não ocorrendo a contratação na forma do item anterior serão convocadas as remanescentes que se enquadrem como pequena empresa na ordem classificatória, para o exercício dos direitos trazidos pela Lei Complementar nº 123/06 e alterações posteriores e pela Lei Municipal nº 9.487/13.

10.10. No caso de equivalência dos valores apresentados pelas pequenas empresas que se encontrem na situação descrita no subitem 10.7.1, será realizado sorteio entre elas para que se identifique aquela que primeiro poderá apresentar a oferta.

10.11. Na hipótese de não contratação nos termos previstos a partir do subitem 10.6, o objeto licitado será adjudicado em favor da proposta originalmente vencedora da sessão pública.

10.11.1. O disposto nos itens anteriores somente se aplicará quando a melhor proposta, superada a fase de lances, não tiver sido apresentada por pequena empresa.

10.12. Nos casos em que os lances incidirem sobre valores globais, para cálculo dos valores unitários finais, será concedido à Licitante vencedora, no decorrer da sessão, a oportunidade de distribuí-los da forma que lhe convier, desde que mantido no valor total o desconto que o sagrou vencedor, formulando nova proposta.

10.12.1. A proposta readequada deverá ser entregue no prazo de até 24 (vinte e quatro) horas, sob pena da aplicação das penalidades previstas nos subitens 16.1 e 16.2 deste Edital.

10.13. Encerrada a etapa competitiva e ordenadas as ofertas, de acordo com o menor preço apresentado, sem prejuízo do disposto nos subitens 10.7 e 10.8, o Pregoeiro verificará a aceitabilidade do melhor preço ofertado, comparando-o com o valor indicado na estimativa de preços e procederá à negociação junto ao particular para obter melhores condições para a Administração.

10.14. Para o caso de não serem ofertados lances verbais, será verificada a conformidade entre a proposta escrita de menor valor e o preço estimado para a contratação, devendo o Pregoeiro negociar junto ao particular melhores condições para a Administração, aplicando os critérios estabelecidos pela Lei Complementar nº 123/06 e alterações posteriores e pela Lei Municipal nº 9.487/13.

10.15. Ultrapassada a fase de lances, sem prejuízo do disposto no subitem 10.6 e aceito o preço final proposto, bem como aprovada a eventual amostra, o Pregoeiro procederá à abertura do envelope "Documentos de Habilitação" da Licitante vencedora, verificando se os documentos apresentados atendem as condições de habilitação fixadas neste Edital e em seus Anexos.

10.16. Caso o preço final não seja aceito ou ocorra a inabilitação da Licitante que tiver apresentado a melhor oferta, o Pregoeiro examinará a oferta subseqüente, sem prejuízo do disposto no subitem 10.6 e, estando esta aprovada, fará análise dos documentos necessários à habilitação da Licitante, na ordem de classificação, e assim sucessivamente, até a apuração de uma proposta que atenda a todos os termos do Edital e de seus Anexos, sendo a respectiva Licitante declarada vencedora, adjudicando-lhe o objeto da sessão pública.

10.16.1. Nessas situações, o Pregoeiro poderá negociar diretamente com a Licitante para que seja obtido o melhor preço.

10.17. As propostas classificadas serão estudadas e julgadas pelo Pregoeiro, a quem caberá a adjudicação do objeto, prosseguindo-se com os demais atos tendentes à homologação pelo(a) Sr(a). Secretário(a) de Assuntos Jurídicos.

10.18. Os envelopes Documentos de Habilitação das Licitantes que tiveram suas propostas comerciais desclassificadas ou que restaram vencidas na fase de lances ficarão retidos até o início da execução contratual.

10.19. Todos os documentos da Licitante vencedora, bem como todas as propostas apresentadas, serão colocados à disposição das presentes para livre exame e rubrica, podendo qualquer Licitante manifestar imediata e motivadamente a intenção de recorrer, conforme os termos do subitem 13.1 deste Edital.

10.20. Se a Licitante vencedora, convocada dentro do prazo de validade de sua proposta, não celebrar o Contrato, quaisquer que sejam os motivos, será convocada outra Licitante, nos termos do subitem 10.16, para efetivar o Contrato e assim sucessivamente, configurando-se neste caso a hipótese descrita no subitem 16.2 e aplicando-se a penalidade ali imposta.

11. JULGAMENTO

11.1. O julgamento das propostas se processará segundo o critério estabelecido no Anexo I, com a observância da melhor oferta, aplicando-se os subitens 10.7 e 10.8, para efeito de classificação.

12. HABILITAÇÃO

12.1. Após o encerramento da fase de lances verbais, com o julgamento das propostas comerciais na forma prescrita neste Edital e em seus Anexos, bem como analisadas eventuais amostras, proceder-se-á à abertura do envelope Documentos de Habilitação, para análise dos documentos da Licitante primeira classificada.

12.2. A Licitante devidamente enquadrada como pequena empresa, em conformidade com a Lei Complementar nº 123/06 e alterações posteriores e com a Lei Municipal nº 9.487/13, deverá apresentar os documentos relativos à regularidade fiscal e trabalhista, ainda que existam pendências, observadas as condições do subitem 9.2.

12.2.1. Será concedido à Licitante vencedora, enquadrada no "caput" deste subitem, quando encerrada a fase de classificação das propostas, o prazo de até 5 (cinco)

dias úteis para a regularização das pendências, prorrogável por uma única vez, por igual período, a critério do Pregoeiro e desde que solicitado, por escrito, pela Licitante.

12.2.2. A não regularização das pendências, no prazo previsto no subitem anterior, implicará em decadência do direito à contratação, sem prejuízo das sanções previstas no artigo 81 da Lei nº 8.666/93, sendo facultado à Administração convocar as Licitantes remanescentes, na ordem de classificação, para a assinatura do contrato ou revogar a licitação.

12.3. Não serão aceitas certidões positivas de débito, exceto quando constar da própria certidão ressalva que autorize a sua aceitação.

12.4. A aceitação dos documentos obtidos via "Internet" ficará condicionada à confirmação de sua autenticidade, também por esse meio, por intermédio do Pregoeiro ou por membro de sua equipe de apoio.

12.5. Para efeito de validade das certidões de regularidade de situação perante a Administração Pública, se outro prazo não constar da Lei ou do próprio documento, será considerado o lapso de 180 (cento e oitenta) dias entre a data de sua expedição e a da abertura da sessão pública.

12.6. Os documentos poderão ser apresentados no original ou por qualquer processo de cópia reprográfica, desde que regularmente autenticada, ou em publicação de órgão da imprensa na forma da Lei.

12.7. No caso de apresentação de documento original, estes serão liberados desde que o envelope de "Documentos de Habilitação" contenha uma cópia, ainda que não autenticada. Nesta hipótese a cópia será autenticada por membro da equipe de apoio do Pregoeiro, à vista do documento original.

12.8. Os documentos exigidos para habilitação, consoante o estabelecido no Anexo III, não poderão em hipótese alguma, ser substituídos por protocolos que configurem o seu requerimento, não podendo, ainda, ser remetidos posteriormente ao prazo fixado para a abertura da sessão pública.

12.9. Será considerada habilitada a Licitante que apresentar os documentos relacionados no Anexo III, sem prejuízo do disposto no subitem 12.2 e subitens deste Edital.

13. FASE RECURSAL

13.1. Declarada a vencedora, as demais Licitantes presentes poderão manifestar imediata e motivadamente a intenção de recorrer, sendo concedido o prazo de 3 (três) dias úteis para apresentação das razões e de igual prazo para as contrarrazões, com imediata intimação de todas as presentes e assegurada também imediata vista dos autos.

13.1.1. O recurso poderá ser feito, na própria sessão, pelo credenciado da Licitante;

13.1.2. A ausência de manifestação e motivação, nos termos do subitem 13.1, importará na decadência do direito de recurso.

13.1.3. O acolhimento de eventual recurso importará na invalidação apenas dos atos insuscetíveis de aproveitamento.

13.1.4. As razões de recurso bem como suas respectivas contrarrazões mencionadas no subitem 13.1 deverão ser protocoladas junto à Praça de Atendimento ao

Munícipe, localizada na Praça IV Centenário nº 01, Térreo I do Prédio da Prefeitura.

14. HOMOLOGAÇÃO

14.1. Decorridas as fases anteriores e procedida a adjudicação do objeto à Licitante vencedora, a decisão será submetida à autoridade devidamente instituída, para homologação.

14.1.1. A homologação do resultado desta licitação não obriga a Administração à aquisição do objeto licitado.

15. CONTRATO OU INSTRUMENTO EQUIVALENTE

15.1. A adjudicatária será expressamente convocada para, no prazo de 5 (cinco) dias úteis da data da convocação, assinar o Contrato ou retirar o instrumento equivalente.

15.2. Responsabiliza-se a Licitante, pelas informações constantes em sua proposta comercial, devendo mantê-las atualizadas junto à Administração.

15.2.1. Havendo a convocação para assinatura do Contrato ou retirada de instrumento equivalente e restando esta frustrada pela inexatidão das informações contidas na proposta comercial ou em razão da desatualização dos dados nela constantes, configurar-se-á a hipótese prevista no subitem 16.2 deste Edital.

15.2.2. Qualquer meio de comunicação escrito (fax, e-mail, correspondência, etc.), é mecanismo hábil para a convocação da adjudicatária.

15.3. O prazo para assinatura do Contrato poderá ser prorrogado por uma vez, desde que solicitado por escrito, antes do término do prazo previsto no subitem 15.1, sob alegação de motivo justo que poderá ou não ser aceito pela Administração.

15.4. Na hipótese do não atendimento à convocação a que se refere o subitem 15.1 ou havendo recusa em fazê-lo, fica facultado à Administração, desde que haja conveniência, proceder à adjudicação para as demais Licitantes, observada a ordem de classificação das propostas.

15.5. A Contratada ficará obrigada a aceitar, nas mesmas condições contratuais e nos preços unitários finais, já aplicado o desconto auferido nos lances, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) dos valores contratados.

15.6. A Contratada ficará responsável pelo pagamento integral dos encargos fiscais, comerciais, trabalhistas, previdenciários e outros que decorrerem dos compromissos assumidos com a Prefeitura, não se obrigando a mesma a fazer restituições ou reembolsos de valores principais e/ou acessórios despendidos com esses pagamentos.

15.7. As Licitantes obrigam-se a manter, durante toda a execução contratual, em compatibilidade com as obrigações por elas assumidas, todas as condições exigidas nos aspectos jurídico e de qualificação técnica, econômica e financeira, bem como de regularidade perante o Fisco e a Justiça do Trabalho, quando das respectivas habilitações. A regularidade dos encargos sociais será comprovada mediante a apresentação da “Certidão Negativa, ou Positiva com efeitos de Negativa, de Débitos relativos a Tributos Federais e à Dívida Ativa da União”, expedida pela Secretaria da Receita Federal do Brasil, nos termos da Portaria Conjunta RFB/PGFN nº 1.751/14, do Certificado de Regularidade do FGTS – CRF expedida pela Caixa Econômica Federal e da Certidão Negativa/Positiva com efeito de Negativa de Débitos Trabalhistas perante a Justiça do Trabalho, na época da apresentação das notas fiscais e pagamento.

15.8. A inexecução parcial ou total do contrato poderá ensejar sua rescisão, nos casos previstos no art. 78, no modo previsto pelo art. 79, com as conseqüências previstas no art. 80, todos da Lei 8.666/93 e alterações posteriores.

16. SANÇÕES ADMINISTRATIVAS

16.1. São aplicáveis as sanções previstas na Lei Federal nº 10.520/02, e subsidiariamente no capítulo IV da Lei Federal nº 8.666/93, com as alterações introduzidas pela Lei Federal nº 8.883/94, e demais normas pertinentes, a seguir indicadas:

16.1.1. Advertência;

16.1.2. Suspensão temporária de participar em licitação e impedimento de contratar com a Administração, nos termos indicados no subitem 16.12.1;

16.1.3. Declaração de inidoneidade para licitar ou contratar com a Administração Pública;

16.1.4. Multa.

16.2. A multa pela recusa da adjudicatária em assinar o Contrato ou em retirar o instrumento equivalente dentro do prazo estabelecido neste Edital será de 10% (dez por cento) do valor da proposta comercial, sem prejuízo da aplicação da pena de suspensão temporária do direito de licitar e contratar com a PMSA, pelo prazo de até 5 (cinco) anos.

16.3. Multa por atraso: 1% (um por cento) por dia sobre o valor da parcela em atraso, até o limite de 10% (dez por cento), podendo a PMSA a partir do 10º dia considerar rescindido o Contrato, sem prejuízo das demais sanções cabíveis.

16.3.1. O prazo para pagamento das multas moratórias será de 3 (três) dias úteis a contar da intimação da Contratada. A critério da Administração e sendo possível, o valor das referidas multas será descontado dos pagamentos eventualmente devidos pela PMSA, garantida a ampla defesa nos termos da Lei.

16.4. Multa por inexecução parcial do Contrato: 10% (dez por cento) sobre o valor da parcela inexecutada.

16.5. Multa por inexecução total do Contrato: 10% (dez por cento) sobre o valor total do Contrato.

16.6. Multa de 10% (dez por cento), por descumprimento de quaisquer das obrigações decorrentes do ajuste, que não estejam previstas nos subitens acima, a qual incidirá sobre o valor total do Contrato.

16.7. Perda da garantia oferecida se houver, em caso de culpa pela rescisão contratual.

16.8. As penalidades são independentes e a aplicação de uma não exclui a das outras, quando cabíveis.

16.9. Constatada a inexecução contratual ou a hipótese do subitem 16.2, será a Contratada intimada da intenção da PMSA quanto à aplicação da penalidade, concedendo-se prazo para interposição de defesa prévia, nos termos do art. 87, §2º e §3º da Lei 8.666/93.

16.10. Não sendo apresentada a defesa prévia pela Contratada ou havendo o indeferimento da mesma quando interposta, a PMSA providenciará a notificação da Contratada quanto à aplicação da penalidade, abrindo-se prazo para interposição de recurso administrativo, nos termos do artigo 109, I, “f” da Lei nº 8.666/93.

16.11. Decorridas as fases anteriores, o prazo para pagamento das multas será de 3 (três) dias úteis a contar da intimação da Contratada. A critério da Administração e sendo possível, o valor devido será descontado da garantia prestada ou sendo esta insuficiente, será descontado dos pagamentos eventualmente devidos pela Administração. Não havendo prestação de garantia, o valor das multas será diretamente descontado do crédito que porventura haja.

16.11.1. Não havendo tais possibilidades, o valor será inscrito em dívida ativa, sujeitando a devedora a processo executivo.

16.12. Sem prejuízo da aplicação de outras penalidades cabíveis, a ocorrência das hipóteses a seguir listadas, acarretará a aplicação da penalidade especificada.

16.12.1. A empresa que, convocada dentro do prazo de validade de sua proposta, não celebrar o Contrato ou deixar de retirar o instrumento equivalente, deixar de entregar documentação exigida para a sessão pública ou apresentar documentação falsa, ensejar o retardamento da execução de seu objeto, não mantiver a proposta, falhar ou fraudar na execução do contrato, comportar-se de modo inidôneo ou cometer fraude fiscal, ficará impedida de licitar e contratar com a Administração Municipal e será descredenciado do Cadastro de Fornecedores desta PMSA, pelo prazo de até 5 (cinco) anos, sem prejuízo das multas previstas em Edital, no Contrato e nas demais cominações legais.

17. RECURSOS ORÇAMENTÁRIOS

17.1. As despesas com a execução do objeto descrito no Anexo I deste Edital onerarão a(s) dotação(ões) consignada(s) no orçamento deste Exercício, e em orçamento(s) futuro(s), quando necessário.

18. DISPOSIÇÕES GERAIS

18.1. Os pedidos de impugnação ao Edital deverão ser encaminhados à Gerência de Compras e Licitações correspondente à COPEL – I dirigidos à autoridade superior (Sr. Secretário de Assuntos Jurídicos), contendo a indicação do número do respectivo Edital, a ser protocolizado junto à Praça de Atendimento, no Térreo I do Prédio da PMSA, sito na Praça IV Centenário nº 1, Centro, neste Município, nos seguintes prazos: a) até 5 (cinco) dias úteis antes da data fixada para a abertura dos envelopes, em sendo formulada por qualquer cidadão; b) até 2 (dois) dias úteis antes da data fixada para a abertura dos envelopes, em sendo formulada pela Licitante. Deverá constar no pedido, endereço, telefone e e-mail para contato.

18.2. Quaisquer esclarecimentos ou informações relativas a esta licitação serão prestadas, mediante solicitação escrita formulada, no mínimo 2 (dois) dias úteis antes da data prevista para entrega dos envelopes, de segunda à sexta-feira, no horário das 8:00 às 17:00 horas, em local descrito no Anexo I deste Edital. Não serão aceitos pedidos de informações ou questionamentos verbais, admitindo-se no caso, as formuladas através de e-mail, cujo endereço está descrito no Anexo I deste Edital. Todos os esclarecimentos ou informações referidas neste subitem deverão ser encaminhados à Gerência de Compras e Licitações correspondente à COPEL - I, contendo o respectivo número do Edital. Deverá constar no pedido, endereço, telefone e e-mail para contato.

18.3. É facultado ao Pregoeiro ou à Autoridade Superior, em qualquer fase da licitação, a promoção de diligência destinada a esclarecer ou complementar a instrução do processo, vedada a inclusão posterior de documento ou informação que deveria constar no ato da sessão pública, exceto no tocante ao disposto no subitem 10.12.1 deste Edital.

PREFEITURA MUNICIPAL DE SANTO ANDRÉ
SECRETARIA DE ASSUNTOS JURÍDICOS
DEPARTAMENTO DE LICITAÇÕES

18.4. Fica assegurado à PMSA o direito de, no interesse da Administração, invalidar ou revogar, a qualquer tempo, no todo ou em parte, a presente licitação, dando ciência às interessadas, na forma da legislação vigente.

18.5. As Licitantes assumem todos os custos de preparação e apresentação de suas propostas e a PMSA não será, em nenhum caso, responsável por esses custos, independentemente da condução ou do resultado do processo licitatório.

18.6. As Licitantes são responsáveis pela fidelidade e legitimidade das informações e dos documentos apresentados em qualquer fase da licitação.

18.7. A apresentação da proposta pela Licitante implica na aceitação tácita de todos os termos do presente Edital e de seus Anexos, respeitado o disposto no artigo 41, § 2º da Lei Federal nº 8.666/93.

18.8. Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a realização da sessão pública na data marcada, a mesma será automaticamente transferida para o primeiro dia útil subseqüente, no mesmo horário e local anteriormente estabelecidos, desde que não haja decisão e comunicação do Pregoeiro em contrário.

18.9. Na contagem dos prazos estabelecidos neste Edital e em seus Anexos, excluir-se-á o dia do início e incluirá o do vencimento. Só se iniciam e vencem os prazos em dias de expediente na PMSA.

18.10. As partes elegerão o Foro da Comarca de Santo André para qualquer procedimento administrativo ou judicial decorrente do processamento desta licitação e do descumprimento do Contrato dela originado.

18.11. Este Edital Padrão de Pregão Presencial da PREFEITURA MUNICIPAL DE SANTO ANDRÉ (PMSA) contém 11 (onze) folhas, numeradas sequencialmente de 1 (um) a 11 (onze), escritas no anverso, com as CONDIÇÕES GERAIS do procedimento licitatório que, em conjunto com os elementos específicos, contidos nos Anexos que o integram, regerão a licitação e a contratação especificada.

18.12. Constituem parte integrante do presente Edital, os seguintes Anexos que conterão a correspondente numeração própria:

18.12.1.	Anexo I	-	Descrição do Objeto e demais Condições
18.12.2.	Anexo II	-	Descrição dos Materiais / Serviços
18.12.3.	Anexo III	-	Descrição dos Documentos de Habilitação
18.12.4.	Anexo IV	-	Modelo de Proposta Comercial
18.12.5.	Anexo V	-	Modelo do Termo de Credenciamento
19.12.6.	Anexo VI	-	Modelo de Declaração de Cumprimento de Requisitos Habilitatórios
18.12.7.	Anexo VII	-	Modelo de Declaração de Pequena Empresa
18.12.8.	Anexo VIII	-	Modelo de Declaração do Licitante
18.12.9.	Anexo IX	-	Minuta de Contrato
18.12.10.	Anexo X	-	Termo de Ciência e de Notificação

Prefeitura Municipal de Santo André, 29 de novembro de 2.019

RENATA GRACIO DE OLIVEIRA
Pregoeiro(a) Oficial
Departamento de Licitações
SECRETARIA DE ASSUNTOS JURÍDICOS

ALAIR MAGNI
Diretor
Departamento de Licitações
SECRETARIA DE ASSUNTOS JURÍDICOS

ANEXO I
DESCRIÇÃO DO OBJETO E DEMAIS CONDIÇÕES

1. DADOS DO PREGÃO PRESENCIAL

1.1. Processo Administrativo nº: **31833/2018**

1.2. Edital nº: **068/2019 (reprogramado)**

1.3. Modalidade: **Pregão Presencial**

1.4. Data da Abertura: **12/12/2019**

1.5. Horário da Abertura: **09h30min**

1.6. Local: **Prédio da Prefeitura Municipal de Santo André (PMSA), 13º andar, sito na Praça IV Centenário nº 01, Centro, neste Município – Sala de Licitações - nº 08.**

1.7. Telefone(s): **(11) 4433-0300 / 4433-0311 / 4433-0319**

1.8. E-mails: **rgoliveira@santoandre.sp.gov.br ecompras@santoandre.sp.gov.br; jmanssur@santoandre.sp.gov.br;**

1.9. Este Pregão Presencial atende à programação das seguintes Secretarias: Secretaria de Saúde, Secretaria de Inovação e Administração e Secretaria de Educação.

2. OBJETO

2.1. Contratação de empresa para o fornecimento de solução de antivírus com licenças do produto, implementação, treinamento, prestação de serviços de manutenção e suporte técnico para toda solução ofertada, conforme descrição e quantidades do Anexo II.

3. RECURSOS ORÇAMENTÁRIOS

3.1. As despesas com a execução do objeto deste Edital estão consignadas no orçamento de 2019 da PMSA, nas dotações orçamentárias abaixo descritas e nas dotações próprias para o exercício subsequente, quando for o caso.

3.2. **Dotações – Tesouro Municipal:**

- 40.70.3.3.90.40.10.122.0034.2.096.01;
- 60.10.3.3.90.40.12.365.0061.2.176.01;
- 34.30.3.3.90.40.04.122.0022.2.067.01.

4. PRAZOS, CONDIÇÕES E LOCAL DE ENTREGA DO(S) MATERIAL(IS) OU DA REALIZAÇÃO DO(S) SERVIÇO(S) E VIGÊNCIA DO CONTRATO

4.1. O contrato terá vigência de **36 (trinta e seis) meses**.

4.2. O objeto de que trata o subitem 2.1 retro deverá ser entregue e implementado no prazo de **30 (trinta) dias corridos**, contados a partir do dia útil seguinte ao da assinatura do contrato.

4.3. Todos os serviços deverão ser prestados por técnicos especializados devidamente credenciados, no local abaixo indicado, correndo por conta exclusiva da contratada todas as despesas decorrentes de transportes até o local indicado:

4.3.1. Local: Paço Municipal, Praça IV Centenário, nº 01 – Centro – Santo André no Prédio do Executivo – 2º Andar.

ANEXO I
DESCRIÇÃO DO OBJETO E DEMAIS CONDIÇÕES

4.4. O objeto de que trata o subitem 2.1 retro deverá ser entregue e/ou executado de acordo com as especificações constantes do Edital e de seus Anexos, sob pena de incorrer a Contratada nas sanções previstas na forma da Lei.

4.5. Todos os produtos ofertados e entregues e suas respectivas embalagens deverão estar de acordo com a legislação vigente e pertinente.

4.6. A Contratada será responsável pelos encargos trabalhistas, previdenciários, fiscais, comerciais e despesas resultantes da execução do contrato. A inadimplência do contratado com referência aos encargos trabalhistas, fiscais e comerciais não transferem à Administração a responsabilidade por seu pagamento, nem poderá onerar o objeto do contrato.

5. CONDIÇÕES DE PAGAMENTO E REAJUSTES

5.1. Os pagamentos serão efetuados através da Tesouraria desta Prefeitura no 30º (trigésimo) dia após a quinzena da entrega/prestação dos serviços.

5.1.1. Considerando a possibilidade de que os pagamentos sejam efetuados através de depósito bancário, a Licitante deverá indicar, em sua Proposta Comercial, sua razão social e respectivo número do CNPJ(MF), o banco (nome e número), a agência (nome e número) e o número da conta corrente.

5.1.2. O não pagamento da fatura, apresentada nas condições previstas, sujeitará a Contratante à atualização financeira dos valores a serem pagos, desde a data final do período do adimplemento de cada parcela até a data do efetivo pagamento.

5.2. Não incidirá qualquer conduta de reajuste de preços na presente hipótese

6. CONDIÇÕES ESPECÍFICAS

6.1. As propostas deverão, preferencialmente, ser elaboradas de acordo com o modelo apresentado no Anexo IV, devendo, em qualquer forma de apresentação, indicar todos os quesitos constantes daquele modelo.

6.2. As propostas deverão ter validade mínima de 60 (sessenta) dias, devendo-se considerar este mesmo prazo no caso de omissão de validade.

6.3. Só será admitida a oferta de um único valor para cada produto, bem como a indicação de uma única marca para o mesmo. A empresa que ofertar mais de um valor, produto ou marca para um determinado item será desclassificada no mesmo.

6.4. No preço, em Real com duas casas decimais, deverão estar inclusos, entre outros, tributos, prêmios de seguro, taxas, inclusive de administração, emolumentos, transporte, quaisquer despesas operacionais, todos encargos trabalhistas, sociais, previdenciários, fiscais e comerciais, despesas e obrigações financeiras de qualquer natureza; frete, carga e descarga, transporte, enfim, todos os componentes de custo dos serviços, necessários à perfeita execução do objeto deste edital.

6.5. A critério do Pregoeiro e/ou da Administração poderão ser convocados outros funcionários desta, para emissão de pareceres técnicos.

ANEXO I
DESCRIÇÃO DO OBJETO E DEMAIS CONDIÇÕES

7. ETAPA DE LANCES

7.1. Os lances efetuados na sessão pública deverão incidir sobre o **preço global.**

8. JULGAMENTO

8.1. O critério de julgamento adotado será o de **menor preço global.**

9. PREGOEIRO E EQUIPE DE APOIO

9.1. É designado(a) Pregoeiro(a) Oficial para esta sessão pública a Sra. **Gisele Aparecida de Marco**, ou o Sr. **Rinaldo Pereira da Silva de Oliveira**, ou o Sr. **Luiz Ignácio**, ou a Sra. **Alessandra Cristine Angeli Pincerato**, ou a Sra. **Karina Tathiane de Oliveira Chimirra,** ou a Sra. **Juliana Manssur**, ou a Sra. **Renata Gracio de Oliveira**, ou o Sr. **Anderson Augusto Bogoni** ou a Sra. **Luci Carlota Daniel Gomes**, todos(as) nomeados(as) através da Portaria nº 412.03.2019. Como equipe de apoio estarão atuando os membros da COPEL I e/ou COPEL II bem como, os demais servidores do Departamento de Licitações, quando necessário.

ANEXO II
DESCRIÇÃO DOS MATERIAIS / SERVIÇOS

1. FUNCIONALIDADES DA SOLUÇÃO E NÚMERO DE LICENÇAS

1.1. A solução a ser contratada deverá possuir os itens descritos abaixo, juntamente com a quantidade de licenças indicadas, sendo que todos os módulos devem ser fornecidos pelo mesmo fabricante.

Item	Quantidade de Licenças (unidade)	Descrição
01	53	Solução de Segurança para Servidores Virtuais – Software Gerenciamento, licenciamento, Implantação e Garantia Técnica de 36 meses.
02	3.500	Solução de Proteção para Endpoints, Implantação e Garantia Técnica de 36 meses.
03	2.500	Solução de Proteção Anti-Sapm, Anti-Spam para Exchange, Implantação e Garantia Técnica de 36 meses.
04	3	Treinamento

2. INSTALAÇÃO, CONFIGURAÇÃO E ACOMPANHAMENTO OPERACIONAL

2.1. Caso a solução a ser fornecida, seja diferente do software de antivírus atualmente instalado na PREFEITURA MUNICIPAL DE SANTO ANDRÉ, a contratada deverá providenciar a desinstalação automática de todas as cópias instaladas do software em estações e servidores e a instalação do novo software de antivírus em um único processo;

2.2. A instalação deverá ser realizada por técnicos qualificados e certificados pelo fabricante para a solução ofertada;

2.3. Caso a solução seja a mesma já existente, a mesma deve ser atualizada para a última versão disponível e todas as configurações revisadas, com as devidas correções ou melhorias implementadas;

2.4. Deverão ser instalados e configurados:

2.4.1. Console de gerenciamento da solução ofertada;
2.4.2. Software de antivírus nas estações de trabalho;
2.4.3. Software de antivírus nos servidores virtuais;
2.4.4. Software de Proteção Anti-Spam, Anti-Spam para Exchange;
2.4.5. Tasks para verificação e geração de relatórios de vulnerabilidades de todo o parque computacional;
2.4.6. Relatórios que serão enviados por e-mail de forma automática pela console, para os responsáveis na PREFEITURA MUNICIPAL DE SANTO ANDRÉ;

ANEXO II
DESCRIÇÃO DOS MATERIAIS / SERVIÇOS

2.5. Independentemente de a solução ofertada ser a de corrente uso na PREFEITURA MUNICIPAL DE SANTO ANDRÉ, deverá ser fornecido acompanhamento operacional de 01 (um) técnico on-site por no mínimo 10 (dez) dias. Este acompanhamento operacional deverá ser realizado no prédio executivo da PREFEITURA MUNICIPAL DE SANTO ANDRÉ, sito a Praça IV Centenário nº 01 – 2º andar – Departamento de Tecnologia e Inovação. Este acompanhamento deve ser feito por técnico qualificado e certificado pelo fabricante da solução ofertada;

2.5.1. Deverão ser executadas as seguintes tarefas em relação a este acompanhamento:
2.5.2. Resolução de dúvidas sobre o produto;
2.5.3. Discussão de melhorias na configuração;
2.5.4. Resolução de problemas;

3. DA SOLUÇÃO DE SEGURANÇA PARA SERVIDORES VIRTUAIS

3.1. Características Gerais

3.1.1. Software de segurança para ambientes virtuais devem incluir:

3.1.1.1. Software antivírus sem agente para ambientes virtuais;
3.1.1.2. Software antivírus baseado em agente para ambientes virtuais;
3.1.1.3. Gerenciamento, monitoramento e atualização de software e vacinas centralizados;
3.1.1.4. Capacidade de atualizar definições de vírus e padrões de ataques;
3.1.1.5. Documentação do administrador;

3.1.2. Compatibilidade com a rede a ser protegida;

3.1.3. Solução deve estar de acordo com os requisitos do Regulamento Geral sobre a Proteção de Dados (GDPR) para a proteção de ambientes virtuais;

3.1.4. Solução deve possuir proteção para virtualização privada e pública (AWS e Azure);

3.1.5. Solução deve possuir console de gerenciamento única para virtualização privada e pública;

3.2. Requerimentos para antivírus em ambientes virtualizados baseado em agente (conector);

3.3. Deverá ser instalado em uma infraestrutura virtualizada, devendo suportar os seguintes hypervisors e sistemas:

ANEXO II
DESCRIÇÃO DOS MATERIAIS / SERVIÇOS

3.3.1. Microsoft Windows Server 2016 Hyper-V;
3.3.2. Microsoft Windows Server 2012 R2 Hyper-V;
3.3.3. Citrix XenServer 7;
3.3.4. Citrix XenServer 7.1 LTSR;
3.3.5. VMware ESXi 6.7;
3.3.6. VMware ESXi 6.5;
3.3.7. VMware ESXi 6.0;
3.3.8. VMware ESXi 5.5;
3.3.9. KVM (Kernel-based Virtual Machine) com um dos seguintes sistemas operacionais:
3.3.10. Ubuntu Server 16.04 LTS;
3.3.11. Ubuntu Server 14.04 LTS;
3.3.12. Red Hat Enterprise Linux Server 7, patch 4;
3.3.13. CentOS 7.4;
3.3.14. Acrópolis;

3.4. O Antivírus baseado em agente deve prover proteção para as máquinas virtuais no Vmware hypervisor nos seguintes sistemas operacionais:

3.4.1. Windows 7 Professional / Enterprise Service Pack 1 (32 / 64-bit);
3.4.2. Windows 8.1 Update 1 Professional / Enterprise (32 / 64-bit);
3.4.3. Windows 10 Pro / Enterprise / Enterprise LTSB / RS1 / RS2 / RS3 / RS4 (32 / 64-bit);
3.4.4. Windows Server 2008 R2 Service Pack 1 (64-bit);
3.4.5. Windows Server 2012 (64-bit);
3.4.6. Windows Server 2012 R2 (64-bit);
3.4.7. Windows Server 2016 (64-bit);
3.4.8. Debian GNU / Linux 8.9 (32 / 64-bit);
3.4.9. Debian GNU / Linux 9.1 (64-bit);
3.4.10. Ubuntu Server 16.04 LTS (32 / 64-bit);
3.4.11. Ubuntu Server 18.04 LTS (64-bit);
3.4.12. CentOS 6.9 (64-bit);
3.4.13. CentOS 7.4 (64-bit);
3.4.14. Red Hat Enterprise Linux Server 6.9 (64-bit);
3.4.15. Red Hat Enterprise Linux Server 7.4 (64-bit);
3.4.16. SUSE Linux Enterprise Server 12 Service Pack 1 (64-bit);

3.5. A Suite VMware tools deve ser instalada para prover integração entre o Hypervisor, máquinas virtuais e o conector;
3.6. O antivírus deve prover as seguintes funcionalidades:

3.6.1. Antivírus e monitoramento residente;
3.6.2. Proteção contra rootkits e auto dialers a sites pagos;
3.6.3. Verificação por heurística para detectar e bloquear malwares desconhecidos;
3.6.4. Transferir a verificação de malware e as tarefas intensivas para uma única máquina virtual responsável pela proteção;
3.6.5. Garantir a continuidade da proteção de arquivos durante pequenas indisponibilidades na máquina de proteção logando todas as operações de arquivos nas máquinas protegidas durante o período de indisponibilidade, e faz a verificação automática de todas alterações após a restauração do acesso;
3.6.6. Proteção baseada em nuvem contra ameaças novas, permitindo a aplicação acessar recursos especializados da fabricante para obter vereditos durante a verificação em tempo real ou agendada;
3.6.7. Deve atender HIPPA e SOX;
3.6.8. Proteção de e-mail contra malwares verificando tráfego de entrada e saída nos protocolos

ANEXO II
DESCRIÇÃO DOS MATERIAIS / SERVIÇOS

IMAP, SMTP, POP3, MAPI e NNTP independente do cliente de e-mail;

3.6.9. Proteção de tráfego Web: verificação de objetos enviados para os computadores dos usuários via HTTP e FTP, com a possibilidade de adicionar sites confiáveis;

3.6.10. Bloqueia banners e pop-ups nas páginas web;

3.6.11. Capacidade de detectar e bloquear sites de phishing;

3.6.12. Proteção contra ameaças não conhecidas baseadas no comportamento;

3.6.13. Capacidade de determinar comportamento anômalo de uma aplicação analisando a sequência de execução. Capacidade de reverter operações de malware durante o tratamento do arquivo;

3.6.14. Capacidade de restringir o privilégio de programas executáveis tal como escrita no registro ou acesso a arquivos e pastas. Detecção automática de nível de detecção baseado na reputação do programa;

3.6.15. O Firewall deve permitir a criação de regras para pacotes de rede em protocolos específicos (TCP, UDP) e portas;

3.6.16. Permitir a criação de regras de rede para programas específicos;

3.6.17. Proteção contra-ataques de hackers utilizando o firewall com IDS/IPS e regras de atividade de rede para as aplicações mais conhecidas;

3.6.18. Criação de regras especiais para bloquear a instalação e/ou execução de uma aplicação. Deve ter a capacidade de controlar a aplicação utilizando o caminho, metadado, MD5, checksum, e categorias predefinidas de aplicações providenciadas pelo fabricante;

3.6.19. Permitir a verificação em máquinas Linux;

3.6.20. Deve ser capaz de usar o “Microsoft System Center Virtual Machine Manager” (SCVMM) para fazer deploy dos appliances virtuais;

3.6.21. Os virtuais appliances responsáveis pela verificação devem ser baseados em Linux;

3.6.22. Deve ser capaz de apresentar uma lista de máquinas virtuais que estão sob proteção de cada virtual appliance seguro;

3.6.23. Capacidade de desativar a interface local na inicialização do sistema para diminuir consumo de memória;

3.6.24. Permitir selecionar a forma de conexão ao appliance virtual de três formas diferentes:

3.6.25. Utilizando Multicast;

3.6.26. Selecionando Servidor de integração;

3.6.27. Utilizando uma lista de appliances virtuais;

3.6.28. Deve ser capaz de verificar vírus, worms, trojans, toolkits, adware, auto-dialers e outros tipos de ameaças em máquinas Linux;

3.6.29. Deve ser capaz de criar exclusões em máquinas Linux por nome ou pasta;

3.6.30. Capacidade de verificar arquivos por formato ou extensão em máquinas Linux;

3.6.31. Permitir configurar limite de tempo de verificação em um arquivo tanto para máquinas Linux como Windows;

3.6.32. Permitir alterar o modo de scan para no mínimo três opções diferentes:

- **3.6.32.1.** Verificação automática;
- **3.6.32.2.** Verificar os arquivos no acesso ou na modificação;
- **3.6.32.3.** Somente no acesso;

3.6.33. Monitorar as atividades de I/O do usuário na utilização de dispositivos externos pelo tipo de dispositivo e/ou BUS usado incluindo a capacidade de criar uma lista de dispositivos confiáveis através do ID;

3.6.34. Capacidade de garantir privilégios na utilização de dispositivos externos para usuários específicos do AD;

3.6.35. Monitorar as atividades do usuário na internet incluindo o bloqueio ou a permissão de acesso a certos recursos bem como a capacidade de bloquear certos tipos de informação (audio, video,etc);

3.6.36. Capacidade de controlar acesso na internet por horário e por usuário do AD;

ANEXO II
DESCRIÇÃO DOS MATERIAIS / SERVIÇOS

3.6.38. Atualizações centralizadas permitindo que parte do banco de dados de definições seja armazenado na máquina de proteção (SVM);
3.6.39. Habilidade de executar tarefas de detecção de vulnerabilidades em aplicações instaladas nos computadores incluindo opção de submeter um relatório de qualquer vulnerabilidade encontrada;
3.6.40. Integração com o Windows Update para instalar patches de acordo com as vulnerabilidades encontradas;
3.6.41. Capacidade de instalar e distribuir remotamente componentes do antivirus em todas as máquinas protegidas sem utilização de ferramentas de terceiros;
3.6.42. Armazenar as informações de arquivos verificados para evitar um novo scan sobre o arquivo e aumentar consumo de recursos;
3.6.43. Bloquear, neutralizar e remover os malwares com a opção de notificar os administradores;
3.6.44. Console de gerenciamento única para todos os componentes de proteção;
3.6.45. Console de gerenciamento única tanto para ambientes físicos como virtuais;
3.6.46. Console única para administração de máquinas virtuais Linux e Windows;
3.6.47. Provê informações detalhadas sobre os eventos e execução de tarefas;
3.6.48. Capacidade de aplicar configurações de segurança diferentes para cada grupo de máquinas virtuais;
3.6.49. Salvar o backup dos arquivos deletados;
3.6.50. Suporta as seguintes tecnologias Vmware: vMotion, Distributed resource Scheduler;
3.6.51. Suporta as seguintes tecnologias Citrix: Virtual User Drive, Citrix Receiver, Multi-stream ICA, XenMotion Live Migration, Automated VM protection and recovery, Dynamic memory control;
3.6.52. Suportar as seguintes tecnologias Hyper-V: Live migration, Cluster shared volumes, Dynamic memory, Live backup;
3.6.53. Suportar rollback do banco de dados de definições;
3.6.54. Suportar o esquema de licença de acordo com o número de máquinas virtuais protegidas e de acordo com o número de hardware CPU cores;

3.7. Requerimentos para administração centralizada, monitoramento e update do software para ambientes virtualizados:

3.7.1. A administração centralizada, monitoramento e atualização de softwares deve funcionar em computadores executando os seguintes sistemas operacionais:

3.7.1.1. Microsoft Windows 7 Todas as edições (32/64 bits);
3.7.1.2. Microsoft Windows 8 Pro/Enterprise 32/64 bits;
3.7.1.3. Microsoft Windows 8.1 Pro/Enterprise 32/64 bits;
3.7.1.4. Microsoft Windows 10 Education RS1;
3.7.1.5. Microsoft Windows 10 Education 32/64 bits;
3.7.1.6. Microsoft Windows 10 Enterprise RS1 e Professional RS1 32/64 bits;
3.7.1.7. Microsoft Windows 10 Enterprise e Professional 32/64 bits;
3.7.1.8. Microsoft Windows Small Business Server 2008 Standard x64;
3.7.1.9. Microsoft Windows Small Business Server 2008 Premium x64;
3.7.1.10. Microsoft Windows Small Business Server 2011 Essential, Premium e Standard;
3.7.1.11. Microsoft Windows Server 2008 Todas edições 32/64 bits;
3.7.1.12. Microsoft Windows Server 2008 R2 Todas edições 32/64 bits;
3.7.1.13. Microsoft Windows Server 2012 Todas edições 32/64 bits;
3.7.1.14. Microsoft Windows Server 2012 R2 Todas edições 32/64 bits;
3.7.1.15. Microsoft Windows Server 2016 x64Banco de dados Suportados pela console de administração centralizada:
3.7.1.16. Microsoft SQL Server Express 2008;
3.7.1.17. Microsoft SQL Server Express 2008 R2;
3.7.1.18. Microsoft SQL Server Express 2008 R2 Service Pack 2;
3.7.1.19. Microsoft SQL Server 2005;
3.7.1.20. Microsoft SQL Server 2008;
3.7.1.21. Microsoft SQL Server 2008 R2;

ANEXO II
DESCRIÇÃO DOS MATERIAIS / SERVIÇOS

3.7.1.22. Microsoft SQL Server 2012;
3.7.1.23. Microsoft SQL Server 2014 Todas as edições x64
3.7.1.24. MySQL Enterprise versions 5.0.67, 5.0.77, 5.0.85, 5.087 Service Pack 1, 5.091;
3.7.1.25. MySQL Enterprise versions 5.0.60 Service Pack 1, 5.0.70, 5.0.82 Service Pack 1, 5.0.90;

3.7.2. A solução deverá ter a capacidade de:

3.7.2.1. Controlar e gerenciar a segurança de múltiplas plataformas e sistemas operacionais a partir de um console único e centralizado do próprio fabricante;
3.7.2.2. Reconhecer e bloquear endereços IP que estejam realizando Network Scan, Port Scan, TCP Null Scan, TCP FYNSYN Scan, TCP Xmas Scan e Computer OS FIngerprint por até 30 minutos;
3.7.2.3. Integração com softwares SIEMs para ser possível o envio de logs para as referidas soluções;
3.7.2.4. Enviar logs para SYSLOGS e enviar eventos da console via SNMP;
3.7.2.5. Gerar pacote de autodiagnostico para coleta de arquivos relevantes ao suporte do produto;
3.7.2.6. Categorizar, por meio de etiquetas, ocorrências de eventos para facilitar gerenciamento, relatórios e visualização;
3.7.2.7. Classificar eventos para que facilitar identificação e visualização de eventos críticos em servidores críticos;
3.7.2.8. Visualização de eventos pela categorização por meio de etiquetas e a possibilidade de escolha das etiquetas a serem visualizadas;
3.7.2.9. Realizar o rastreamento portas abertas, identificando possíveis serviços ativos e escutando;
3.7.2.10. Baixar as assinaturas na console de gerenciamento, mas não distribuí-las aos clientes;
3.7.2.11. Permitir que agentes de atualização espalhados pelo ambiente possam distribuir patterns e novos componentes;
3.7.2.12. Criação de múltiplos perfis de segurança, que serão vinculados aos diferentes tipos de servidores do ambiente;
3.7.2.13. Agendar e automatizar o processo de atualizações de assinaturas, permitindo inclusive que as mesmas ocorram de hora em hora;
3.7.2.14. Informar, no gerenciamento de licenças, a quantidade contratada e a quantidade em utilização pelos clientes;

3.7.3. Deverão ser implementadas as funcionalidades:

3.7.3.1. De Antimalware, Controle de Acesso a Sites Maliciosos, Firewall, IDS/IPS, Controle de Aplicações, Proteção de aplicações Web, Inspeção de Logs nos sistemas operacionais Windows através de um único agente;

3.7.4. A solução deverá possuir:

3.7.4.1. Comunicação criptografada com os agentes;
3.7.4.2. Dashboards customizáveis pelo administrador para monitoramento, devendo a personalização ser realizada pelas variáveis “quantidade” e “período”;
3.7.4.3. Mecanismos de procura no console de gerenciamento para facilitar a busca de regras;

3.7.5. A solução deverá ser gerenciada por Internet Explorer, Firefox ou MMC;
3.7.6. Brechas de segurança descobertas deverão ser protegidas de forma automática e transparente, interrompendo somente o tráfego de rede malicioso;

3.8. Do Console de Gerenciamento

ANEXO II
DESCRIÇÃO DOS MATERIAIS / SERVIÇOS

3.8.1. O gerenciamento da solução deverá ser por console Web, devendo suportar certificado digital ou MMC;

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

3.8.2.1. Nome do computador;
3.8.2.2. Nome do domínio;
3.8.2.3. Range de IP;
3.8.2.4. Sistema Operacional;
3.8.2.5. Máquina virtual.

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

3.8.4. 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;

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

3.8.6. 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;

3.8.7. 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;

3.8.8. 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;

3.8.9. 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;

3.8.10. Deve fornecer as seguintes informações dos computadores:

3.8.10.1. Se o antivírus está instalado;
3.8.10.2. Se o antivírus está iniciado;
3.8.10.3. Se o antivírus está atualizado;
3.8.10.4. Minutos/horas desde a última conexão da máquina com o servidor administrativo;
3.8.10.5. Minutos/horas desde a última atualização de vacinas;
3.8.10.6. Data e horário da última verificação executada na máquina;
3.8.10.7. Versão do antivírus instalado na máquina;
3.8.10.8. Se é necessário reiniciar o computador para aplicar mudanças;
3.8.10.9. Data e horário de quando a máquina foi ligada;
3.8.10.10. Quantidade de vírus encontrados (contador) na máquina;
3.8.10.11. Nome do computador;
3.8.10.12. Domínio ou grupo de trabalho do computador;
3.8.10.13. Data e horário da última atualização de vacinas;
3.8.10.14. Sistema operacional com Service Pack;
3.8.10.15. Quantidade de processadores;
3.8.10.16. Quantidade de memória RAM;
3.8.10.17. Usuário(s) logado(s) naquele momento, com informações de contato (caso disponíveis no Active Directory);
3.8.10.18. Endereço IP;
3.8.10.19. Aplicativos instalados, inclusive aplicativos de terceiros, com histórico de instalação, contendo data e hora que o software foi instalado ou removido;
3.8.10.20. Atualizações do Windows Updates instaladas;
3.8.10.21. Informação completa de hardware contendo: processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de áudio, adaptadores de rede, monitores, drives de CD/DVD;
3.8.10.22. Vulnerabilidades de aplicativos instalados na máquina;

ANEXO II
DESCRIÇÃO DOS MATERIAIS / SERVIÇOS

3.8.11. Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterá-las;
3.8.12. Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como:

3.8.12.1. Alteração de Gateway Padrão;
3.8.12.2. Alteração de subrede;
3.8.12.3. Alteração de domínio;
3.8.12.4. Alteração de servidor DHCP;
3.8.12.5. Alteração de servidor DNS;
3.8.12.6. Alteração de servidor WINS;
3.8.12.7. Alteração de subrede;
3.8.12.8. Resolução de Nome;
3.8.12.9. Disponibilidade de endereço de conexão SSL;

3.8.13. Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet;
3.8.14. Todos os eventos e ações realizadas no console de gerenciamento precisam ser gravados para fins de auditoria;
3.8.15. O console de gerenciamento e administração deverá permitir:

3.8.15.1. Envio de notificações via SMTP;
3.8.15.2. Replicação da estrutura do active directory no console de administração;
3.8.15.3. Armazenar políticas e logs em base de dados. A escolha da base de dados é facultativa, sendo as opções: Oracle, SQL e Derby Apache;
3.8.15.4. Apresentar capacidade de gerar roll back de suas atualizações de regras;
3.8.15.5. Integrar-se com:

3.8.15.5.1. Com o Active Directory para que os usuários do Active Directory possam administrar a solução de acordo com as permissões;
3.8.15.5.2. Com o Active Directory para que possa ser efetuado o controle das máquinas no Active Directory;
3.8.15.5.3. Com o Vmware vCenter 4.0 ou Superior, de modo a importar e sincronizar os objetos (hosts vmware e guests vm) para a console de gerenciamento da solução;

3.9. De Agentes e Perfis de Usuários

3.9.1. Os usuários deverão ser capazes de receber determinados perfis para administração da solução, incluindo no mínimo: "acesso total" e "acesso parcial";
3.9.2. Os componentes do acesso parcial deverão ser customizáveis;

3.9.2.1. Quando configurado o acesso parcial, este deve permitir que um usuário tenha permissões de poder gerenciar a segurança de um único computador, podendo ainda definir em quais módulos de proteção será possível ou não editar ou criar novas politicas de segurança;
3.9.2.2. A solução deverá:

3.9.2.2.1. Oferecer perfis default pré-definidos e aptos a funcionarem de acordo com sua denominação;
3.9.2.2.2. Possuir a capacidade de criar políticas de forma global para todas as máquinas, por perfis e individualmente para cada host;

3.9.3. Cada perfil poderá ser atribuído para um host ou um conjunto de hosts;

3.9.4. Os agentes deverão ser capazes de executar rastreamento nas máquinas onde estão instalados e após isso deverão fornecer uma lista de todas as recomendações de segurança para os softwares que estejam instalados nas máquinas bem como do sistema operacional;

ANEXO II
DESCRIÇÃO DOS MATERIAIS / SERVIÇOS

3.9.4.1. Os rastreamentos devem ocorrer de forma periódica a ser definida pelo administrador;

3.9.5. Os agentes deverão ter a capacidade de enviar logs para um dispositivo SIEM (Security Information and Event Management);

3.9.6. Agentes de atualização deverão buscar os updates das assinaturas e distribuí-las para os agentes. Quando ocorrer a atualização, esta deverá ocorrer de modo absolutamente seguro utilizando-se SSL com o servidor de onde ela buscará as informações;

3.9.7. Agentes para plataforma Microsoft deverão ser instalados por pacote MSI e posteriormente ativados pela console de gerenciamento de forma a proporcionar maior segurança ao ambiente;

3.9.8. Agentes para plataforma Linux deverão ser instalados por pacote RPM ou DEB e posteriormente ativados pela console de gerenciamento de forma a proporcionar maior segurança ao ambiente;

3.9.9. Para efeito de administração, a solução deverá avisar quando um agente encontrar-se não conectado a sua console de gerenciamento;

3.10. Da Emissão de Relatórios

3.10.1. A solução deverá permitir a criação e apresentar relatórios customizados de todas as suas funcionalidades;

3.10.2. A criação e envio dos relatórios deverá ocorrer sob demanda ou por meio de agendamento, com envio automático via e-mail;

3.10.3. A solução deverá permitir a exportação de relatórios no formato PDF e RTF;

3.10.4. Os relatórios deverão ser enviados para uma lista de contatos independente de login no console de administração;

3.11. Das Características do Firewall

3.11.1. Deverá operar como firewall de host, através da instalação de agente nos servidores protegidos;

3.11.2. O mecanismo de filtragem da solução deverá ser stateful bidirecional, de modo que a solução deverá logar na atividade stateful;

3.11.3. 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;

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

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

3.11.3.1.2. 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.

3.11.4. A solução deverá ser capaz de reconhecer e possibilitar o bloqueio endereços IP que estejam realizando Network Scan, Port Scan, TCP Null Scan, TCP FYNSYN Scan, TCP Xmas Scan e Computer OS FIngerprint por até 30 minutos;

3.11.4.1. As regras de firewall devem possuir a capacidade de:

3.11.4.1.1. Se apoiar em objetos (lista de ips, lista de MACs, e lista de portas) a fim de facilitar sua criação e administração;

3.11.4.1.2. Serem definidas distintamente conforme a especificidade de cada interface de rede;

ANEXO II
DESCRIÇÃO DOS MATERIAIS / SERVIÇOS

3.12. Características do Web Reputation

3.12.1. A solução deverá permitir:

3.12.1.1. A proteção contra acesso a websites ou URL consideradas maliciosas ou de baixa reputação;
3.12.1.2. A criação de listas de exclusão, permitindo que usuários acessem determinadas URLs especificadas pelo administrador do sistema;

3.12.2. A lista de URLs deverá ser fornecida e atualizada automaticamente pelo fabricante, permitindo a consulta em uma base local ou na nuvem da reputação das URLs acessadas;

3.13. Características do Anti-malware

3.13.1. A solução deverá permitir a proteção:

3.13.1.1. Contra códigos maliciosos através da instalação de agentes, permitindo rastreio de ameaças em tempo real e a varredura sob demanda e conforme agendamento, possibilitando a tomada de ações distintas para cada tipo de ameaça;
3.13.1.2. De anti-malware em ambiente Linux (Ubuntu, Red Hat e SuSe) utilizando agentes;
3.13.1.3. De anti-malware em ambiente Windows com ou sem agentes;

3.13.2. A solução deverá possibilitar:

3.13.2.1. A criação de listas de exclusão, para que o processo do antivírus não execute a varredura de determinados diretórios ou arquivos do SO;
3.13.2.2. A verificação de ameaças dentro de arquivos compactados, efetuando a limpeza apenas de arquivos maliciosos em casos de detecção;

4. DA SOLUÇÃO DE PROTEÇÃO PARA ENDPOINTS

4.1. Proteção para endpoints – Windows

4.1.1. O módulo de proteção Anti-Malware deve ter a capacidade de:

4.1.1.1. Realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais:

4.1.1.1.1. Windows Server 2003 sp2 (32/64-bit);
4.1.1.1.2. Windows Server 2008 (32/64-bit) e Windows Server 2008 r2 (32/64-bit);
4.1.1.1.3. Windows Server 2012;
4.1.1.1.4. Windows Server 2016;
4.1.1.1.5. Windows XP sp3 (x86/x64);
4.1.1.1.6. Windows vista (x86/x64);
4.1.1.1.7. Windows 7 (x86/x64);
4.1.1.1.8. Windows 8 e 8.1 (x86/x64);
4.1.1.1.9. Windows 10;
4.1.1.1.10. Detectar, analisar e eliminar programas maliciosos, tais como vírus, spyware, worms, cavalos de tróia, key loggers, programas de propaganda, rootkits, phishing, dentre outros;

4.1.1.2. Detectar, analisar e eliminar, automaticamente e em tempo real, programas maliciosos em:

4.1.1.2.1. Processos em execução em memória principal (RAM);
4.1.1.2.2. Arquivos executados, criados, copiados, renomeados, movidos ou modificados, inclusive em sessões de linha de comando (DOS ou Shell);
4.1.1.2.3. Arquivos compactados automaticamente, em pelo menos nos seguintes formatos: zip, exe, arj, mime/uu, Microsoft cab;
4.1.1.2.4. Arquivos recebidos por meio de programas de comunicação instantânea.

4.1.1.3. Detectar e proteger em tempo real a estação de trabalho contra

ANEXO II
DESCRIÇÃO DOS MATERIAIS / SERVIÇOS

vulnerabilidades e ações maliciosas executadas em navegadores web por meio de scripts em linguagens tais como javascript, vbscript/Activex;

4.1.1.4. Detectar variantes de malwares que possam ser geradas em tempo real na memória da estação de trabalho ou notebook, permitindo que seja tomada ação de quarentenar a ameaça;

4.1.1.5. Disponibilizar evidências de varredura em todas as estações de trabalho, identificando as atualizações de sucesso e as ações de insucesso visando o monitoramento de tais casos para futura tomada de ações pontuais;

4.1.2. Aferir a reputação das URLs acessadas pelas estações de trabalho e notebooks, sem a necessidade de utilização de qualquer tipo de programa adicional ou plug-in ao navegador web, de forma a proteger o usuário independente da maneira de como a URL está sendo acessada;

4.1.3. O módulo de proteção Anti-Malware deve permitir:

4.1.3.1. Configurar o consumo de CPU que será utilizada para uma varredura manual ou agendada;

4.1.3.2. Diferentes configurações de detecção tanto no modo varredura como no modo rastreamento, sendo as configurações disponíveis:

4.1.3.2.1. Em tempo real de arquivos acessados pelo usuário;

4.1.3.2.2. Em tempo real dos processos em memória, para a captura de programas maliciosos executados em memória, sem a necessidade de escrita de arquivo;

4.1.3.2.3. Manual, imediato ou programável, com interface gráfica em janelas, personalizável, com opção de limpeza;

4.1.3.2.4. Por linha-de-comando, parametrizável, com opção de limpeza;

4.1.3.2.5. Automáticos do sistema com as seguintes opções:

4.1.3.2.5.1. Escopo: todos os discos locais, discos específicos, pastas específicas ou arquivos específicos;

4.1.3.2.5.2. Ação: somente alertas, limpar automaticamente, apagar automaticamente, renomear automaticamente, ou mover automaticamente para área de segurança (quarentena);

4.1.3.2.5.3. Frequência: horária, diária, semanal e mensal;

4.1.3.2.5.4. Exclusões: pastas ou arquivos (por nome e/ou extensão) que não devem ser rastreados;

4.1.3.3. A restauração de maneira granular de arquivos quarentenados sob suspeita de representarem risco de segurança;

4.1.4. A solução deve possuir:

4.1.4.1. Detecção heurística de vírus desconhecidos;

4.1.4.2. Mecanismo de cachê de informações dos arquivos já escaneados;

4.1.4.3. Cachê persistente dos arquivos já escaneados para que nos eventos de desligamento e reinicialização das estações de trabalho e notebooks, a cache não seja descartada;

4.1.4.4. Ferramenta de alterações de parâmetros de comunicação entre o cliente antivírus e o servidor de gerenciamento da solução de antivírus;

4.2. Proteção para endpoints - Linux

4.2.1. Compatibilidade:

4.2.1.1. Plataforma 32-bits:

4.2.1.1.1. Ubuntu 14.04.5 LTS;

4.2.1.1.2. Ubuntu 16.04.4 LTS;

4.2.1.1.3. Ubuntu 17.10.1;

ANEXO II
DESCRIÇÃO DOS MATERIAIS / SERVIÇOS

4.2.1.1.4. Red Hat® Enterprise Linux® 6.9;
4.2.1.1.5. CentOS-6.9;
4.2.1.1.6. Debian GNU/Linux 8.10;
4.2.1.1.7. Debian GNU/Linux 9.4;

4.2.1.2. Plataforma 64-bits:

4.2.1.2.1. Ubuntu 14.04.5 LTS;
4.2.1.2.2. Ubuntu 16.04.4 LTS;
4.2.1.2.3. Ubuntu 17.10.1;
4.2.1.2.4. Ubuntu 18.04;
4.2.1.2.5. Red Hat® Enterprise Linux® 6.9;
4.2.1.2.6. Red Hat® Enterprise Linux® 7.4;
4.2.1.2.7. CentOS-6.9;
4.2.1.2.8. CentOS-7.4;
4.2.1.2.9. Debian GNU/Linux 8.10;
4.2.1.2.10. Debian GNU/Linux 9.4;
4.2.1.2.11. OracleLinux 7.4;
4.2.1.2.12. SUSE® Linux Enterprise Server 12 SP3;
4.2.1.2.13. openSUSE® 42.3;

4.2.2. Características:

4.2.2.1. Deve prover as seguintes proteções:

4.2.2.1.1. Antivírus de arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
4.2.2.1.2. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;

4.2.2.2. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

4.2.2.2.1. Capacidade de criar exclusões por local, máscara e nome da ameaça;
4.2.2.2.2. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);

4.2.2.3. Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;
4.2.2.4. Dectectar aplicações que possam ser utilizadas como vetor de ataque por hackers;
4.2.2.5. Fazer detecções através de heurística utilizando no mínimo as seguintes opções de nível:

4.2.2.5.1. Alta;
4.2.2.5.2. Média;
4.2.2.5.3. Baixa;
4.2.2.5.4. Recomendado;

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

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

ANEXO II
DESCRIÇÃO DOS MATERIAIS / SERVIÇOS

4.2.2.8. Em caso erros, deve ter capacidade de criar *logs* automaticamente, sem necessidade de outros softwares;
4.2.2.9. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
4.2.2.10. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;
4.2.2.11. Capacidade de verificar objetos usando heurística;
4.2.2.12. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;
4.2.2.13. Deve possuir módulo escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).

4.3. Proteção para endpoints - MAC

4.3.1. Compatibilidade:

4.3.1.1. masOS High Sierra 10.13;
4.3.1.2. macOS Sierra 10.12;
4.3.1.3. Mac OS X 10.11 (El Capitan);
4.3.1.4. Mac OS X 10.10 (Yosemite);
4.3.1.5. Mac OS X 10.9 (Mavericks).

4.3.2. Características:

4.3.2.1. Deve prover proteção residente para arquivos (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
4.3.2.2. Possuir módulo de web-antivírus para proteger contra ameaças durante navegação na internet com possíbilidade de analisar endereços https;
4.3.2.3. Possuir módulo de bloqueio á ataques na rede;
4.3.2.4. Possibilidade de bloquear a comunicação entre a máquina atacante e os demais computadores por tempo definido pelo administrador;
4.3.2.5. Capacidade de criar exclusões para computadores que não devem ser monitorados pelo módulo de bloqueio à ataques na rede;
4.3.2.6. Possibilidade de importar uma chave no pacote de instalação;
4.3.2.7. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
4.3.2.8. Deve possuir suportes a notificações utilizando o Growl;
4.3.2.9. 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);
4.3.2.10. Capacidade de voltar para a base de dados de vacina anterior;
4.3.2.11. Capacidade de varrer a quarentena automaticamente após cada atualização de vacinas;
4.3.2.12. 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;
4.3.2.13. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);

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

ANEXO II
DESCRIÇÃO DOS MATERIAIS / SERVIÇOS

arquivo;

4.3.2.15. Capacidade de verificar somente arquivos novos e alterados;
4.3.2.16. Capacidade de verificar objetos usando heurística;
4.3.2.17. Capacidade de agendar uma pausa na verificação;
4.3.2.18. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

4.3.2.18.1. Perguntar o que fazer, ou bloquear acesso ao objeto;
4.3.2.18.2. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
4.3.2.18.3. Caso positivo de desinfecção: Restaurar o objeto para uso;
4.3.2.18.4. Caso negativo de desinfecção: Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);

4.3.2.19. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
4.3.2.20. Capacidade de verificar arquivos de formato de e-mail;
4.3.2.21. Possibilidade de trabalhar com o produto pela linha de comando, com no mínimo opções para atualizar as vacinas, iniciar uma varredura, para o antivírus e iniciar o antivírus pela linha de comando;
4.3.2.22. Capacidade de ser instalado, removido e administrado pela mesma console central de gerenciamento.

4.4. Proteção para Estações de Trabalho – Funcionalidades de Atualização

4.4.1. As funcionalidades de atualização da solução devem incluir a capacidade de permitir:

4.4.1.1. A programação de atualizações automáticas das listas de definições de vírus, a partir de local predefinido da rede, ou de site seguro da internet, com frequência (no mínimo diária) e horários definidos pelo administrador da solução;
4.4.1.2. A atualização incremental da lista de definições de vírus;
4.4.1.3. A atualização automática do engine do programa de proteção a partir de localização na rede local ou na internet, a partir de fonte autenticável;
4.4.1.4. O rollback das atualizações das listas de definições de vírus e engines;
4.4.1.5. A indicação de agentes para efetuar a função de replicador de atualizações e configurações, de forma que outros agentes possam utiliza-los como fonte de atualizações e configurações, não sendo necessária a comunicação direta com o servidor de anti-malware para essas tarefas;
4.4.1.6. Deve permitir que os agentes de atualização possam replicar os componentes de vacinas, motores de escaneamento, versão de programas, hotfix e configurações específicas de domínios da árvore de gerenciamento;

4.4.2. O servidor da solução de anti-malware, deve ser capaz de gerar localmente versões incrementais das vacinas a serem replicadas com os agentes replicadores de atualizações e configurações, de maneira a reduzir o consumo de banda necessário para execução da tarefa de atualização;
4.4.3. O agente replicador de atualizações e configurações deve ser capaz de gerar localmente versões incrementais das vacinas a serem replicadas com os demais agentes locais, de maneira a reduzir o consumo de banda necessário para execução da tarefa de atualização;

4.5. Proteção para Estações de Trabalho – Console de Gerenciamento e Administração da Solução

4.5.1. A administração da solução se dará por console de gerenciamento, de modo que esta deverá:

4.5.1.1. Ser via web com gerenciamento por Internet Explorer, Firefox ou MMC;
4.5.1.2. Possuir dashboards customizáveis para monitoramento;
4.5.1.3. A customização deverá ser realizada pelo administrador da solução;

ANEXO II
DESCRIÇÃO DOS MATERIAIS / SERVIÇOS

4.5.1.4. As variáveis customizáveis deverão ser “quantidade” e “período”;
4.5.1.5. O administrador deverá poder optar por janelas de monitoramento no dashboard a sua disposição e poderá livremente adicionar ou remover de acordo com sua necessidade de visualização;

4.5.2. O console de gerenciamento deverá possuir a capacidade de:

4.5.2.1. Atualizar as vacinas, engines, assinaturas e recursos de inspeção de conteúdo de forma agendada e automática;
4.5.2.2. Facilitar a busca por detecções via mecanismo;
4.5.2.3. Identificar ameaças evasivas em tempo real com o provimento de análise profunda e inteligência para identificar e prevenir ataques;
4.5.2.4. Correlacionar regras de detecção de conteúdo malicioso durante todas as fases de um ataque.
4.5.2.5. Adicionar e remover os diversos recursos de visualização de informações na tela principal de monitoramento da ferramenta.

4.5.3. A solução deve possuir funcionalidade que permitam:

4.5.3.1. A proteção das configurações da solução instalada na estação de trabalho através de senha ou controle de acesso, em ambos os casos, controlada por política gerenciada pela console de administração da solução completa;
4.5.3.2. O bloqueio por nome de arquivo;
4.5.3.3. O rastreamento e bloqueio de infecções;
4.5.3.4. A desinstalação através da console de gerenciamento da solução;
4.5.3.5. Exportar/importar configurações da solução através do console de gerenciamento;
4.5.3.6. Realização do backup da base de dados através de mapeamento de rede controlado por senha;
4.5.3.7. Deletar os arquivos quarentenados;
4.5.3.8. A remoção automática de clientes inativos por determinado período de tempo;
4.5.3.9. A utilização de consulta externa a base de reputação de sites integrada e gerenciada através da solução de anti-malware, com opção de configuração para estações dentro e fora da rede, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante;
4.5.3.10. A criação de subdomínios consecutivos dentro da árvore de gerenciamento;
4.5.3.11. A criação de usuários locais de administração da console de anti-malware;
4.5.3.12. A gerência de domínios separados para usuários previamente definidos;
4.5.3.13. O envio de notificações específicas aos respectivos administradores de cada domínio definido na console de administração;
4.5.3.14. Instalação "silenciosa";
4.5.3.15. Efetuar a instalação remota nas estações de trabalho, sem requerer outro software ou agente adicional, previamente instalado e sem necessidade de reiniciar a estação de trabalho;
4.5.3.16. Desinstalar automaticamente e remotamente a solução de antivírus atual, sem requerer outro software ou agente;
4.5.3.17. Backup da base de dados da solução através do console de gerenciamento;
4.5.3.18. Designação do local onde o backup automático será realizado;
4.5.3.19. Determinar a capacidade de armazenamento da área de quarentena;
4.5.3.20. Prover segurança através de SSL para as comunicações entre o servidor e a console de gerenciamento web;
4.5.3.21. Prover segurança através de SSL para as comunicações entre o servidor e os agentes de proteção;
4.5.3.22. Bloquear acessos indevidos a área de administração do agente que não estejam na tabela de políticas definidas pelo administrador;
4.5.3.23. Criar perfis de usuários customizáveis, concedendo acessos também customizáveis ao console de gerenciamento;
4.5.3.24. Registrar no sistema de monitoramento de eventos do console de anti-malware informações relativas ao usuário logado no sistema operacional;

ANEXO II
DESCRIÇÃO DOS MATERIAIS / SERVIÇOS

4.5.4. As funcionalidades da solução devem possuir:

4.5.4.1. Mecanismo de detecção de ameaças baseado em comportamento de processos que estão sendo executados nas estações de trabalho e notebooks;
4.5.4.2. Solução de consulta do hash dos arquivos integrada e gerenciada através da solução de antivírus, cancelando o download ou execução do arquivo, de forma automática, baseado na resposta à consulta da base do fabricante;
4.5.4.3. Solução de reputação de sites local para sites já conhecidos como maliciosos integrada e gerenciada através da solução de antivírus, com opção de configuração para estações dentro e fora da rede, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante;
4.5.4.4. Mecanismo de autenticação da comunicação entre o servidor de administração e os agentes de proteção distribuídos nas estações de trabalho e notebooks;

4.5.5. A solução deverá prover ao administrador:

4.5.5.1. Relatórios de conformidade do status dos componentes, serviços, configurações das estações de trabalho e notebooks que fazem parte do escopo de gerenciamento da console de antivírus;
4.5.5.2. Informações sobre quais estações de trabalho e notebooks fazem parte do escopo de gerenciamento da console de anti-malware não realizaram o escaneamento agendado ou o escaneamento demandado pelo administrador no período determinado de dias;

4.5.6. A solução deverá integrar-se ao Active Directory para:

4.5.6.1. Acesso ao console de gerenciamento para administração;

4.5.6.1.1. A solução deverá suportar múltiplas florestas e domínios confiáveis do Active Directory;
4.5.6.2. Identificar quais máquinas estão sem a solução de anti-malware instalada;
4.5.6.3. Permitir agrupamento automático de estações de trabalho e notebooks do console de gerenciamento baseando-se no escopo do Active Directory ou IP;

4.6. Proteção para Estações de Trabalho – Do Controle de Dispositivos

4.6.1. O controle de dispositivos deverá controlar:

4.6.1.1. Acesso a discos removíveis reconhecidos como dispositivos de armazenamento em massa através de interfaces USB e outras, com as seguintes opções: acesso total, leitura e escrita, leitura e execução, apenas leitura, e bloqueio total;
4.6.1.2. Acesso a drives de mídias de armazenamento como CD-Rom, DVD, e pendrives, com as opções de acesso total, leitura e escrita, leitura e execução, apenas leitura e bloqueio total;

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

4.6.2.1. Discos de armazenamento locais;
4.6.2.2. Armazenamento removível;
4.6.2.3. Impressoras;
4.6.2.4. CD/DVD;
4.6.2.5. Drives de disquete;
4.6.2.6. Modems;
4.6.2.7. Dispositivos de fita;
4.6.2.8. Dispositivos multifuncionais;
4.6.2.9. Leitores de smart card;
4.6.2.10. Dispositivos de sincronização via ActiveSync (Windows CE, Windows Mobile, etc);
4.6.2.11. Wi-Fi;
4.6.2.12. Adaptadores de rede externos;

ANEXO II
DESCRIÇÃO DOS MATERIAIS / SERVIÇOS

4.6.2.13. Dispositivos MP3 ou smartphones;
4.6.1.14. Dispositivos Bluetooth;
4.6.1.15. Câmeras e Scanners.

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

4.6.3. Capacidade de habilitar "logging" em dispositivos removíveis tais como Pendrive, Discos externos, etc.

4.7. Proteção para Estações de Trabalho – Da Autoproteção

4.7.1. A solução deverá possuir mecanismo de proteção contra uso não autorizado no qual o agente do antivírus deve ser protegido contra mudança do seu estado (não possibilitar que um administrador da estação de trabalho e notebook possa parar o serviço do antivírus) bem como mecanismo para restaurar seu estado normal;

4.7.2. Devem estar inclusas no mecanismo de autoproteção:

4.7.2.1. Proteção e verificação dos arquivos de assinatura;
4.7.2.2. Proteção dos processos do agente de segurança;
4.7.2.3. Proteção das chaves de registro do agente de segurança;
4.7.2.4. Proteção do diretório de instalação do agente de segurança.

4.8. Proteção para Estações de Trabalho – Características do Host Firewall

4.8.1. O host firewall deverá ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais:

4.8.1.1. Windows Server 2003 sp2 (32/64-bit);
4.8.1.2. Windows Server 2008 (32/64-bit) e Windows Server 2008 r2 (32/64-bit);
4.8.1.3. Windows Server 2012 (32/64-bit);
4.8.1.4. Windows XP sp2 / sp3 (x86/x64);
4.8.1.5. Windows vista (x86/x64);
4.8.1.6. Windows 7 (x86/x64);
4.8.1.7. Windows 8 e 8.1 (x86/x64).

4.8.2. O host firewall deverá permitir a criação de:

4.8.2.1. Políticas de segurança personalizadas;
4.8.2.2. Regras de firewall utilizando os seguintes protocolos:
4.8.2.3. Icmp, icmpv6, igmp, tcp, udp, tcp+udp;
4.8.2.4. Regras de firewall por origem de ip ou mac ou porta e destino de ip ou mac ou porta;
4.8.2.5. Grupos lógicos através de lista de ip, mac ou portas;
4.8.2.6. Contextos para a aplicação para criação de regras de firewall;

4.8.3. Devem ser funcionalidades do host firewall:

4.8.3.1. Ativação e desativação do produto sem a necessidade de remoção do mesmo;
4.8.3.2. Varredura de portas lógicas do sistema operacional para identificar quais estejam abertas, possibilitando também o tráfego de entrada e saída;
4.8.3.3. Emissão de alertas via smtp e snmp;
4.8.3.4. Configuração e manipulação de políticas de firewall através de prioridades.

4.8.4. A solução deverá permitir a criação de dashboards customizáveis:

4.8.4.1. Os dashboards serão compostos por blocos de informações (widgets), visualizados através de gráficos ou tabelas;

4.8.4.2. As informações pertencentes aos painéis personalizáveis devem permitir filtros

ANEXO II
DESCRIÇÃO DOS MATERIAIS / SERVIÇOS

personalizados para facilitar a visualização e gerenciamentos;

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

4.8.5. Todas as regras das funcionalidades de firewall de host devem permitir apenas detecção (log) ou prevenção (bloqueio);

4.8.6. A solução deverá possuir módulo para proteção de vulnerabilidades com as funcionalidades de host firewall.

4.9. Proteção para Estações de Trabalho – Do Gerenciamento Centralizado dos Módulos

4.9.1. A solução de gerenciamento centralizado deve permitir a integração com a solução de segurança para proteção de estações de trabalho (desktops e notebooks), com todos os seus módulos e dispositivos móveis;

4.9.2. A instalação do servidor deverá ser na plataforma Windows 2003 Server ou superior, seja o servidor físico ou virtual;

4.9.3. O gerenciamento centralizado de módulos deverá:

4.9.3.1. Suportar base de dados sql;

4.9.3.2. Gerenciar logs das atividades e eventos gerados pela solução;

4.9.3.3. Integrar-se ao Microsoft ad – Active Directory;

4.9.3.4. Disponibilizar sua interface através dos protocolos http e https;

4.9.3.5. Possuir acompanhamento dos comandos administrativos em execução, tal como seu status de conclusão, alvo e usuário.

4.9.4. Os métodos de envio suportados devem incluir: e-mail, gravação de registros de eventos do Windows, SNMP e SYSlog;

4.9.5. A solução deverá permitir:

4.9.5.1. Atualização de todos os componentes de todos os módulos gerenciados;

4.9.5.2. Criação de planos de entrega das atualizações, com hora de início ou postergação da entrega após o download dos componentes;

4.9.5.3. Controle individual de cada componente a ser atualizado;

4.9.5.4. Definição de exceções por dias e horas para não realização de atualizações;

4.9.5.5. Ter como fonte de atualização um compartilhamento de rede no formato UNC;

4.9.5.6. Níveis de administração por usuários ou grupos de usuários;

4.9.5.7. Constituição de políticas genéricas aplicáveis a grupos de máquinas, ou aplicáveis a grupos de usuários;

4.9.5.8. Alteração das configurações das ferramentas ofertadas, de maneira remota;

4.9.5.9. Diferentes níveis de administração, de maneira independente do login da rede;

4.9.5.10. Pesquisas personalizadas para a consulta de eventos (logs) através de:

4.9.5.10.1. Categorias;

4.9.5.10.2. Critérios lógicos, com base em todos os campos pertencentes aos eventos consultados;

4.9.5.11. Configuração de/do:

4.9.5.11.1. Eventos administrativos ou de segurança que geram notificações, tal como o método de envio e o destinatário;

4.9.5.11.2. Intervalo de comunicação com os módulos gerenciados;

4.9.5.11.3. Intervalo de tempo necessário para que um módulo seja considerado fora do ar (off-line);

4.9.5.11.4. Informações que não são enviadas dos módulos à solução de gerenciamento centralizado;

4.9.5.11.5. Manutenção dos registros de eventos (logs), com base no intervalo de tempo que devem ser mantidos e no número máximo de registros, por tipo de evento;

4.9.5.12. Visualização de eventos de violação de segurança de todos os módulos

ANEXO II
DESCRIÇÃO DOS MATERIAIS / SERVIÇOS

gerenciados, agrupado por usuário numa linha de tempo, configurável;

4.9.5.13. Investigação de incidentes de vazamento de informação através de um número identificador de incidentes;

4.9.5.14. Gerencia dos módulos baseados no modelo de nuvem (cloud), quando existentes;

4.9.6. A solução deverá permitir a criação de políticas de segurança personalizadas;

4.9.6.1. As políticas de segurança devem permitir a seleção dos alvos baseados nos seguintes critérios:

4.9.6.1.1. Nome parcial ou completo das estações de trabalho, permitindo a utilização de caractere coringa para identificação do nome parcial da máquina;

4.9.6.1.2. Range de endereços IPS;

4.9.6.1.3. Sistema operacional;

4.9.6.1.4. Agrupamento lógico dos módulos;

4.9.6.2. As políticas de segurança devem permitir a combinação lógica dos critérios para identificação do(s) alvo(s) de cada política;

4.9.7. A solução deverá permitir a criação de modelos de relatórios customizáveis:

4.9.7.1. Relatórios e gráficos deverão ser parametrizáveis nos formatos HTML, PDF, XLS;

5. DA SOLUÇÃO DE PROTEÇÃO ANTI-SPAM, ANTI-SPAM PARA EXCHANGE

5.1. ANTI-SPAM (Software)

5.1.1. Servidor de Administração e Console Administrativa;

5.1.1.1. Compatibilidade Hardware e Software:

5.1.1.1.1. Vmware ESXI 5.5 Update 2;

5.1.1.1.2. Vmware ESXI 6.0 e 6.5.

5.1.2. Console de administração Linux ou Windows;

5.1.3. Capacidade de configuração dos seguintes parâmetros de ambiente de rede:

5.1.3.1. Alteração do Hostname;

5.1.3.2. Configurações de rede;

5.1.3.3. Configuração das interfaces de rede;

5.1.3.4. Configuração de DNS;

5.1.3.5. Configuração de rotas;

5.1.3.6. Reset de dispositivos de rede.

5.1.4. Capacidade de verificar o status das interfaces de rede;

5.1.5. Permite visualizar as todas de rede;

5.1.6. Capacidade de ativar serviços tais como:

5.1.6.1. Postfix;

5.1.6.2. Agente de atualização;

5.1.6.3. SNMP;

5.1.6.4. SSH;

5.1.6.5. Interface de administração web.

5.1.7. Executa comando ping a partir das interfaces selecionadas;

5.1.8. Possibilidade de selecionar teclado;

5.1.9. Alteração de timezone;

5.1.10. Capacidade de alterar a senha do administrador para acesso a console web;

5.1.11. Capacidade de alterar a senha do administrador para acesso a console via Terminal/SSH;

ANEXO II
DESCRIÇÃO DOS MATERIAIS / SERVIÇOS

5.1.12. Permite configurar o agente de rede incluindo as seguintes configurações:

5.1.12.1. Endereço;
5.1.12.2. Porta;
5.1.12.3. Uso de SSL;
5.1.12.4. Modo gateway;
5.1.12.5. Verificar comunicação com a console de gerenciamento;

5.1.13. Capacidade de visualizar logs através do terminal;
5.1.14. Habilita o modo de suporte para configurações básicas;

5.2. Configurações do anti-spam via console WEB:

5.2.1. Possui Assistente interativo de integração com a infraestrutura;
5.2.2. Capacidade de integrar com Edge Gateway;
5.2.3. Possibilidade de adicionar domínios locais no escopo;
5.2.4. Possibilidade de configurar rotas de direcionamento;
5.2.5. Possibilidade de adicionar redes e hosts confiáveis;
5.2.6. Possui sistema de Autenticação SPF;
5.2.7. Verifica se o e-mail do usuário existe quando está recebendo mensagens;
5.2.8. Capacidade de monitorar tráfego de e-mail com as seguintes características:

5.2.8.1. Limpos;
5.2.8.2. Não verificados;
5.2.8.3. Ameaças;
5.2.8.4. Phishing;
5.2.8.5. Spam;
5.2.8.6. Violação de autenticação;
5.2.8.7. Conteúdo.

5.2.9. Capacidade de verificar logs de mensagens por quantidade e tamanho;
5.2.10. Capacidade de verificar logs de mensagens enviadas com os seguintes parâmetros:

5.2.10.1. Hora;
5.2.10.2. Dia;
5.2.10.3. Semana;
5.2.10.4. 30 dias;
5.2.10.5. Parametrizável.

5.2.11. Gera relatórios de últimas ameaças detectadas;
5.2.12. Capacidade de monitorar a performance e recursos do sistema;
5.2.13. Monitora interfaces de envio e recebimento de mensagens por tamanho das mensagens e horário;
5.2.14. Possibilidade de criar regras de WhiteList;
5.2.15. Possibilidade de criar regras de BlackLists;
5.2.16. Capacidade de criar regras de conteúdo;
5.2.17. Possibilidade de utilizar as configurações do módulo de verificação;
5.2.18. Possibilidade de rejeitar mensagens sem verificação;
5.2.19. Possibilidade de excluir mensagens do processo de verificação;
5.2.20. Capacidade de gerar vereditos para os seguintes itens:
5.2.21. Se a mensagem for Spam:

5.2.21.1. Ignorar;
5.2.21.2. Rejeitar;
5.2.21.3. Deletar.

5.2.22. Se for um possível spam:

ANEXO II
DESCRIÇÃO DOS MATERIAIS / SERVIÇOS

5.2.22.1. Ignorar;
5.2.22.2. Rejeitar;
5.2.22.3. Deletar.

5.2.23. Se o endereço do remetente está em uma blacklist do DNSBL:

5.2.23.1. Ignorar;
5.2.23.2. Rejeitar;
5.2.23.3. Deletar.

5.2.24. Se for mensagens em massa:

5.2.24.1. Ignorar;
5.2.24.2. Rejeitar;
5.2.24.3. Deletar.

5.2.25. Capacidade de criar tags para e-mails considerados spam, prováveis spams, e-mails na blacklist e e-mails em massa;
5.2.26. Possibilidade de utilizar tecnologias de processamento de imagens gráficas;
5.2.27. Capacidade de verificar anexos em RTF;
5.2.28. Possibilidade de aumentar pontuação de spam se a mensagem estiver escrita em idiomas específicos;
5.2.29. Em caso de arquivos infectados as seguintes ações podem ser tomadas:

5.2.29.1. Desinfectar;
5.2.29.2. Deletar anexo;
5.2.29.3. Deletar mensagem;
5.2.29.4. Rejeitar mensagem;
5.2.29.5. Ignorar.

5.2.30. Se a desinfecção falhar, as seguintes ações podem ser tomadas:

5.2.30.1. Deletar anexo;
5.2.30.2. Deletar mensagem;
5.2.30.3. Rejeitar mensagem.

5.2.31. Capacidade de adicionar textos no assunto de e-mails com objetos infectados ou possivelmente infectados;
5.2.32. Capacidade de adicionar textos no assunto de e-mails que foram limpos pelo antivírus;
5.2.33. Se houver falhas da verificação de vírus do e-mail, as seguintes ações podem ser tomadas:

5.2.33.1. Deletar o anexo;
5.2.33.2. Deletar a mensagem;
5.2.33.3. Rejeitar;
5.2.33.4. Ignorar.

5.2.34. Capacidade de adicionar texto no campo assunto de emails que não foram verificados devido algum erro;
5.2.35. As seguintes ações podem ser tomadas caso um objeto criptografado seja detectado:

5.2.35.1. Deletar anexo;
5.2.35.2. Deletar mensagem;
5.2.35.3. Rejeitar a mensagem;
5.2.35.4. Ignorar.

5.2.36. Possibilidade de adicionar textos no campo assunto para e-mails com conteúdo criptografado;
5.2.37. Capacidade de criar exclusões de e-mails a serem verificados com os seguintes
5.2.38. parâmetros:

ANEXO II
DESCRIÇÃO DOS MATERIAIS / SERVIÇOS

5.2.38.1. Se o objeto for maior que;
5.2.38.2. Se o anexo contém prefixos específicos;
5.2.38.3. Não verifica arquivos anexos por tipo de arquivo.

5.2.39. Capacidade de criar exclusões de e-mails a serem verificados através das seguintes categorias:

5.2.39.1. Arquivos executáveis;
5.2.39.2. Arquivos do office;
5.2.39.3. Planilhas;
5.2.39.4. Apresentações;
5.2.39.5. Especializadas (.msg, .pub, etc);
5.2.39.6. Arquivos multimídia;
5.2.39.7. Arquivos de áudio;
5.2.39.8. Arquivos de imagem;
5.2.39.9. Arquivos compactados;
5.2.39.10. Arquivos de banco de dados;
5.2.39.11. Outros tipos de arquivos: .txt, .chm, .html e .htm.

5.2.40. Capacidade de tomar as seguintes ações para emails de phishing:

5.2.40.1. Deletar mensagem;
5.2.40.2. Rejeitar;
5.2.40.3. Ignorar.

5.2.41. Possibilidade de adicionar texto ao campo “assunto” dos e-mails com mensagens de phishing;
5.2.42. Possibilidade de adicionar texto ao campo “assunto” dos e-mails contendo URLs de sites com malware;
5.2.43. Capacidade de estabelecer parâmetros de filtro de conteúdo;
5.2.44. Possibilidade de tomar as seguitnes ações se o e-mail ultrapassar o tamanho permitido:

5.2.44.1. Rejeitar;
5.2.44.2. Deletar;
5.2.44.3. Ignorar.

5.2.45. Possibilidade de estabelecer o tamanho máximo permitido de uma mensagem de e-mail;
5.2.46. Toma as seguintes ações se um tipo de anexo for detectado:

5.2.46.1. Rejeitar;
5.2.46.2. Deletar mensagem;
5.2.46.3. Deletar anexo;
5.2.46.4. Ignorar.

5.2.47. Capacidade de configurar os tipos de anexos proibidos na empresa;
5.2.48. Possibilidade de tomar as seguintes ações quando um nome de anexo for proibido:

5.2.48.1. Rejeitar;
5.2.48.2. Deletar mensagem;
5.2.48.3. Deletar anexo;
5.2.48.4. Ignorar.

5.2.49. Capacidade de especificar nomes de anexos que serão proibidos.
5.2.50. Possibilidade de notificar as seguintes partes quando um objeto infectado é detectado:

5.2.50.1. Administrador;
5.2.50.2. Remetente;
5.2.50.3. Desditanário;
5.2.50.4. E-mails adicionais.

5.2.51. Capacidade de notificar administradores, remetentes, destinatários e e-mails adicionais

ANEXO II
DESCRIÇÃO DOS MATERIAIS / SERVIÇOS

quando um objeto criptografado é identificado;

5.2.52. Capacidade de notificar administradores, remetentes, destinatários e e-mails adicionais quando detectado erros na verificação de mensagens;

5.1.53. Capacidade de notificar administradores, remetentes, destinatários, e e-mails adicionais quando detectado problemas no filtro de conteúdo;

5.1.54. Capacidade de notificar administradores, remetentes, destinatários e e-mails adicionais quando mensagens de phishing são detectadas;

5.1.55. Possibilidade de criar “avisos legais” de vazamento de informações confidenciais e emails potenciamente inseguros;

5.1.56. Possibilidade de inserir “avisos legais” (disclaimer) em mensagens com conteúdo criptografado, com phishing, infectadas e corrompidas;

5.1.57. Capacidade de validar SPF;

5.1.58. Capacidade de verificar autenticação DKIM;

5.1.59. Se uma violação de DMARC é detecada, toma as seguintes ações:

- **5.1.59.1.** Aplica a política DMARC;
- **5.1.59.2.** Rejeita;
- **5.1.59.3.** Deleta a mensagem;
- **5.1.59.4.** Ignora;

5.1.60. Capacidade de sincronização com LDAP;

5.1.61. Capacidade de adicionar remetentes e destinatários por Email, endereço IP e contas do LDAP;

5.1.62. Suporta criptografia em TLS;

5.1.63. Capacidade de tornar a criptografia em TLS negada, aceita ou requerida;

5.1.64. Aceita protocolos SMTP e LMTP;

5.1.65. Possibilidade de criar backups e limitar o tamanho máximo do mesmo;

5.1.66. Possibilidade de configurar um limite de espaço em disco para enviar notificação;

5.1.67. Possibilidade de liberar a entrega de mensagens infectadas;

5.1.68. Capacidade de tomar as seguintes ações se o backup estiver indisponível:

- **5.1.68.1.** Processar mensagem;
- **5.1.68.2.** Falha temporariamente;
- **5.1.68.3.** Rejeita mensagens;

5.1.69. Efetuar backup em tempo real;

5.1.70. Capacidade de monitorar a fila de e-mails através do seguintes parâmetros:

- **5.1.70.1.** Mensagens deferidas;
- **5.1.70.2.** Mensagens Ativas;
- **5.1.70.3.** Mensagens de entrada e saída;
- **5.1.70.4.** ID da mensagem;
- **5.1.70.5.** Remetente;
- **5.1.70.6.** Destinatário;
- **5.1.70.7.** Período de tempo;
- **5.1.70.8.** Tamanho da mensagem.

5.1.71. Capacidade de criar relatórios customizados e enviá-lo ao administrador e/ou e-mails adicionais em formato .PDF;

6. CONFIGURAÇÕES GERAIS

6.1. Capacidade de configurar Proxy com possibilidade de ignorá-lo para endereços locais;

6.2. Possibilidade de personalizar endereço de e-mail da aplicação e do administrador;

6.3. Possibilidade de habilitar conta para suporte, podendo editar o usuário, senha e liberar envio de

ANEXO II
DESCRIÇÃO DOS MATERIAIS / SERVIÇOS

mensagens infectadas pelo usuário para teste;

6.4. Capacidade de personalizar os eventos de log de sistema;
6.5. Configuração de grupos de verificação personalizável;
6.6. Pode ser feito adição de mensagens no cabeçalho da mensagem;
6.7. Possibilidade de criar templates quando um anexo é removido da mensagem;
6.8. Capacidade de exportar configurações;
6.9. Possibilidade de importar configurações;
6.10. Configurações de MTA personalizáveis tais como: Nome do domínio, hostname, etc;
6.11. Possibilidade de configurar limite de tamanho para mensagens no MTA;
6.12. Configurações avançadas de SMTP;
6.13. Possibilidade de limitar tentativas de conexão. Ou seja, evita ataques de DoS;
6.14. Capacidade de limitar número de conexões simultâneas;
6.15. Limita a quantidade de solicitações de entrega de e-mail;
6.16. Possibilidade de configurar o "timeout" de conexões SMTP;
6.17. Capacidade de limitar tempo de uma mensagem na fila de entrega;
6.18. "Timeout" para "bounce messages" configurável;
6.19. Possibilidade de enviar mensagens para destinatários específicos em todas as mensagens recebidas;
6.20. Verifica se o formato do endereço está dentro da RFC 821;
6.21. Possibilidade de desativar a verificação de destinatários;
6.22. Capacidade de atualizar a versão do produto somente importando o arquivo de instalação;
6.23. Possibilidade de utilizar servidores proxy para atualizar as definições;
6.24. Capacidade de agendar horários específicos para atualização do banco de dados;
6.25. Possibilidade de sincronizar com servidores NTP através da console Linux;
6.26. O PRÉ-FILTRO deverá permitir a verificação:

6.26.1. De hash das mensagens em tempo real para proteção contra SPAMs;
6.26.2. Heurística contra vírus recém-lançados, mesmo sem uma vacina disponível;
6.26.3. Do tipo real do arquivo, mesmo que o mesmo for renomeado.

6.27. O PRÉ-FILTRO deverá permitir O bloqueio:

6.27.1. De servidores spammers através da metodologia conhecida por Domain Keys Identified Mail (DKIM);
6.27.2. De malware empacotado (packed malware) de forma heurística.

6.28. O PRÉ-FILTRO deverá permitir proteção contra:

6.28.1. Phishings;
6.28.2. Spywares, sem a necessidade de um software ou agente adicional;
6.28.3. Dialers, sem a necessidade de um software ou agente adicional;
6.28.4. Ferramentas Hackers, sem a necessidade de um software ou agente adicional;
6.28.5. Ferramentas para descobrir senhas de aplicativos, sem a necessidade de um software ou agente adicional;
6.28.6. Adwares, sem a necessidade de um software ou agente adicional;
6.28.7. Ferramentas, sem a necessidade de um software ou agente adicional.

6.29. O PRÉ-FILTRO deverá permitir a detecção de:

6.29.1. Command and Control; VIRUS;
6.29.2. SPAMs utilizando tecnologia heurística, podendo ser configurada a sensibilidade da ferramenta.

6.30. Funcionalidades permitidas pelo PRÉ-FILTRO:

6.30.1. Approved list para domínios em se habilitando o domain keys identified mail (DKIM);
6.30.2. Criação de White e Black Lists para um melhor ajuste na detecção de SPAMs;
6.30.3. Verificação da reputação de links que estejam dentro do corpo das mensagens;
6.30.4. Ajuste do nível de sensibilidade do bloqueio de mensagens que tiverem links com má

ANEXO II
DESCRIÇÃO DOS MATERIAIS / SERVIÇOS

reputação;

6.30.5. White List para a checagem de reputação em URLs dentro de mensagens;
6.30.6. Escaneamento de arquivos executáveis comprimidos em tempo real.

6.31. A solução deverá possuir um filtro de conteúdo com pesquisa por palavras-chave no cabeçalho e corpo da mensagem, e em arquivos Microsoft Office anexados, utilizando operadores lógicos tais como AND, OR, OCCUR, NEAR, (,), [,] e assim por diante;

6.32. O FILTRO deverá permitir:

6.32.1. A criação de:

6.32.1.1. Filtros definidos pelo tamanho de mensagem;
6.32.1.2. Exceções para os filtros, definidos por rotas, grupos de usuários ou usuários específicos;
6.32.1.3. Regras distintas para mensagens que entram e saem do ambiente;
6.32.1.4. Áreas de quarentenas separadas para cada tipo de filtro;
6.32.1.5. Grupos de usuários para configuração de regras por grupo ou usuário.

6.32.2. O bloqueio de:

6.32.2.1. Anexos pela extensão, pelo tipo real do arquivo, nome, tamanho, e número de anexos;
6.32.2.2. Arquivos anexos baseado em sua extensão, tamanho, tipo real do arquivo (independente da extensão) e dentro de arquivos compactados.

6.32.3. A verificação:

6.32.3.1. Em arquivos compactados nos formatos mais utilizados em até 10 níveis de compactação;
6.32.3.2. Contra conteúdos não autorizados dentro dos arquivos anexados nas mensagens;
6.32.3.3. Recurso que retire anexos indesejados e entregues com a mensagem original para o destinatário;
6.32.3.4. Limitação do número de destinatários por mensagem;
6.32.3.5. Regra específica para anexos protegidos por senha.

6.33. FILTROS POR IP deverão permitir:

6.33.1. A prevenção contra ataques de:

6.33.1.1. SPAM, permitindo rejeitar a conexão quando exceder configuração personalizada para esse ataque;
6.33.1.2. Vírus, permitindo rejeitar a conexão quando exceder configuração personalizada para esse ataque;
6.33.1.3. DHA (Directory Harvest Attack).

6.33.2. A configuração:

6.33.2.1. Individual entre Reputação Global (da empresa prestadora do serviço) e Reputação Local (personalizada);
6.33.2.2. Do nível de sensibilidade da reputação de Ips em até quatro níveis;
6.33.2.3. Do código de erro para mensagens rejeitadas.

6.33.3. A personalização dos filtros baseado em:

6.33.3.1. Tempo;
6.33.3.2. Total de mensagens;
6.33.3.3. Porcentagem de mensagens;
6.33.3.4. Ação a ser tomada.

ANEXO II
DESCRIÇÃO DOS MATERIAIS / SERVIÇOS

6.33.4. A verificação de:

6.33.4.1. Endereços IPs para checar a sua legitimidade, sendo elas, conexões suspeitas, apresentando o domínio responsável pela conexão, apresentando o total de conexões e dessas, o percentual de conexões maliciosas;
6.33.4.2. Exceções ao bloqueio por reputação com base em pais, IP ou range de IP;
6.33.4.3. Checagem na rede Global (colaborativa) da reputação dos IPs que tentam se conectar ao ambiente para enviar mensagens.

6.34. Os FILTROS POR IP deverão:

6.34.1. Não necessitar instalação adicional;
6.34.2. Possuir bases do mesmo fabricante do software para gateway SMTP;
6.34.3. Possuir configuração personalizada para cada tipo de ataque (SPAM, Vírus, Dicionário (DHA) e Mensagens de Retorno (Bounced Mails));

7. ANTI-SPAM (SOFTWARE)

7.1. Descrição das ações da solução - a solução deverá permitir:

7.1.1. Adiamento da entrega de determinadas mensagens para um horário específico;
7.1.2. Envio notificações de ocorrências customizadas ao administrador, remetente, destinatário ou qualquer outro endereço de e-mail;
7.1.3. Customização:

7.1.3.1. Das ações que a ferramenta deve tomar de acordo com as necessidades do ambiente;
7.1.3.2. Da mensagem que será inserida no corpo das mensagens.

7.1.4. Inserção de:

7.1.4.1. Carimbo no assunto da mensagem;
7.1.4.2. Header customizado (X-header);
7.1.4.3. Texto no corpo da mensagem.

7.1.5. Direcionamento da mensagem para servidor diferente do padrão (próximo hop) de acordo com a necessidade do ambiente;
7.1.6. Exclusão de anexos indesejados com envio de mensagem ao destinatário informando da ação;
7.1.7. Determinação do local onde se irá colocar a notificação customizada para o começo ou fim da mensagem original;
7.1.8. Inserção de variáveis nas notificações, onde informem:

7.1.8.1. Remetente;
7.1.8.2. Destinatário;
7.1.8.3. Assunto;
7.1.8.4. Data;
7.1.8.5. Nome do arquivo detectado;
7.1.8.6. Nome do vírus detectado;
7.1.8.7. Protocolo de escaneamento;
7.1.8.8. Tamanho total da mensagem e seus anexos;
7.1.8.9. Tamanho total do anexo;
7.1.8.10. Número de anexos detectados pela regra;
7.1.8.11. Ação tomada pela ferramenta;
7.1.8.12. Nome da quarentena para onde a mensagem foi enviada.

7.1.9. Configurar ações para mensagens fora do padrão (mensagens mal formadas);
7.1.10. Ação personalizada para mensagens com anexos protegidos por senha;
7.1.11. Quarentenar mensagens de SPAM;

ANEXO II
DESCRIÇÃO DOS MATERIAIS / SERVIÇOS

7.1.12. Encaminhar as mensagens em cópia oculta para destinatário não inserido originalmente na mensagem;
7.1.13. Arquivar as mensagens sem que o remetente ou destinatário saibam para fins de auditoria;

7.2. ANTI-SPAM (Software) – Quarentena

7.2.1. A solução deverá Apresentar Console web para que os usuários possam verificar as mensagens que estejam em quarentena por motivo de spam;
7.2.2. Possuir Acesso à área de quarentena dos usuários por meio de integração com o AD ou via SMTP autentication.
7.2.3. Exclusão automática das mensagens em quarentena;
7.2.4. Permitir que usuários:

7.2.4.1. Criem lista de exceções a remetentes no console web de quarentena de mensagens;
7.2.4.2. Verifiquem mensagens suspeitas postas em quarentena e aprovem remetentes sem intervenção do administrador.

7.3. ANTI-SPAM (Software) – Da Administração

7.3.1. O gerenciamento da solução deverá ser via console web HTTPS (Internet Explorer/ Firefox);
7.3.2. A solução deverá possuir um passo a passo (Wizard) de instalação e configuração;
7.3.3. A administração deverá permitir:

7.3.3.1. O gerenciamento das áreas de quarentena, com pesquisa, reprocessamento, entrega ou exclusão de mensagem;
7.3.3.2. Realizar atualização de forma automática das vacinas de forma incremental e da versão do software. A atualização deve permitir conexão através de serviço Proxy;
7.3.3.3. Possibilidade de configurar “greeting” SMTP;
7.3.3.4. Controle de relay baseado no domínio e/ou endereço IP;
7.3.3.5. Recurso que faça uma monitoração do sistema, alertando o administrador caso haja falta de espaço em disco, se o serviço estiver indisponível e se a fila de mensagens chegarem a um número estabelecido como máximo pelo administrador;
7.3.3.6. Verificação de mensagens no protocolo POP3, permitindo configurar que porta TCP será utilizada;
7.3.3.7. Capacidade de checagem por DNS reverso com até quatro diferentes níveis de bloqueio;
7.3.3.8. Definição de timeout de conexão SMTP;
7.3.3.9. Suporte a ilimitadas conexões SMTP.

7.3.4. Possuir Capacidade de ter vários servidores de rastreamento de tráfego SMTP gerenciado por console único;
7.3.5. Proteção do tráfego POP3;
7.3.6. Gerência de área exclusiva para quarentena ou cópia de mensagens;
7.3.7. Domínio mascarado;
7.3.8. Autenticação via TLS (Transport Layer Security);
7.3.9. Apresentação de relatórios criados através de console web;
7.3.10. Disponibilização de relatórios gerenciais que podem ser "on demand" ou agendados;
7.3.11. Relatórios gerenciais de utilização de mensagens por destinatário, remetente, assunto;
7.3.12. Templates predefinidos para relatórios de forma a facilitar a geração de relatórios;
7.3.13. Integração com (Microsoft Active Directory, Lotus Domino, Sun iPlanet Directory);
7.3.14. Recebimento de tráfego em TLS e realizar conexões em TLS para outros servidores;
7.3.15. Tráfego via Secure SMTP;
7.3.16. Reindexação da base de dados de forma agendada;

ANEXO II
DESCRIÇÃO DOS MATERIAIS / SERVIÇOS

7.3.17. Importação e exportação de suas políticas através da console de gerenciamento;
7.3.18. Criação de usuários com acessos diferentes de administrador à console de gerenciamento;
7.3.19. Integração do login do console de gerenciamento com o serviço de LDAP pré-configurado.

8. PROTEÇÃO PARA EXCHANGE

8.1. Características gerais - O produto deverá suportar:

8.1.1. VSAPI 2.5 e 2.6 da Microsoft;
8.1.2. Cluster Microsoft bem como as versões do MS-Exchange 2003, 2007 e 2010. No caso do MS-Exchange 2007, suportar a instalação na plataforma Windows 2008.

8.2. O produto deverá Integrar-se a/ao:

8.2.1. MOM/SCOM da Microsoft para envio de notificações;
8.2.2. A pasta JUNK MAIL ou SPAM do Outlook de modo que os spams sejam direcionados diretamente para essa pasta.

8.3. Possuir capacidade de gerar um certificado para o servidor web, para um acesso seguro;
8.4. Possuir serviço clusterizado e trabalho em cluster ativo-ativo e ativo-passivo;
8.5. A proteção para Exchange deverá permitir:

8.5.1. Regras de controle de conteúdo definidos por rotas, usuários e grupos;
8.5.2. Filtração com base no tamanho das mensagens.

8.6. A instalação:

8.6.1. Do tipo remoto múltiplos servidores Exchange, monitorando o status de cada instalação;
8.6.2. Do tipo silencioso, sem intervenção do administrador.

8.7. A configuração:

8.7.1. Das portas de comunicação para o gerenciamento;
8.7.2. Das notificações a serem enviadas para o administrador, via email e SNMP.

8.8. A verificação:

8.8.1. Do Internet Mail Connector (IMC);
8.8.2. De conteúdos não autorizados dentro dos arquivos anexados nas mensagens.

8.9. Gerenciamento de:

8.9.1. Vários servidores Exchange simultaneamente;
8.9.2. Quarentena, podendo enviar, encaminhar e apagar mensagens que estiverem nela;
8.9.3. Os usuários devem ter a capacidade de, se permitido, criar suas exceções de recebimento através de white list gerenciada no próprio Outlook.

8.10. Em relação à verificação:

8.10.1. Deverá ser realizada em background para não impactar a performance;
8.10.2. Deverá possuir as opções: verificação em tempo real, verificação manual e verificação agendada de grupos e bases de dados no Exchange
8.10.3. A solução deverá possuir verificação em memória e multi-threaded;
8.10.4. A verificação no Information Store deve ser realizada nas Public e Private Stores.

8.11. A verificação deverá ser realizada:

8.11.1. Contra códigos maliciosos no corpo da mensagem;
8.11.2. Em arquivos baseado em seu tipo real, independente da extensão apresentada;
8.11.3. Somente em arquivos passíveis de códigos maliciosos, permitindo assim um melhor

ANEXO II
DESCRIÇÃO DOS MATERIAIS / SERVIÇOS

desempenho da solução.

8.12. O produto deverá ter a capacidade de:

- **8.12.1.** Ação de limpeza para os arquivos anexados;
- **8.12.2.** Prover proteção para mensagens enviadas via Outlook Web Access (OWA);
- **8.12.3.** Detectar SPAMs utilizando tecnologia heurística, podendo ser configurada a sensibilidade da ferramenta.

8.13. Possuir approved list para recebimento de mensagens de determinados senders;
8.14. Avaliar reputação de links HTTP que estejam dentro do e-mail quanto a sua reputação e, em caso reputação negativa, deverá ser tomada uma ação na mensagem;
8.15. Marcar as mensagens detectadas como SPAM no campo "assunto", preservando também o conteúdo original;
8.16. Gerenciar via console web (Internet Explorer), com controle de time-out.
8.17. Realizar ações específicas para cada tipo de código malicioso;
8.18. Em caso de epidemia, bloquear a entrada de determinados emails, baseado nas características de códigos maliciosos, restaurando as configurações originais ao término da epidemia, ambos de forma automática através de políticas recebidas do fabricante;
8.19. Proteção contra spywares, sem a necessidade de um software ou agente adicional;
8.20. Detectar e bloquear malwares empacotados (packed malwares);
8.21. Realizar reputação dos IPs que estejam conectando no Exchange server e caso IP seja de má reputação que a mensagem seja bloqueada;
8.22. Executar rastreamento agendado ou manual nas mailboxes dos usuários;
8.23. Possuir acessos por papéis em sua console com diferentes perfis de acessos e diferentes acessos a menus;
8.24. Filtrar conteúdo realizando o rastreamento dentro do anexo da mensagem;
8.25. Procurar por conteúdo no subject, corpo e cabeçalho da mensagem em caso de regra de controle de conteúdo;
8.26. Deverão ser gerados relatórios de:

- **8.26.1.** Vírus, spyware, grayware e outros malwares, com gráficos em escala horária, diária, semanal e mensal;
- **8.26.2.** Principais vírus/malwares, spywares e graywares;
- **8.26.3.** Principais senders de vírus/malwares, spywares e graywares;
- **8.26.4.** Resumo das ações tomadas contra vírus/malwares, spywares e graywares;
- **8.26.5.** Resumo do bloqueio de anexos;
- **8.26.6.** Gráfico do bloqueio de anexos, com escala horária, diária, semanal e mensal;
- **8.26.7.** Principais tipos de anexos bloqueados;
- **8.26.8.** Principais nomes de anexos bloqueados;
- **8.26.9.** Principais extensões de anexos bloqueados;
- **8.26.10.** Gráfico do filtro de mensagens, com escala horária, diária, semanal e mensal;
- **8.26.11.** Principais remetentes e destinatários filtrados.
- **8.26.12.** Resumo de spam;
- **8.26.13.** Gráfico do filtro de spams, com escala horária, diária, semanal e mensal;
- **8.26.14.** Principais fontes e destinatários de spam;
- **8.26.15.** Tráfego por hora, dia e mês.

8.27. Sobre os bloqueios:

- **8.27.1.** Deverão ser permitidos bloqueios de arquivos anexos baseado em sua extensão, tamanho, tipo real do arquivo (independente da extensão) e também dentro de arquivos compactados;
- **8.27.2.** Os bloqueios dos arquivos em anexos devem ser com base em política por usuário e integrado com o active directory para a criação dessas políticas;
- **8.27.3.** Políticas de bloqueio de anexo e de bloqueio de conteúdo deverão possuir exceções;

ANEXO II
DESCRIÇÃO DOS MATERIAIS / SERVIÇOS

8.28. A solução deverá ter a possibilidade de executar as seguintes ações:

8.28.1. Em caso de conteúdo malicioso: substituir por um texto, quarentenar a mensagem inteira, quarentenar parte da mensagem, deletar a mensagem inteira, fazer back-up/cópia da mensagem, passar parte da mensagem;
8.28.2. Em caso de violação de anexo não desejado, substituir por um texto, quarentenar a mensagem inteira, quarentenar parte da mensagem, deletar a mensagem inteira, fazer o back-up/cópia da mensagem;
8.28.3. Em caso de mensagens infectadas: substituir por um texto, quarentenar a mensagem inteira, deletar a mensagem inteira, passar, quarentenar par te da mensagem.

8.29. Em relação à quarentena:

8.29.1. Deverá possuir uma área de quarentena para o usuário final, integrada à ferramenta, para serem armazenados os emails detectados como SPAM, para que o usuário possa refinar a ferramenta;
8.29.2. Deverá possuir área de quarentena no servidor com gerencia pelo administrador através da liberação de mensagens ou deleção.

9. FORNECIMENTO DE TREINAMENTO E CAPACITAÇÃO

9.1. Deverão ser contemplados 3 (três) treinamentos oficiais on site para a capacitação de profissionais da PREFEITURA MUNICIPAL DE SANTO ANDRÉ na solução ofertada, com carga horária conforme abaixo:

9.1.1. 1º Treinamento (Turma 1): Solução de proteção para endpoint e para servidores virtuais – no mínimo 20 horas – participação de 3 (três) profissionais;
9.1.2. 2º Treinamento (Turma 2): Solução de proteção para endpoint e para servidores virtuais – no mínimo 20 horas; - participação de 3 (três) profissionais;
9.1.3. 3º Treinamento (Turma única): Solução de proteção “Anti-Spam” e “Anti-Spam para Exchange” – no mínimo 8 Horas – participação de 6 (seis) profissionais.

9.2. O treinamento oferecido deverá conter, no mínimo:

9.2.1. Funcionalidades básicas;
9.2.2. Gerenciamento avançado;
9.2.3. Instalação e desinstalação do software cliente;
9.2.4. Instalação e desinstalação do software.

9.3. O treinamento deverá ser realizado por instituição qualificada e certificada pelo fabricante da solução ofertada;
9.4. O treinamento deverá ser oficial e com material dos produtos ofertados.

ANEXO III
DESCRIÇÃO DOS DOCUMENTOS DE HABILITAÇÃO

1. DOCUMENTOS DE HABILITAÇÃO

1.1 Registro Comercial, em se tratando de **Empresa Individual de responsabilidade limitada e de Empresário Individual**, **no segundo caso**, acompanhado da Cédula de Identidade (caso este documento tenha sido entregue juntamente com o credenciamento da Licitante não será necessário sua inclusão no envelope "Documentos de Habilitação");

1.2 Ato Constitutivo, Estatuto ou Contrato Social em vigor, devidamente registrado na Junta Comercial, acompanhado de suas respectivas alterações, em se tratando de Sociedade Empresária (caso este documento tenha sido entregue juntamente com o credenciamento da Licitante não será necessário sua inclusão no envelope "Documentos de Habilitação");

1.3 Documentos de eleição dos atuais administradores, acompanhados da documentação mencionada no subitem anterior (Estatuto), em se tratando de Sociedade por Ações (caso este documento tenha sido entregue juntamente com o credenciamento da Licitante não será necessário sua inclusão no envelope "Documentos de Habilitação");

1.4 Ato Constitutivo ou Contrato Social em vigor, devidamente registrado no Cartório de Registro Civil de Pessoas Jurídicas e/ou na Junta Comercial, acompanhado de suas respectivas alterações bem como de prova da diretoria em exercício, em se tratando de Sociedade Simples (caso este documento tenha sido entregue juntamente com o credenciamento da Licitante não será necessário sua inclusão no envelope "Documentos de Habilitação");

1.5 Decreto de Autorização e Ato de Registro ou Autorização para Funcionamento, expedido pelo órgão competente, quando a atividade assim o exigir, em se tratando de empresa ou sociedade estrangeira em funcionamento no País (caso este documento tenha sido entregue juntamente com o credenciamento da Licitante não será necessário sua inclusão no envelope "Documentos de Habilitação");

1.6 Comprovante de inscrição e de situação cadastral no CNPJ – Cadastro Nacional da Pessoa Jurídica expedido pelo Ministério da Fazenda – Secretaria da Receita Federal do Brasil;

1.7 Prova de regularidade relativa ao Fundo de Garantia por Tempo de Serviço (FGTS) através do documento "Certificado de Regularidade do FGTS – CRF", expedido pela Caixa Econômica Federal, demonstrando situação regular no cumprimento dos encargos sociais instituídos por Lei (a aceitação deste documento condiciona-se à confirmação de sua autenticidade via internet, pelo Pregoeiro ou por membro de sua equipe de apoio, conforme mencionado no item 12.4 deste Edital);

1.8 Prova de regularidade relativa à Seguridade Social e tributos federais através do documento "Certidão Negativa, ou Positiva com efeitos de Negativa, de Débitos relativos a Tributos Federais e à Dívida Ativa da União", expedida pela Secretaria da Receita Federal do Brasil, nos termos da Portaria Conjunta RFB/PGFN nº 1.751/14 (a aceitação deste documento condiciona-se à confirmação de sua autenticidade via internet, pelo Pregoeiro ou por membro de sua equipe de apoio, conforme mencionado no item 12.4 deste Edital);

1.9 Prova de inexistência de débitos trabalhistas através do documento "Certidão Negativa de Débitos Trabalhistas – CNDT ou Certidão Positiva de Débitos Trabalhistas com os mesmos efeitos da CNDT", expedida pela Justiça do Trabalho conforme Lei nº. 12.440, de 07 de julho de 2011 (a aceitação deste documento condiciona-se à confirmação de sua autenticidade via internet, pelo Pregoeiro ou por membro de sua equipe de apoio, conforme mencionado no item 12.4 deste Edital).

ANEXO III
DESCRIÇÃO DOS DOCUMENTOS DE HABILITAÇÃO

1.10 Prova de regularidade para com as Fazendas:

1.10.1 **ESTADUAL**, através do documento Certidão Negativa, ou positiva com efeitos de negativa, de Débitos **INSCRITOS** relativos aos Tributos Estaduais do domicílio ou sede da Licitante. (em conformidade com a Portaria CAT-20, de 01.04.98 – Governo do Estado de São Paulo);

1.10.2 **MUNICIPAL**, através do documento "Certidão Negativa, ou Positiva com efeitos de Negativa, de Débitos relativos aos Tributos Mobiliários Municipais" do domicílio ou sede da Licitante, ou outra equivalente na forma da Lei.

1.11 Certidão Negativa de Falência ou Concordata, Recuperação Judicial ou Extrajudicial, expedida pelo Distribuidor Judicial do Foro da sede da Licitante, emitido em prazo, conforme subitem 12.5 do Edital, não superior a 180 (cento e oitenta) dias entre a data de sua expedição e a da abertura da sessão pública;

1.12 Declaração expressa do Licitante firmada, sob as penas da lei, de que:
(Conforme Anexo VIII do edital)

1.12.1 Não se encontra sujeito aos efeitos de declaração de inidoneidade para licitar ou contratar com a Administração Pública, nos termos do artigo 87, IV, da Lei nº 8.666/93, firmada em quaisquer das esferas da Federação, ou a qualquer outro título;

1.12.2 Não existe qualquer fato impeditivo à sua habilitação ou eventual contratação com o Poder Público, por atender integralmente às condições exigidas para sua habilitação, nos termos previstos na legislação em vigor e no presente Edital;

1.12.3 Não descumpre as proibições quanto à utilização de mão de obra infantil, menor de 16 (dezesseis) anos, bem como não emprega menores de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre, conforme disposto no Artigo 7º, Inciso XXXIII, da Constituição Federal.

1.13 Declaração expressa, sob as penas da lei, de que a(o) interessada(o), em sendo vencedor(a) do certame, para fins de contratação, compromete-se a efetiva comprovação do(s) documento(s) abaixo relacionado(s):

1.13.1 Comprovação da certificação técnica para instalação e configuração, de pelo menos 01 (um) profissional da solução ofertada;

1.13.2 O(s) documento(s) acima relacionado(s) deverá(ao) ser entregue(s) junto à Gerência de Compras e Licitações I, em **02 (dois) dias úteis** em que declarada vencedora do certame.

1.13.3 A não apresentação ou apresentação incompleta ou defeituosa acarretará em inabilitação, impedirá a contratação e sujeitará a empresa às sanções legais pertinentes.

1.13.4 **O(s) documento(s) poderá(ao) ser apresentado(s) no original, ou por meio de cópias autenticadas (a critério do(a) licitante), ou por meio de cópia simples, caso em que o interessado deverá exibir o original para comparação e atestação da autenticidade pelos membros da COPEL-I, na própria sessão, ou por meio de autenticação digital, ou por publicação oficial.**

ANEXO III
DESCRIÇÃO DOS DOCUMENTOS DE HABILITAÇÃO

1.13.5 Caso a vencedora do certame seja portadora da documentação acima arrolada na própria sessão pública e ali mesmo queira apresentá-la, não será necessária a concessão do prazo previsto de **02 (dois) dias úteis;**

1.13.6 Se houver condições de análise na sessão pública e a documentação acima arrolada for reprovada, a Administração dará a mesma oportunidade aos subsequentes melhores colocados, observando-se o constante nos subitens 1.13.2. e 1.13.5.

ANEXO IV
MODELO DE PROPOSTA COMERCIAL

1. PROPOSTA COMERCIAL

1.1. A Proposta Comercial de cada Licitante, além de atender ao disposto nos subitens 9.4 e 9.5 do Edital, deverá conter, no mínimo, as seguintes informações:

1.1.1. Número do Edital de Pregão Presencial;

1.1.2. Código de Registro da Licitante no Cadastro de Fornecedores da PMSA, caso seja cadastrada;

1.1.3. Razão Social completa;

1.1.4. Endereço completo (Logradouro, Número, Bairro, CEP, Cidade, Estado);

1.1.5. Contatos (Telefone, Fax, E-mail);

1.1.6. Número do CNPJ(MF);

1.1.7. Número da Inscrição Estadual;

1.1.8. Dados Bancários Completos (Banco, nº da Agência e respectivo Dígito, nº da Conta Corrente e respectivo Dígito), conforme subitem 5.1.1 do Anexo I;

1.1.9. Item(ns) do(s) material(is) a ser(em) adquirido(s) e/ou serviço(s) a ser(em) prestado(s), conforme descrito no Anexo II;

1.1.10. Especificação do(s) material(is) a ser(em) adquirido(s) e/ou serviço(s) a ser(em) prestado(s), conforme descrito no Anexo II;

1.1.11. Marca / Fabricante do(s) material(is) a ser(em) adquirido(s) do(s) item(ns) especificado(s). Será aceita a indicação / menção de apenas uma Marca / Fabricante por material;

1.1.12. Quantidade de cada item especificado;

1.1.13. Unidade de cada item especificado;

1.1.14. Valor unitário de cada item, expresso em Reais;

1.1.15. Valor total de cada item, expresso em Reais;

1.1.16. Valor total da Proposta Comercial;

1.1.17. Declaração expressa de que a Licitante está sujeita e aceita todas e quaisquer exigências estabelecidas no presente Edital de Pregão Presencial e seus respectivos Anexos, inclusive normas, prazos e garantia, quando houver;

1.1.18. Data da Proposta Comercial (Dia /Mês /Ano);

1.1.19. Validade da Proposta Comercial : 60 (sessenta) dias

1.1.20. Assinatura do representante legal da Licitante;

1.1.21. Nome do representante legal da Licitante;

1.1.22. Número da Cédula de Identidade do representante legal da Licitante;

1.1.23. Cargo do representante legal da Licitante.

1.2. Segue modelo de Proposta Comercial para fornecimento de materiais e/ou prestação de serviços que, facultativamente, poderá ser utilizada pela Licitante:

ANEXO IV
MODELO DE PROPOSTA COMERCIAL

À
PREFEITURA MUNICIPAL DE SANTO ANDRÉ
DEPARTAMENTO DE LICITAÇÕES

Cadastro de Fornecedor PMSA – Código da Empresa :		
Edital nº :	Data / Abertura :	Horário :
Razão Social :		
Endereço :		CEP : 00000-000
Bairro :	Cidade / Estado :	
Telefone(s) : (11) 0000-0000	Fax : (11) 0000-0000	
CNPJ (MF) : 00.000.000/0000-00	Inscrição Estadual : 000.000.000.000	
E-mail :		
Banco :	Agência :	Conta Corrente :

ITEM	QTDE	UND	DESCRIÇÃO	VALOR UNITÁRIO – R$	VALOR TOTAL – R$
01	53	UN.	Solução de Segurança para Servidores Virtuais – Software Gerenciamento, licenciamento, Implantação e Garantia Técnica de 36 meses.		
02	3.500	UN.	Solução de Proteção para Endpoints, Implantação e Garantia Técnica de 36 meses.		
03	2.500	UN.	Solução de Proteção Anti-Sapm, Anti-Spam para Exchange, Implantação e Garantia Técnica de 36 meses.		
04	10	DIAS	Instalação, configuração e acompanhamento operacional		
05	3	UN.	Treinamento on site da solução contratada.		
VALOR GLOBAL DA PROPOSTA COMERCIAL					**XXXXX (POR EXTENSO)**

Declaramos expressamente que nos sujeitamos e aceitamos todas e quaisquer exigências estabelecidas no presente Edital de Pregão Presencial e seus respectivos Anexos, inclusive normas, prazos e garantia, quando houver, tendo a presente proposta a validade de 60 (sessenta) dias.

_____ , ____ de _____ de 2.019

_____

Nome :

RG :

Cargo :

ANEXO V
MODELO DE TERMO DE CREDENCIAMENTO

TERMO DE CREDENCIAMENTO

A Licitante _____ , com sede na _____ , inscrita no CNPJ(MF) sob o nº _____ , representada legalmente neste ato pelo(a) Sr.(a) _____ , (Cargo) _____ , portador(a) da Cédula de Identidade RG nº _____ , e inscrito(a) no CPF sob o nº _____ , **CREDENCIA** o(a) Sr.(a) _____ , portador(a) da Cédula de Identidade RG nº _____ , e inscrito(a) no CPF sob o nº _____ , para ***representá-la*** perante a **PREFEITURA MUNICIPAL DE SANTO ANDRÉ** no Pregão Presencial referente ao Edital nº _____ , podendo formular lances verbais e praticar todos e quaisquer atos inerentes a sessão pública, inclusive interpor e desistir de recursos em todas as etapas da mesma.

_____ , ____ de _____ de 2.019

_____

Assinatura

ANEXO VI
MODELO DE DECLARAÇÃO DE CUMPRIMENTOS DE REQUISITOS HABILITATÓRIOS

DECLARAÇÃO DE CUMPRIMENTO DE REQUISITOS HABILITATÓRIOS

A Licitante _____ , com sede na _____ , inscrita no CNPJ(MF) sob o nº _____ , representada legalmente neste ato pelo(a) Sr.(a) _____ , (Cargo) _____ , portador(a) da Cédula de Identidade RG nº _____ , e inscrito(a) no CPF sob o nº _____ , ***declara***, sob as penas da Lei, estar cumprindo plenamente os requisitos de habilitação através dos documentos contidos no envelope "B – DOCUMENTOS DE HABILITAÇÃO", conforme especificações constantes do Edital de Pregão Presencial nº _____ e seus Anexos.

A Licitante acima qualificada também declara que, por se enquadrar como "Microempresa (ME)" ou "Empresa de Pequeno Porte (EPP)", conforme declaração apresentada nos termos do Anexo VII deste Edital, utilizar-se-á dos benefícios previstos na Lei Complementar nº 123/06 e alterações posteriores e na Lei Municipal nº 9.487/13.

_____ , ____ de _____ de 2.019

_____

Assinatura

Obs.: O último parágrafo destacado em "negrito itálico" deverá ser utilizado apenas quando se tratar de "Microempresa (ME) ou "Empresa de Pequeno Porte (EPP)", nos termos da Lei Complementar nº 123/06 e alterações posteriores.

ANEXO VII
MODELO DE DECLARAÇÃO DE PEQUENA EMPRESA

DECLARAÇÃO DE MICROEMPRESA (ME) OU EMPRESA DE PEQUENO PORTE (EPP)

Referente Edital de Pregão Presencial nº _____

A Microempresa (ME) **ou** Empresa de Pequeno Porte (EPP) _____ , com sede na _____ , inscrita no CNPJ(MF) sob o nº _____ , representada legalmente neste ato pelo(a) Sr.(a) _____ , (Cargo) _____ , portador(a) da Cédula de Identidade RG nº _____ , e inscrito(a) no CPF sob o nº _____ , ***declara***, para os devidos fins e sob as penas da Lei, que sua receita bruta anual não excederá, neste exercício, o limite fixado no artigo 3º da Lei Complementar 123/06 e na Lei Municipal nº 9.487/13, e que não se enquadra em qualquer das hipóteses de exclusão relacionadas na mesma legislação.

_____ , ____ de _____ de 2.019

_____

Assinatura

ANEXO VIII
MODELO DE DECLARAÇÃO DO LICITANTE

DECLARAÇÃO DO LICITANTE

Referente Edital de Pregão Presencial nº _____

A Licitante _____ , com sede na _____ , inscrita no CNPJ(MF) sob o nº _____ , representada legalmente neste ato pelo(a) Sr.(a) _____ , (Cargo) _____ , portador(a) da Cédula de Identidade RG nº _____ , e inscrito(a) no CPF sob o nº _____ , **declara,** expressamente, sob as penas da lei, que:

A) Não se encontra sujeito aos efeitos de declaração de inidoneidade para licitar ou contratar com a Administração Pública, nos termos do artigo 87, IV, da Lei nº 8.666/93, firmada em quaisquer das esferas da Federação, ou a qualquer outro título;

B) Não existe qualquer fato impeditivo à sua habilitação ou eventual contratação com o Poder Público, por atender integralmente às condições exigidas para sua habilitação, nos termos previstos na legislação em vigor e no presente Edital;

C) Não descumpre as proibições quanto à utilização de mão de obra infantil, menor de 16 (dezesseis) anos, bem como não emprega menores de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre, conforme disposto no Artigo 7o, Inciso XXXIII, da Constituição Federal.

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

(Observação: Em caso afirmativo, assinalar a ressalva acima.)

_____ , ____ de _____ de 2.019

_____

Assinatura

ANEXO IX
MINUTA DE CONTRATO

CONTRATO ENTRE A PREFEITURA MUNICIPAL DE SANTO ANDRÉ E A EMPRESA _____, PARA FORNECIMENTO DE SOLUÇÃO DE ANTIVÍRUS COM LICENÇAS DO PRODUTO, IMPLEMENTAÇÃO, TREINAMENTO, PRESTAÇÃO DE SERVIÇOS DE MANUTENÇÃO E SUPORTE TÉCNICO PARA TODA SOLUÇÃO OFERTADA.

I - PREÂMBULO

1. **CONTRATANTES** - De um lado, a Prefeitura Municipal de Santo André, doravante denominada simplesmente "CONTRATANTE", representada pelo(a) _____, com fundamento no artigo 11 do Decreto Municipal n° 16.653/15, e, de outro lado, a empresa _____., inscrita no CNPJ/MF sob o nº _____, estabelecida na Rua _____ – Bairro: _____ – _____ – ____ – _____, representada por _____, portador do RG nº _____ e do CPF:_____, a seguir denominada "CONTRATADA", ficando as partes subordinadas às disposições da Lei Federal nº 10.520/02 e, subsidiariamente, às da Lei Federal nº 8.666/93, Lei Complementar nº 123/06, Leis Municipais nºs 9487/13 e 9940/17 e dos Decretos Municipais nºs 15.926/09, 15.929/09, 16.653/15 e 17.030/18 naquilo em que forem aplicáveis às condições constantes deste contrato.

2. **FUNDAMENTO DO CONTRATO** - Este contrato decorre da homologação efetuada pelo(a) Secretário(a) de Assuntos Jurídicos do Pregão Presencial, a que se refere o Edital nº_____, o qual se acha juntado ao **Processo Administrativo nº 31833/2018.**

II - DESCRIÇÃO E CONDIÇÕES

1. **OBJETO DO CONTRATO** - A "CONTRATADA" obriga-se a fornecer solução de antivírus com licenças do produto, implementação, treinamento, prestação de serviços de manutenção e suporte técnico para toda solução ofertada.

2. **LOCAL DA PRESTAÇÃO DOS SERVIÇOS:** Paço Municipal, Praça IV Centenário, nº 01 – Centro – Santo André no Prédio do Executivo – 2º Andar.

3. **CONDIÇÕES** – Os serviços deverão ser prestados de acordo com as especificações constantes deste contrato e na forma prevista na proposta da “CONTRATADA”, dentro dos prazos estabelecidos, sob pena de incorrer a mesma nas sanções nele previstas.

4. **RESPONSABILIDADES DA “CONTRATADA**” - A "CONTRATADA" assume integral responsabilidade pelo pagamento dos encargos fiscais, comerciais, trabalhistas, previdenciários e outros que decorram dos compromissos assumidos neste contrato, não se obrigando a "CONTRATANTE" a fazer-lhe restituição ou reembolso de qualquer valor despendido com estes pagamentos.

   4.1. A ”CONTRATADA” compromete-se, para fins de execução do objeto deste contrato, a não descumprir as proibições quanto à utilização da mão de obra infantil de menores de 16 anos, bem como não empregar menores de 18 anos em trabalho noturno, perigoso ou insalubre, conforme disposto no artigo 7º, inciso XXXIII, da Constituição Federal, sob pena de rescisão automática e imediata do ajuste.

   4.2. Será permitida a subcontratação dos serviços descritos no item 4.2 (suporte) e seus subitens nos termos do artigo 72 da Lei 8.666/93.

      4.2.1. Nenhuma subcontratação isentará a “CONTRATADA” de quaisquer de suas responsabilidades ou obrigações deste Contrato, sendo a mesma a responsável perante a CONTRATANTE por todos os atos e omissões das subcontratadas, bem como por atos de pessoas direta ou indiretamente por elas empregadas.

ANEXO IX
MINUTA DE CONTRATO

4.3. SUPORTE

4.3.1. A Empresa Contratada deverá prover garantia, manutenção e suporte para a solução ofertada (todos os componentes) por 36 (trinta e seis) meses a partir da assinatura do contrato, com atendimento para abertura de chamados em regime 24x7 e efetiva solução de problemas num prazo máximo de 08 (oito) horas corridas após a abertura dos chamados;
4.3.2. Abertura de chamados poderá ser realizada por e-mail, sistema on-line ou telefone;
4.3.3. A garantia deve incluir, sem custo adicional, durante o período de 36 meses a contar da data de assinatura do contrato;
4.3.4. Atualização preventiva e corretiva dos softwares fornecidos;
4.3.5. Orientação remota, por telefone, e-mail e páginas na internet, sobre operação dos equipamentos e suporte para configuração.

4.4. DAS OBRIGAÇÕES DA CONTRATADA

4.4.1. Além dos encargos de ordem legal e os demais assumidos em outros itens do Contrato e nos documentos que o integram, sem alteração do preço estipulado, obriga-se, ainda, a Contratada a:

4.4.1.1. Executar o fornecimento do objeto do Contrato, em conformidade com a Especificação Técnica e demais exigências técnicas que a tornaram vencedora no processo licitatório e, ainda, com as instruções recebidas da fiscalização;
4.4.1.2. Fornecer, a qualquer momento, todas as informações pertinentes ao objeto do Contrato, que a Contratante julgue necessárias conhecer ou analisar;
4.4.1.3. Manter, durante a vigência do presente Instrumento, as mesmas condições que propiciaram a sua habilitação e a classificação no processo licitatório;
4.4.1.4. Pagar os tributos, taxas e encargos de qualquer natureza de sua responsabilidade em decorrência do Contrato;
4.4.1.5. Manter atualizadas, junto aos órgãos competentes, as inscrições/registros específicos que a legitime a exercer os serviços objeto do Contrato e seus Anexos;
4.4.1.6. Responsabilizar-se pelo deslocamento dos seus técnicos a Prefeitura Municipal de Santo André, para execução dos serviços contratados, assim como por todas as demais despesas;
4.4.1.7. Realizar todos os serviços de configuração e testes necessários à perfeita utilização dos softwares contratados;
4.4.1.8. Alocar um responsável técnico, que deverá assumir, pessoal e diretamente, a gestão administrativa do contrato, a execução e coordenação dos serviços;
4.4.1.9. Não efetuar, sob nenhum pretexto, a transferência de qualquer responsabilidade para outras entidades, seja fabricante, técnicos, subempreiteiros etc., sem a anuência expressa e por escrito do Departamento de Tecnologia e Inovação da PREFEITURA MUNICIPAL DE SANTO ANDRÉ;
4.4.1.10. Responsabilizar-se pelo credenciamento e descredenciamento de acesso às dependências da PREFEITURA MUNICIPAL DE SANTO ANDRÉ;
4.4.1.11. Atender às instruções do Departamento de Tecnologia e Inovação da

ANEXO IX
MINUTA DE CONTRATO

PREFEITURA MUNICIPAL DE SANTO ANDRÉ quanto à execução e aos horários de realização dos serviços, permanência e circulação de pessoas nas dependências da PREFEITURA MUNICIPAL DE SANTO ANDRÉ;

4.4.1.12. Responsabilizar-se por danos causados ao patrimônio da PREFEITURA MUNICIPAL DE SANTO ANDRÉ, ou de terceiros, ocasionados por seus empregados, em virtude de dolo ou culpa, durante a execução do objeto contratado;

4.4.2. À Contratada é vedado prestar informações a terceiros sobre a natureza ou andamento do fornecimento, objeto do Contrato, ou divulgá-los através da imprensa escrita, falada, televisada e/ou outro meio qualquer de divulgação pública, salvo autorização expressa da Contratante.

5. DAS OBRIGAÇÕES DA CONTRATANTE

5.1. Efetuar à Contratada os pagamentos nas condições estabelecidas neste instrumento;
5.2. Fornecer, quando detiver, outras informações que se fizerem necessárias a realização dos serviços contratados;
5.3. Rejeitar o(s) softwares entregues se estiverem em desacordo com as especificações exigidas;
5.4. Certificar as faturas correspondentes e encaminhá-las ao Órgão Financeiro após constatar o fiel cumprimento das obrigações contratuais;
5.5. Exigir da Contratada o cumprimento rigoroso das obrigações assumidas;
5.6. Sustar o pagamento de faturas no caso de inobservância, pela Contratada, de condições contratuais;
5.7. Aplicar, nos termos contratuais, multa(s) à Contratada dando-lhe ciência do ato, por escrito, e proceder à dedução da multa de qualquer crédito da Contratada;
5.8. Emitir Termo de Recebimento Definitivo.

6. **PREPOSTO** - Fica designado pela "CONTRATANTE" _____, como seu "preposto", a quem caberá a responsabilidade pelo acompanhamento e fiscalização da regular execução deste contrato.

III – PREÇO, CONDIÇÕES DE PAGAMENTO E REAJUSTAMENTO

1. **PREÇO** - A "CONTRATANTE" remunerará à "CONTRATADA" o valor global mensal de _____ (_____).

2. **CONDIÇÕES DE PAGAMENTO** – Conforme edital.

3. **REAJUSTAMENTO** – Conforme edital.

IV - PRAZOS

1. **PRAZO DE DURAÇÃO** – Conforme edital.

2. **PRAZO PARA INÍCIO** – No dia útil seguinte ao da assinatura do Contrato.

ANEXO IX
MINUTA DE CONTRATO

V – VALOR E DOTAÇÃO

1. **VALOR –** O valor total anual deste contrato é de _____ (_____).

2. **DOTAÇÃO** - As despesas com a execução deste contrato onerarão as dotações próprias consignadas sob n°. 40.70.339040.10.122.0034.2.096.01; 60.10.339040.12.365.0061.2.176.01 e 34.30.339040.04.122.0022.2.067.01.

VI - RESCISÃO CONTRATUAL

1. A inexecução total ou parcial do contrato ensejará sua rescisão, nos casos enumerados no artigo 78, no modo previsto pelo artigo 79, com as conseqüências previstas no artigo 80, todos da Lei Federal 8.666/93.

VII - DAS SANÇÕES ADMINISTRATIVAS

1. São aplicáveis as sanções previstas na Lei 10.520/02 e, subsidiariamente, no capítulo IV da Lei federal nº 8.666/93, com as alterações introduzidas pela Lei federal nº 8.883/94 e demais normas pertinentes a seguir:

1.12. Advertência;
1.13. Suspensão temporária de participar em licitação e impedimento de contratar com a Administração, nos termos indicados no subitem 12.1.
1.14. Declaração de inidoneidade para licitar ou contratar com a Administração Pública.
1.15. Multa

2. A multa pela recusa da adjudicatária em assinar o termo de contrato ou em retirar o instrumento equivalente dentro do prazo estabelecido no edital será de 10% (dez por cento) do valor da proposta, sem prejuízo da aplicação da pena de suspensão temporária do direito de licitar e contratar com a PMSA, pelo prazo de até 5 (cinco) anos.

3. Multa por atraso: 1% (um por cento) por dia sobre o valor da parcela em atraso, até o limite de 10% (dez por cento), podendo a Prefeitura a partir do 10º dia considerar rescindido o contrato, sem prejuízo das demais sanções cabíveis.

3.12. O prazo para pagamento das multas moratórias será de 3 (três) dias úteis a contar da intimação da contratada. A critério da Administração e sendo possível, o valor devido será descontado dos pagamento a serem efetuados pela Administração, garantida a ampla defesa, nos termos da lei.

4. Multa por inexecução parcial do contrato: 10% (dez por cento) sobre o valor da parcela inexecutada.

5. Multa por inexecução total do contrato: 10% (dez por cento) sobre o valor total do contrato.

6. Multa de 10% (dez por cento), por descumprimento de quaisquer das obrigações decorrentes do ajuste, que não estejam previstas nos itens acima, a qual incidirá sobre o valor total do contrato.

7. Perda da garantia oferecida, se houver, em caso de culpa pela rescisão contratual.

8. As penalidades são independentes e a aplicação de uma não exclui a das outras, quando cabíveis.

ANEXO IX
MINUTA DE CONTRATO

9. Constatada a inexecução contratual ou a hipótese do item 2, será a contratada intimada da intenção da Prefeitura quanto à aplicação da penalidade, concedendo-se prazo para interposição de defesa prévia, nos termos do art. 87, §2º e §3º da Lei 8.666/93.

10. Não sendo apresentada a defesa prévia pela contratada ou havendo o indeferimento da mesma quando interposta, a Prefeitura providenciará a notificação da contratada quanto à aplicação da penalidade, abrindo-se prazo para interposição de recurso administrativo, nos termos do art. 109, I, "f" da Lei 8.666/93.

11. Decorridas as fases anteriores, o prazo para pagamento das multas será de 03 (três) dias úteis a contar da intimação da contratada. A critério da Administração e sendo possível, o valor devido será descontado da eventual garantia prestada ou, sendo esta insuficiente, será descontado dos pagamentos devidos pela Administração. Não havendo prestação de garantia, o valor das multas será diretamente descontado do crédito que porventura haja.

11.12. Não havendo tais possibilidades, o valor será inscrito em dívida ativa, sujeitando a devedora a processo executivo.

12. Sem prejuízo da aplicação de outras penalidades cabíveis, a ocorrência das hipóteses a seguir listadas, acarretará a aplicação da penalidade especificada.

12.12. A empresa que, convocada dentro do prazo de validade de sua proposta, não celebrar o Contrato ou deixar de retirar o instrumento equivalente, deixar de entregar documentação exigida para a sessão pública ou apresentar documentação falsa, ensejar o retardamento da execução de seu objeto, não mantiver a proposta, falhar ou fraudar na execução do contrato, comportar-se de modo inidôneo ou cometer fraude fiscal, ficará impedida de licitar e contratar com a Administração Municipal e será descredenciado do Cadastro de Fornecedores desta PMSA, pelo prazo de até 5 (cinco) anos, sem prejuízo das multas previstas em Edital, no Contrato e nas demais cominações legais.

VIII - DISPOSIÇÕES GERAIS

1. **CONDIÇÕES INTEGRANTES** - Ficam fazendo parte integrante deste, independentemente de transcrições, o edital que regeu a licitação de que o mesmo decorre e a proposta da "CONTRATADA", essa somente naquilo em que não colidir com as disposições legais.

2. **ACRÉSCIMOS OU SUPRESSÕES** – A "CONTRATADA" ficará obrigada a aceitar, nas mesmas condições contratuais, acréscimos ou supressões que se fizerem necessários, na prestação de serviços, até o limite de 25% (vinte e cinco por cento) do valor inicialmente contratado.

3. **MANTENÇA DAS CONDIÇÕES HABILITATÓRIAS** - A "CONTRATADA" obriga-se a manter, durante toda a execução contratual, em compatibilidade com as obrigações por elas assumidas, todas as condições exigidas nos aspectos jurídico e de qualificação técnica, econômica e financeira, bem como de regularidade perante o Fisco e a Justiça do Trabalho, quando das respectivas habilitações. A regularidade dos encargos sociais será comprovada mediante a apresentação da "Certidão Negativa, ou Positiva com efeitos de Negativa, de Débitos relativos a Tributos Federais e à Dívida Ativa da União", expedida pela Secretaria da Receita Federal do Brasil, nos termos da Portaria Conjunta RFB/PGFN nº 1.751/14, do Certificado de Regularidade do FGTS – CRF expedida pela Caixa Econômica Federal e da Certidão Negativa/Positiva com efeito de Negativa de Débitos Trabalhistas perante a Justiça do Trabalho, na época da apresentação das notas fiscais e pagamento.

4. **FORO** - As partes elegem, em comum acordo, o Foro desta Comarca de Santo André como seu domicílio legal, para qualquer procedimento relacionado com o descumprimento deste contrato.

ANEXO IX
MINUTA DE CONTRATO

Por haverem assim ajustado, firmaram este compromisso, registrado e digitado na Gerência de Contratos, do qual foi extraída 01 (uma) via de idêntico teor, presentes as testemunhas abaixo indicadas.

Eu, _____, _____, _____, digitei-o, e eu, _____, _____, Gerente de Contratos, conferi e o subscrevo.

Santo André, ___ de _____ de 20__

_____
SECRETÁRIO(A)

_____
EMPRESA

TESTEMUNHAS:

1. - _____

2. - _____

ANEXO X
TERMO DE CIÊNCIA E DE NOTIFICAÇÃO

TERMO DE CIÊNCIA E DE NOTIFICAÇÃO

CONTRATANTE: PREFEITURA MUNICIPAL DE SANTO ANDRÉ

CONTRATADO: _____

CONTRATO Nº (DE ORIGEM):_____

OBJETO: _____

ADVOGADO(S) / Nº OAB: (*) _____

Pelo presente TERMO, nós, abaixo identificados:

1. Estamos CIENTES de que:

a) o ajuste acima referido estará sujeito a análise e julgamento pelo Tribunal de Contas do Estado de São Paulo, cujo trâmite processual ocorrerá pelo sistema eletrônico;

b) poderemos ter acesso ao processo, tendo vista e extraindo cópias das manifestações de interesse, Despachos e Decisões, mediante regular cadastramento no Sistema de Processo Eletrônico, conforme dados abaixo indicados, em consonância com o estabelecido na Resolução nº 01/2011 do TCESP;

c) além de disponíveis no processo eletrônico, todos os Despachos e Decisões que vierem a ser tomados, relativamente ao aludido processo, serão publicados no Diário Oficial do Estado, Caderno do Poder Legislativo, parte do Tribunal de Contas do Estado de São Paulo, em conformidade com o artigo 90 da Lei Complementar nº 709, de 14 de janeiro de 1993, iniciando-se, a partir de então, a contagem dos prazos processuais, conforme regras do Código de Processo Civil;

d) Qualquer alteração de endereço – residencial ou eletrônico – ou telefones de contato deverá ser comunicada pelo interessado, peticionando no processo.

2. Damo-nos por NOTIFICADOS para:

a) O acompanhamento dos atos do processo até seu julgamento final e consequente publicação;

b) Se for o caso e de nosso interesse, nos prazos e nas formas legais e regimentais, exercer o direito de defesa, interpor recursos e o que mais couber.

Local e Data: _____

GESTOR DO ÓRGÃO/ENTIDADE:
Nome: _____
Cargo:_____
CPF: _____ RG: _____
Data de Nascimento: ____/____/_____
Endereço residencial completo: _____
E-mail institucional _____
E-mail pessoal:_____
Telefone(s):_____
Assinatura:_____

ANEXO X
TERMO DE CIÊNCIA E DE NOTIFICAÇÃO

Responsáveis que assinaram o ajuste:

Pelo CONTRATANTE:

Nome: _____

Cargo:_____

CPF: _____ RG: _____

Data de Nascimento: ____/____/_____

Endereço residencial completo: _____

E-mail institucional _____

E-mail pessoal:_____

Telefone(s):_____

Assinatura: _____

Pela CONTRATADA:

Nome: _____

Cargo:_____

CPF: _____ RG: _____

Data de Nascimento: ____/____/_____

Endereço residencial completo: _____

E-mail institucional _____

E-mail pessoal:_____

Telefone(s):_____

Assinatura: _____

Advogado:

(*) Facultativo. Indicar quando já constituído, informando, inclusive, o endereço eletrônico