PREGÃO ELETRÔNICO SESC/DR-PE Nº 006/2026 - REGISTRO DE PREÇOS
Licitação número 1086030 (www.licitacoes-e.com.br)

E D I T A L

O SESC - SERVIÇO SOCIAL DO COMÉRCIO, Departamento Regional em Pernambuco, entidade de direito privado, sem fins lucrativos, comunica a realização de licitação, na modalidade **PREGÃO ELETRÔNICO,** do tipo **MENOR PREÇO, POR LOTE, PARA REGISTRO DE PREÇOS**, com modo de disputa "aberto", conforme condições especificadas neste edital e seus anexos.

A presente licitação é regida pela **Resolução Sesc Nº 1.593/2024**, de 02/05/2024, do Conselho Nacional do Serviço Social do Comércio, e pelas disposições deste instrumento convocatório e de seus anexos.

O processo licitatório será conduzido pela Comissão de Licitação e pelo Pregoeiro com a equipe de apoio, todos designados, conforme **Portaria Normativa SESC/PE Nº 262/2024**, de 20 de maio de 2024.

Os documentos a serem encaminhados **APÓS A SESSÃO PÚBLICA DE LANCES** — **proposta comercial ajustada, documentação de habilitação** e, quando houver, **catálogos** — deverão ser enviados **exclusivamente por e-mail** para **licitacao@sescpe.com.br**, **não devendo ser anexados** ao sistema eletrônico do **Banco do Brasil S/A (Licitações-e)**, ainda que este assim indique.

A Sessão Pública de Lances será realizada, via internet, às **14 horas do dia 28 de janeiro de 2026**, horário de Brasília-DF, no endereço eletrônico **www.licitacoes-e.com.br** do Banco do Brasil S/A., sob o nome "Sesc – Departamento Regional em Pernambuco", **licitação número 1086030.**

Os interessados poderão inserir propostas eletrônicas no seguinte período: **a partir das 08 horas do dia 26 de janeiro de 2026 até as 10 horas do dia 28 de janeiro de 2026**.

1. DO OBJETO

1.1 – O presente Pregão Eletrônico destina-se ao **REGISTRO DE PREÇO, PARA RENOVAÇÃO DE LICENÇAS DE ANTIVÍRUS, KASPERSKY ENDPOINT SECURITY, A FIM DE SUPRIR AS NECESSIDADES DO PARQUE TECNOLÓGICO DO SESC-DR/PE, COM UMA SOLUÇÃO DE SOFTWARE INTEGRADO DE SEGURANÇA E PROTEÇÃO CONTRA SPAM DE E-MAIL, VAZAMENTOS DE DADOS, TENTATIVAS DE PHISHING E HACKING, ANTIMALWARE - VÍRUS, RANSOMWARE, CAVALOS DE TRÓIA, ROOTKITS, BACKDOORS, COM CRIPTOGRAFIA DE DADOS, SEGURANÇA MÓVEL, SEGURANÇA DA PLATAFORMA OFFICE 365, GERENCIAMENTO DE DISPOSITIVOS MÓVEIS, GERENCIAMENTO DE SISTEMAS E TREINAMENTO DE EQUIPE TÉCNICA SESC/DR-PE, COM ATUALIZAÇÕES PARA 36 (TRINTA E SEIS) MESES, SERVIÇO DE IMPLANTAÇÃO E MANUTENÇÃO, A FIM DE GARANTIR A PROTEÇÃO LÓGICA DOS COMPUTADORES, SERVIDORES FÍSICOS E VIRTUAIS, MS OFFICE 365, BEM COMO, EQUIPAMENTOS MÓVEIS (LAPTOPS, SMARTPHONES, TABLETS) INTEGRADOS A REDE LÓGICA DE DADOS DO SESC-DR/PE E DEMAIS UNIDADES DA INSTITUIÇÃO, CONTRA A ENTRADA E ATUAÇÃO DE MALWARES E PROGRAMAS MALICIOSOS** em conformidade com as especificações técnicas descritas no **TERMO DE**

SESC – Serviço Social do Comércio | Departamento Regional em Pernambuco | www.sescpe.org.br
Casa do Comércio/Edifício Josias Albuquerque | Avenida Visconde de Suassuna, nº 265, Santo Amaro - Recife-PE.
CEP: 50.050-540 TEL + 55 81 3216 1739

REFERÊNCIA (ANEXO I), observadas as demais condições estabelecidas neste instrumento convocatório e seus anexos.

1.2 – Sendo Registro de Preços, o Sesc/DR-PE não se obriga a adquirir o objeto desta licitação, podendo realizar contratação com terceiros, sempre que se mostre mais vantajosa para a Entidade.

1.2.1 – **O quantitativo total constante no TERMO DE REFERÊNCIA (ANEXO I) deste edital é estimado e representa as previsões do Sesc/DR-PE durante o prazo de 12 (doze) meses.**

1.3 – **O licitante vencedor deverá permanecer em condições de fornecer o objeto dentro dos prazos definidos pelo Sesc/DR-PE, durante o período de validade da Ata de Registro de Preços, não cabendo à empresa nenhum adicional além do que foi previsto inicialmente. Estes custos deverão constar do valor da proposta apresentada pela empresa.**

1.4 – A qualquer tempo, durante o período de vigência, os preços registrados poderão ser revistos em decorrência de eventual redução dos preços praticados no mercado ou de fato que eleve o custo dos serviços ou bens registrados, cabendo ao Sesc/DR-PE convocar a empresa fornecedora para promover as negociações necessárias, até que se defina o novo valor, conforme o entendimento da legislação vigente.

2. DAS CONDIÇÕES DE ENTREGA

2.1 – A empresa signatária da Ata de Registro de Preços se compromete a fornecer os produtos em conformidade com as especificações e condições descritas no TERMO DE REFERÊNCIA (ANEXO I) deste edital, pelos preços registrados na Ata de Registro de Preços, durante o período de sua vigência.

2.2 – A desobediência aos prazos e condições estabelecidos acarretará a aplicação, ao licitante vencedor, das sanções estabelecidas neste edital e na Ata de Registro de Preços ou documento equivalente (Pedido de Compra), no que couber.

2.3 – É facultado ao Sesc/DR-PE, quando o licitante convocado não aceitar realizar a entrega do(s) produto(s) no prazo e condições estabelecidos, convocar o(s) licitante(s) remanescente(s), na ordem de classificação, para fazê-lo em igual prazo e nas mesmas condições propostas pelo primeiro classificado, ou cancelar a Ata de Registro de Preços, independentemente das cominações que à empresa serão impostas.

2.4 – **Decorrido o prazo de validade de 12 (doze) meses, sem convocação para contratação, ficam os licitantes classificados com preços registrados liberados dos compromissos assumidos.**

3. DAS CONDIÇÕES DE PARTICIPAÇÃO

3.1 – Poderão participar do certame os interessados que atenderem a todas as condições estabelecidas neste edital e seus anexos.

SESC – Serviço Social do Comércio | Departamento Regional em Pernambuco | www.sescpe.org.br
Casa do Comércio/Edifício Josias Albuquerque | Avenida Visconde de Suassuna, nº 265, Santo Amaro - Recife-PE.
CEP: 50.050-540 TEL + 55 81 3216 1739

3.2 – Estarão impedidas de participar desta licitação pessoas jurídicas que:

a) Estejam sob decretação de falência, concurso de credores, dissolução, liquidação judicial ou extrajudicial; e

b) Estejam suspensas de licitar com o Sesc, Departamento Regional em Pernambuco.

3.3 – CREDENCIAMENTO

3.3.1 – Para participar da presente licitação os interessados deverão estar credenciados no provedor do sistema *"Licitações-e"*, do Banco do Brasil S/A., na página **www.licitacoes-e.com.br**.

3.3.2 – O credenciamento dar-se-á pela atribuição de chaves de identificação e de senhas individuais a serem fornecidas pelo provedor do sistema quando do credenciamento.

3.3.3 – Maiores informações poderão ser obtidas em qualquer agência do **Banco do Brasil S/A.** ou pelo telefone **4004-0001** (Capitais e Regiões Metropolitanas) e **0800-7290001** (demais localidades).

3.3.4 – O uso da senha de acesso pelo licitante é de sua inteira e exclusiva responsabilidade, incluindo qualquer transação efetuada diretamente ou por seu representante, não cabendo ao provedor do sistema, ou ao Sesc/DR-PE, responsabilidades por eventuais danos decorrentes do uso indevido da senha, ainda que por terceiros.

3.3.5 – O credenciamento da empresa e de seu representante legal, junto ao sistema Eletrônico, implica responsabilidade legal pelos atos praticados, e na presunção de capacidade técnica para realização das transações inerentes ao Pregão Eletrônico.

3.4 – CONEXÃO COM O SISTEMA

3.4.1 – A participação no Pregão dar-se-á por meio da conexão do licitante com o sistema eletrônico anteriormente citado, pela digitação de sua senha (nos termos do subitem 3.3.1 deste edital) e o subsequente encaminhamento da proposta, **exclusivamente**, por meio do referido sistema eletrônico, observados datas e horários limites, estabelecidos neste edital.

3.4.2 – O encaminhamento da proposta pressupõe o pleno conhecimento e atendimento às exigências constantes neste edital e seus anexos. A empresa será responsável pelas transações que forem efetuadas em seu nome, no sistema eletrônico, assumindo como firmes e verdadeiras suas propostas e lances.

3.4.3 – Caberá, ainda, ao licitante, acompanhar o andamento do Pregão, observando as informações fornecidas pelo sistema eletrônico, ficando a mesma responsável pelo ônus decorrente da perda de negócios diante da inobservância de mensagens ali inseridas durante a sessão pública, ou de sua desconexão.

3.4.4 – No caso de desconexão com o Pregoeiro(a), no decorrer da etapa competitiva do Pregão, o sistema eletrônico poderá permanecer acessível aos licitantes para a recepção dos lances.

3.4.4.1 – O Pregoeiro(a), quando possível, dará continuidade à sua atuação no certame, sem prejuízo

SESC – Serviço Social do Comércio | Departamento Regional em Pernambuco | www.sescpe.org.br
Casa do Comércio/Edifício Josias Albuquerque | Avenida Visconde de Suassuna, nº 265, Santo Amaro - Recife-PE.
CEP: 50.050-540 TEL + 55 81 3216 1739

dos atos realizados.

3.4.4.2 – Quando a desconexão persistir por tempo superior a 10 (dez) minutos, a sessão será suspensa e terá reinício somente após comunicação expressa do Pregoeiro(a) aos participantes, conforme previsto no subitem 14.1 deste edital.

4. DA PROPOSTA COMERCIAL

Para fins de julgamento considerar-se-á a proposta comercial de duas formas, não excludentes entre si:

a) PROPOSTA ELETRÔNICA: Proposta comercial do **valor total do lote**, enviada por todos os licitantes através do sistema *"Licitações-e"*, conforme subitem 4.1 deste edital.

b) PROPOSTA AJUSTADA: Proposta comercial detalhada enviada pelo licitante arrematante, conforme subitem 4.2 deste edital.

4.1 – PROPOSTA ELETRÔNICA

4.1.1 – Deverá ser enviada, **exclusivamente**, por meio do sistema eletrônico, conforme subitens 6.1.1 deste edital, inserindo na caixa **"DESCRIÇÃO/OBSERVAÇÕES (CONFORME INSTRUMENTO CONVOCATÓRIO)"** as especificações/características dos equipamentos (itens) cotados, **desde que em conformidade com as especificações técnicas e exigências estabelecidas neste edital.**

4.1.2 – A apresentação do **VALOR TOTAL DO LOTE** na proposta eletrônica pressupõe o cumprimento das condições estabelecidas neste edital e seus anexos, em especial:

a) O cumprimento das especificações constantes no ANEXO I deste edital;

b) Que o valor total apresentado corresponda ao fornecimento de acordo com a forma de julgamento constante no item 7 deste edital, o **VALOR DO LOTE OFERTADO**; e

c) A proposta deverá apresentar preços correntes de mercado, sem quaisquer acréscimos em virtude de expectativa inflacionária ou de custo financeiro.

4.1.3 – **O licitante deverá cotar o VALOR TOTAL DO LOTE**, em moeda corrente nacional, com duas casas decimais, incluindo, obrigatoriamente todas as despesas com encargos sociais, tributos, descontos, emolumentos, impostos, despesas diretas e indiretas, **todo o material de consumo e insumo necessários à realização dos serviços de manutenção preventiva e corretiva,** e demais condições de fornecimento que sejam devidas, em decorrência direta e indireta, do objeto desta licitação, em conformidade com as especificações e quantitativos descritos no TERMO DE REFERÊNCIA (ANEXO I) deste edital.

4.1.3.1 – O LICITANTE DEVERÁ LANÇAR O VALOR TOTAL DO LOTE ESCOLHIDO, RESULTADO DA FÓRMULA: SOMATÓRIO DO PRODUTO DAS MULTIPLICAÇÕES = PREÇO UNITÁRIO DOS ITENS QUE COMPOEM O LOTE X QUANTIDADE TOTAL DE CADA ITEM DO LOTE, EM CONFORMIDADE COM AS CONDIÇÕES ESTABELECIDAS NO TERMO DE

SESC – Serviço Social do Comércio | Departamento Regional em Pernambuco | www.sescpe.org.br
Casa do Comércio/Edifício Josias Albuquerque | Avenida Visconde de Suassuna, nº 265, Santo Amaro - Recife-PE.
CEP: 50.050-540 TEL + 55 81 3216 1739

REFERÊNCIA (ANEXO I) DESTE EDITAL.

4.1.3.2 – **QUANDO DA COMPOSIÇÃO DO VALOR TOTAL DO LOTE ESCOLHIDO, O LICITANTE DEVERÁ COTAR TODOS OS ITENS QUE COMPOEM O LOTE, EM CONFORMIDADE COM O TERMO DE REFERÊNCIA (ANEXO I) DESTE EDITAL.**

4.1.4 – **COM O OBJETIVO DE GARANTIR O SIGILO DAS PROPOSTAS ELETRÔNICAS DE PREÇOS INICIAIS INSERIDAS NO SISTEMA DO *"LICITAÇÕES-E"*, O LICITANTE NÃO PODERÁ IDENTIFICAR-SE DE FORMA ALGUMA (NOME, LOGOMARCA DA EMPRESA, ETC.) NOS CAMPOS DE PREENCHIMENTO DA DESCRIÇÃO DO ITEM, MARCA E VALORES, DURANTE A FASE DE RECEBIMENTO E ABERTURA DAS PROPOSTAS ELETRÔNICAS, BEM COMO DURANTE A FASE DE LANCES, ATÉ QUE O PRÓPRIO SISTEMA IDENTIFIQUE OS RESPECTIVOS ARREMATANTES, SOB PENA DE DESCLASSIFICAÇÃO.**

4.1.5 – **Os termos constantes da proposta apresentada são de exclusiva responsabilidade do licitante.**

4.2 – PROPOSTA COMERCIAL AJUSTADA

A Proposta Comercial Ajustada deverá ser apresentada conforme MODELO DE PROPOSTA COMERCIAL (ANEXO II) deste edital, obedecendo aos termos do Edital e seus Anexos, devendo ser encaminhada à Comissão de Licitação/Pregoeiro(a), **exclusivamente, para o e-mail: licitacao@sescpe.com.br, dentro do prazo de até 24 (vinte e quatro) horas, contados a partir da solicitação do Pregoeiro(a)**, atendendo as seguintes exigências:

4.2.1 – FORMA DE APRESENTAÇÃO

a) 01 (uma) via digitada, impressa em papel timbrado do licitante, redigida com clareza, em língua portuguesa, sem emendas ou rasuras, devendo estar datada, e devidamente assinada na última folha e rubricadas nas demais **pelo responsável legal da empresa, cuja comprovação de delegação de poderes também deve ser encaminhada, seja procuração pública ou privada ou documento equivalente, juntamente com o documento de identificação do representante, através da apresentação da Cédula de identidade, Carteira Nacional de Habilitação ou Identidade Profissional (CREA, CRC, OAB, entre outros) através do original ou cópia autenticada em cartório.**

a.1) QUANDO SE TRATAR DE PROCURAÇÃO PÚBLICA OU PRIVADA, PODERÁ O ADMINISTRADOR, FAZER SUBSTITUIR-SE EXCEPCIONALMENTE, DESDE QUE SEJA CONCEDIDA PROCURAÇÃO COM PODERES ESPECÍFICOS, NOS LIMITES DE SEUS PODERES, ESTABELECIDOS NO CONTRATO SOCIAL.

b) Ser redigida de forma clara, não sendo aceitas as que apresentarem rasuras, entrelinhas, ressalvas ou emendas.

4.2.2 – INFORMAÇÕES QUE DEVERÃO ESTAR CONTIDAS NA PROPOSTA AJUSTADA

a) PREÇO DOS PRODUTOS: PREÇO UNITÁRIO E TOTAL DE TODOS OS ITENS QUE COMPÕEM O LOTE E PREÇO TOTAL DO LOTE (conforme valor arrematado na Sessão Pública de Lances),

SESC – Serviço Social do Comércio | Departamento Regional em Pernambuco | www.sescpe.org.br
Casa do Comércio/Edifício Josias Albuquerque | Avenida Visconde de Suassuna, nº 265, Santo Amaro - Recife-PE.
CEP: 50.050-540 TEL + 55 81 3216 1739

em algarismo e por extenso, em moeda nacional, com 02 (duas) casas decimais, incluindo, obrigatoriamente, todas as despesas com salários, encargos sociais, tributos, descontos, emolumentos, obrigações trabalhistas e previdenciárias, contribuições fiscais e parafiscais, uniformes, administração, mão de obra, transporte, **fretes**, **carga e descarga**, e demais despesas incidentes direta e indiretamente no fornecimento do objeto desta licitação, inclusive o lucro.

a.1) DEVERÃO SER COTADOS TODOS OS ITENS CONSTANTES NO LOTE, CONFORME ANEXO I DESTE EDITAL. A FALTA DE UM ITEM QUE COMPÕE O LOTE IMPLICARÁ NA DESCLASSIFICAÇÃO DO LICITANTE PARA O REFERIDO LOTE ARREMATADO.

b) ESPECIFICAÇÃO COMPLETA DO PRODUTO: Na proposta deverá constar a especificação completa do(s) item(ns) constantes no lote arrematado(s), mencionando: as quantidades, a marca, o fabricante, o modelo, a procedência, se nacional ou estrangeira, conforme for o caso, entre outros, **em conformidade com as especificações técnicas contidas no TERMO DE REFERÊNCIA (ANEXO I) deste edital.**

c) ASSINATURA DA ATA: Na proposta também deverá constar a identificação do representante legal da empresa que assinará a Ata de Registro de Preços.

4.2.3 – DA CONFERÊNCIA DA PROPOSTA

a) Havendo discrepância entre os preços unitários e totais da proposta ajustada, prevalecerá o valor unitário arrematado e, havendo discordância entre o valor total em algarismo e o total por extenso, prevalecerá o que equivale ao valor arrematado.

b) Se na proposta a especificação estiver incompleta, esta será considerada igual à exigida no presente edital, obrigando-se o proponente à entrega de produto que atenda em plenitude às condições do ANEXO I deste edital.

c) Serão desclassificadas ainda as propostas que apresentem irregularidades ou defeitos capazes de dificultar o julgamento ou que imponham condições ou ressalvas em relação às condições estabelecidas neste edital.

d) Configurando o erro detectado como vício material, cuja solução não possa ser promovida pela Comissão de Licitação/Pregoeiro(a), sem alteração substancial da proposta, esta será considerada desclassificada.

4.2.4 – CONSIDERAÇÕES GERAIS SOBRE A PROPOSTA

a) Os prazos exigidos neste edital deverão estar expressos na proposta, NÃO sendo admitidas expressões do tipo *"de acordo com o item xx do edital"* ou equivalentes, podendo a critério da Comissão de Licitação/Pregoeiro(a), implicar na desclassificação do licitante.

b) Os termos constantes na proposta apresentada são de exclusiva responsabilidade do licitante.

c) Os preços unitários deverão ser firmes e irreajustáveis.

d) A **validade da proposta não poderá ser inferior a 120 (cento e vinte) dias**, a contar da data da Sessão Pública.

d.1) Caso haja o vencimento da validade da proposta sem que a licitação tenha sido homologada, a Ata de Registro de Preços ou documento equivalente (Pedido de Compra) assinado, esta fica automaticamente prorrogada, exceto se houver manifestação contrária formal do licitante, para o **e-mail: licitacao@sescpe.com.br**, dirigida à Comissão de Licitação/Pregoeiro(a), caracterizando seu declínio em continuar na licitação.

5. DA HABILITAÇÃO

O licitante arrematante também deverá encaminhar, **exclusivamente, para o e-mail: licitacao@sescpe.com.br**, dentro do prazo de até 24 (vinte e quatro) horas, contadas a partir da solicitação do Pregoeiro(a), **os documentos de Habilitação, abaixo relacionados**, **conforme indicados nos subitens a seguir:**

5.1 – HABILITAÇÃO JURÍDICA

a) ATO CONSTITUTIVO e suas últimas alterações ou **ALTERAÇÃO CONTRATUAL** com sua respectiva consolidação contratual, devidamente registrado na Junta Comercial do Estado da sede do licitante, onde deverá estar indicado ramo de atividade compatível com o objeto da licitação.

a.1) Ato de nomeação ou de eleição dos administradores, devidamente registrado no órgão competente, na hipótese de terem sido nomeados ou eleitos em separado.

Observações:

1 – Deverá apresentar Registro Comercial e/ou Certificado da Condição do Microempreendedor Individual (CCMEI), no caso de empresário individual.
2 – Em se tratando de sociedade por ações, o ato constitutivo deverá ser acompanhado de documentação da eleição de seus administradores.
3 – Tratando-se de sociedade civil, o ato constitutivo deverá estar inscrito no órgão de classe e acompanhado de prova da diretoria em exercício.
4 – Os documentos solicitados nas alíneas “a” e “a.1”, acima mencionados, deverão estar adaptados às novas regras do novo Código Civil vigente.

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

b) DOCUMENTO DE IDENTIFICAÇÃO, válido em todo o território nacional, no caso de firma individual.

5.2 – QUALIFICAÇÃO TÉCNICA

a) No mínimo 01 (uma) **DECLARAÇÃO/ATESTADO DE CAPACIDADE TÉCNICA**, fornecida (o) por pessoa jurídica de direito público ou privado, **impresso em papel timbrado da pessoa jurídica que**

expediu o atestado, constando o nome, cargo e telefone de contato do responsável, informando se foi cumprido o prazo de entrega e se o emitente ficou satisfeito com a qualidade dos produtos, comprovando que a empresa forneceu produtos da mesma natureza e porte do objeto da presente licitação.

a.1) As empresas que já forneceram os produtos, objeto desta licitação, para o Sesc/DR-PE PODERÃO apresentar declaração (ões), no mínimo 01 (uma), fornecida pela Coordenação de Compras, comprovando que os equipamentos fornecidos atenderam aos padrões de qualidade exigidos pelo Sesc/DR-PE e aos prazos estabelecidos.

a.2) O Sesc/DR-PE se reserva o direito de diligenciar sobre a veracidade das informações contidas nos Atestados de que trata o subitem anterior.

a.3) O Sesc/DR-PE PODERÁ realizar diligência/visita técnica, a fim de complementar informações ou comprovar a veracidade do (s) atestado (s) de capacidade técnica apresentado (s) pelo licitante, quando, PODERÁ ser requerida cópia do (s) contrato (s), Nota (s) Fiscal (is) ou qualquer outro documento que comprove inequivocamente que o serviço/produto apresentado no atestado foi prestado.

5.3 – REGULARIDADE FISCAL

a) Prova de inscrição no Cadastro Nacional das Pessoas Jurídicas do Ministério da Fazenda – **CNPJ/MF**.

b) Certificado de Regularidade Fiscal - CRF, perante o Fundo de Garantia por Tempo de Serviço - **FGTS**, relativo ao domicílio ou sede do licitante, atualizada.

c) Certidão Conjunta Negativa ou Positiva com efeitos de Negativa de Débitos relativos aos Tributos Federais, Dívida Ativa da União e Contribuições Previdenciárias, expedida em conjunto pela Secretaria da Receita Federal do Brasil e Procuradoria-Geral da Fazenda Nacional, nos termos da Portaria MF 358, de 5/9/2014, atualizada.

d) Prova de Regularidade para com a Fazenda Estadual, atualizada.

d.1) Se a empresa licitante NÃO FOR CONTRIBUINTE DO ICMS, DEVERÁ APRESENTAR CERTIDÃO DE NÃO CONTRIBUINTE. Quando for o caso, a DECLARAÇÃO DE NÃO CONTRIBUINTE poderá ser através de Declaração assinada pelo Contador responsável, devidamente registrado no CRC (Conselho Regional de Contabilidade) e pelo responsável legal da empresa, de que a mesma não é contribuinte do ICMS.

e) Prova de Regularidade para com a Fazenda Municipal, atualizada.

e.1) Se a empresa licitante NÃO FOR CONTRIBUINTE DO ISS, DEVERÁ APRESENTAR CERTIDÃO DE NÃO CONTRIBUINTE. Quando for o caso, a DECLARAÇÃO DE NÃO CONTRIBUINTE poderá ser através de Declaração assinada pelo Contador responsável, devidamente registrado no CRC (Conselho Regional de Contabilidade) e pelo responsável legal da empresa, de que a mesma não é contribuinte do ISS.

5.3.1 – Caso a (s) certidão (ões) expedida (s) pela (s) fazenda (s) federal, estadual e municipal seja (m) POSITIVA (S), o Sesc/DR-PE se reserva o direito de só aceitá-la (s) se a (s) mesma (s) contiver (em) expressamente o efeito de NEGATIVA, nos termos do art. 206 do Código Tributário Nacional, passado pelo seu emitente.

5.3.2 – **Sendo ou não contribuinte, o licitante fica obrigado a apresentar as certidões de regularidade expedidas pelas fazendas federal, estadual e municipal, nos termos das alíneas "c" a "e" do subitem 5.3 deste edital.**

5.3.3 – Todos os documentos apresentados deverão estar em nome do licitante e com o número do CNPJ e endereço respectivo. **Se o licitante for matriz, todos os documentos deverão estar em nome da matriz, se for filial, todos os documentos deverão estar em nome da filial, exceto aqueles que pela própria natureza, forem comprovadamente emitidos apenas em nome da matriz**.

5.4 – CONSIDERAÇÕES GERAIS SOBRE OS DOCUMENTOS

5.4.1 – A documentação deverá ser enviada para o **e-mail: licitacao@sescpe.com.br**, em **fotocópias autenticadas por cartório, por tabelião de notas ou publicação em órgão de imprensa oficial, não sendo aceito cópia ilegível.** Se julgar necessário, a Comissão de Licitação/Pregoeiro(a) poderá solicitar aos licitantes a apresentação dos documentos originais para fins de confrontação com as fotocópias autenticadas apresentadas.

5.4.2 – Não serão aceitas cópias coloridas ou documentos que contenham rasuras, borrões ou quaisquer outras marcas que denotem que não sejam originais, mas meramente fotocópias, que deverão estar autenticadas por cartório ou por tabelião de notas ou publicação em órgão de imprensa oficial.

5.4.3 – No caso de apresentação apenas dos documentos na forma original, os mesmos não serão devolvidos, passando a integrar a documentação do processo.

5.4.4 – **Os documentos que forem emitidos pela internet estarão sujeitos a posterior conferência na página eletrônica do órgão emissor, para verificação de sua autenticidade e validade.**

5.4.5 - Os documentos exigidos para habilitação DEVERÃO ESTAR VÁLIDOS NA DATA DA SESSÃO PÚBLICA DE LANCES, salvo para os casos previstos abaixo:

a) Caso o licitante inicialmente classificado seja desclassificado, inabilitado ou decline, o licitante remanescente poderá ser convocado para apresentar os documentos exigidos, desde que estes estejam válidos na **data da convocação**, devendo atender ao disposto no subitem 6.4.1 do edital, sob pena de inabilitação.

b) Em relação aos Atestados de Capacidade Técnica (subitem 5.2 deste edital), a experiência comprovada deverá ser preexistente à data da sessão pública de lances, sendo vedada a apresentação de atestados referentes a serviços prestados/fornecimentos ou iniciados após essa data.

5.4.6 – Quando o órgão emitente for omisso em relação ao prazo de validade dos mesmos, considerar-se-á o prazo de validade de **180 (cento e oitenta) dias**.

5.4.7 – A habilitação do licitante estrangeiro poderá ser comprovada por meio da apresentação de seus atos constitutivos ou documentos similares e de documentos de qualificação-técnica (subitem 5.2 deste edital), dispensada a apresentação da comprovação dos documentos de habilitação fiscal e de econômico-financeira.

6. DOS PROCEDIMENTOS LICITATÓRIOS

6.2 – ABERTURA DAS PROPOSTAS

6.2.1 – Findo o prazo de recebimento das propostas eletrônicas, a Comissão de Licitação/Pregoeiro(a) fará a análise destas, desclassificando aquelas que não estiverem em consonância com o estabelecido neste edital e seus anexos. A decisão sobre a classificação das propostas comerciais será disponibilizada no sistema eletrônico para acompanhamento em tempo real, pelos licitantes.

6.2.2 – Da decisão de desclassificar as propostas comerciais, somente caberá pedido de reconsideração à própria Comissão de Licitação/Pregoeiro(a), a ser enviado, **exclusivamente, para o e-mail: licitacao@sescpe.com.br**, acompanhado da justificativa de suas razões, no prazo de 30 (trinta) minutos a contar do momento em que vier a ser disponibilizada no sistema eletrônico.

6.2.3 – A Comissão de Licitação/Pregoeiro(a) decidirá no mesmo prazo, salvo motivos que justifiquem sua prorrogação, cabendo o Pregoeiro registrar no sistema eletrônico a decisão tomada, para que seja acompanhada em tempo real por todos os licitantes.

6.2.4 – Da decisão da Comissão de Licitação/Pregoeiro(a) relativa ao pedido de reconsideração, não caberá recurso.

6.3 – SESSÃO PÚBLICA DE LANCES

6.3.1 – Classificadas as propostas, iniciar-se-á a fase de lances, na qual os autores das propostas classificadas poderão oferecer seus lances **exclusivamente** por meio do sistema eletrônico, sem restrições de quantidade, ordem classificatória ou cronológica específica, mas sempre inferior ao seu último lance ofertado. A cada lance ofertado o participante será imediatamente informado de seu recebimento, horário de registro e valor, pressupondo-se a necessidade das empresas estarem conectadas ao sistema eletrônico.

6.3.2 – Na hipótese de haver lances iguais, prevalecerá como de menor valor, o lance que tiver sido primeiramente registrado.

6.3.3 – Será adotado para o envio de lances no Pregão Eletrônico o modo de disputa “aberto”, em que os licitantes apresentarão lances públicos e sucessivos, com prorrogações, observado o horário fixado e as regras de aceitação dos mesmos.

6.3.3.1 – Durante a sessão pública de lances, os licitantes deverão observar e respeitar, obrigatoriamente, o ***"intervalo mínimo diferença de valores"*** e o ***"valor mínimo cobrir melhor oferta"*****,** estabelecidos para cada item/lote no sistema *"Licitações-e"* do Banco do Brasil.

6.3.4 – Durante o transcurso da sessão pública de lances, as empresas licitantes participantes serão informadas, em tempo real, do valor do menor lance registrado. O sistema não identificará os autores dos lances aos demais participantes e aos representantes do Sesc/DR-PE (Comissão de Licitação/Pregoeiro[a]).

6.3.5 – A etapa de lances da sessão pública terá duração de 10 (dez) minutos e, após isso, será prorrogada automaticamente pelo sistema *"Licitações-e"* quando houver lance ofertado nos últimos dois minutos do período de duração da sessão pública.

6.3.5.1 – A prorrogação automática da etapa de lances, de que trata o subitem 6.3.5 acima, será de dois minutos e ocorrerá sucessivamente sempre que houver lances enviados neste período de prorrogação, inclusive no caso de lances intermediários.

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

6.3.7 – Encerrada a fase competitiva, sem que haja a prorrogação automática pelo sistema, poderá o Pregoeiro(a), assessorado pela Comissão de Licitação, justificadamente, admitir o reinício da sessão pública de lances, em prol da consecução do melhor preço.

6.3.8 – OS PREÇOS OFERTADOS NA ETAPA DE LANCES SERÃO DE EXCLUSIVA RESPONSABILIDADE DO LICITANTE, NÃO LHE ASSISTINDO O DIREITO DE PLEITEAR QUALQUER ALTERAÇÃO, SOB ALEGAÇÃO DE ERRO, OMISSÃO OU QUALQUER OUTRO PRETEXTO.

6.3.9 – O sistema informará a proposta de menor preço imediatamente após o encerramento da etapa de lances. **Os licitantes deverão consultar regularmente o sistema eletrônico para verificar o resultado da licitação**.

6.3.9.1 – Na hipótese de **não** haver lances ofertados durante a fase da sessão pública de lances, permanecendo apenas as propostas eletrônicas, inicialmente cadastradas na fase de acolhimento (conforme subitem 4.1 deste edital), o sistema "Licitações-e" realizará, de forma automática e aleatória, sorteio eletrônico entre as propostas empatadas, para definição da classificação.

6.3.10 – O sistema eletrônico gerará ATA circunstanciada com o registro da indicação do lance vencedor, classificação dos lances e demais informações relativas à sessão realizada.

6.3.11 – Após o encerramento da etapa de lances da sessão pública, o Pregoeiro(a) poderá solicitar, pelo sistema eletrônico, contraproposta ao licitante que tenha apresentado lance mais vantajoso, para que seja obtida melhor proposta, observando o critério de julgamento, não se admitindo negociar condições diferentes daquelas previstas no edital.

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

6.3.13 – **O *"valor estimado do lote"*, divulgado ao término da sessão de lances, é de caráter informativo e NÃO deve ser utilizado como referência final para a elaboração das Propostas Comerciais Ajustadas pelos licitantes. Isso posto, em eventual necessidade de negociações, os licitantes arrematantes deverão considerar as contrapropostas encaminhadas pelo Pregoeiro(a).**

6.4 – ENVIO DA PROPOSTA COMERCIAL AJUSTADA E DOS DOCUMENTOS DE HABILITAÇÃO

6.4.1 – Ordenados os lances em forma crescente de preço, o Pregoeiro(a) determinará ao autor do lance classificado como "ARREMATANTE" (menor lance) que entregue no **prazo máximo de 24 (vinte e quatro) horas** a **PROPOSTA COMERCIAL AJUSTADA**, e os **DOCUMENTOS DE HABILITAÇÃO**, conforme itens 4 e 5, ambos deste edital, a contar da solicitação e divulgação pelo Pregoeiro(a) no sistema *"Licitações-e"* do Banco do Brasil S/A., **exclusivamente, para o e-mail: licitacao@sescpe.com.br**, indicando no campo assunto do e-mail o número deste Pregão Eletrônico.

6.4.1.1 – Os documentos deverão ser enviados com antecedência necessária para o recebimento pela Comissão de Licitação/Pregoeiro(a), no prazo estabelecido pelo Pregoeiro(a).

6.5 – ÁNÁLISE DA PROPOSTA COMERCIAL AJUSTADA E DOS DOCUMENTOS DE HABILITAÇÃO

6.5.1 – A PROPOSTA COMERCIAL AJUSTADA e os DOCUMENTOS DE HABILITAÇÃO serão analisados pela Comissão de Licitação/Pregoeiro(a), para fins de verificação da conformidade com este edital e seus anexos, e será julgada de acordo com este instrumento convocatório.

6.5.2 – **A Proposta Comercial Ajustada e os documentos referentes à Qualificação Técnica (subitem 5.2 do edital) PODERÃO ser submetidos à análise da área técnica do Sesc/DR-PE, que emitirá laudo técnico, com efeito classificatório, confirmando que os referidos documentos estão de acordo com as especificações, condições e exigências estabelecidas neste edital.**

6.5.3 – O desatendimento de exigências meramente formais que não comprometam a aferição da qualificação do licitante ou a compreensão do conteúdo de sua proposta não importará seu afastamento da licitação ou a invalidação do processo.

6.5.4 – Será permitida a inclusão de documento complementar ou atualizado, desde que não alterem a substância das propostas, dos documentos e sua validade jurídica e seja comprobatório de condição atendida pelo licitante quando apresentada sua proposta, que não foi juntado com os demais documentos por equívoco ou falha, o qual deverá ser solicitado e avaliado pela Comissão de Licitação/Pregoeiro(a).

6.5.5 – **Na hipótese de inabilitação, de reprovação da Proposta Comercial Ajustada ou de descumprimento das exigências estabelecidas neste edital e seus anexos, caberá à Comissão de Licitação/Pregoeiro(a) autorizar o Pregoeiro(a) a convocar o autor do segundo menor lance e, se necessário, observado a ordem crescente de preço, os autores dos demais lances, desde que atendam às exigências deste edital e seus anexos.**

SESC – Serviço Social do Comércio | Departamento Regional em Pernambuco | www.sescpe.org.br
Casa do Comércio/Edifício Josias Albuquerque | Avenida Visconde de Suassuna, nº 265, Santo Amaro - Recife-PE.
CEP: 50.050-540 TEL + 55 81 3216 1739

6.5.6 – Na hipótese de inabilitação de todos os licitantes ou de desclassificação de todas as propostas, PODERÁ ser fixado novo prazo para a apresentação de documentações e/ou de propostas retificadas.

6.6 – DECLARAÇÃO DO VENCEDOR E FINALIZAÇÃO DA LICITAÇÃO

6.6.1 – **Após análise e verificação da regularidade da documentação de Habilitação, julgada a Proposta de menor lance e considerando atendidas todas as exigências editalícias, o *"ARREMATANTE"* será declarado VENCEDOR pela Comissão de Licitação/Pregoeiro(a)**. A Comissão consignará esta decisão e os eventos ocorridos em ATA própria, que será publicada no site do Sistema *"Licitações-e"* do Banco do Brasil S/A. (www.licitacoes-e.com.br) e no site do Sesc/DR-PE (www.sescpe.org.br/sobre-o-sesc/licitacoes).

6.6.2 – Após a declaração de vencedor, na própria ATA publicada, a Comissão de Licitação/Pregoeiro(a) emitirá um COMUNICADO, abrindo a possibilidade para qualquer licitante que esteja classificado, se manifestar no sentido de se habilitar a aderir e praticar o menor preço registrado, para assinar posteriormente a Ata de Registro de Preços.

6.6.2.1 – **O licitante terá o prazo de 24 (vinte e quatro) horas, após a publicação do COMUNICADO, para se manifestar no Sistema *"Licitações-e"* do Banco do Brasil S/A. (www.licitacoes-e.com.br)**, quanto a sua intenção de ADERIR e praticar o menor preço registrado, bem como enviar para o **e-mail da Comissão de Licitação/Pregoeiro(a): licitacao@sescpe.com.br**, a **PROPOSTA COMERCIAL AJUSTADA**, e os **DOCUMENTOS DE HABILITAÇÃO**, em conformidade com os itens 4 e 5, ambos deste edital. Os referidos documentos serão analisados pela Comissão de Licitação/Pregoeiro(a) e área técnica do Sesc/DR-PE, para posteriormente, se constatado o cumprimento das exigências estabelecidas em edital, declarar o licitante habilitado e aderente a Ata de Registro de Preços.

6.6.3 – O Pregoeiro(a) consignará todas as decisões e os eventos ocorridos em ATA própria, que será publicada no sistema *"Licitações-e"* do Banco do Brasil S/A. (**www.licitacoes-e.com.br**) e no site do Sesc/DR-PE (**www.sescpe.org.br/sobre-o-sesc/licitacoes**).

6.6.4 – Após a publicação da ATA, com a declaração de vencedor, não havendo manifestação de recurso, o processo será encaminhado à autoridade competente para homologação do objeto ao licitante vencedor.

6.6.4.1 – Homologado o processo, será divulgado o **RESULTADO** do certame, sendo publicado no sistema *"Licitações-e"* do Banco do Brasil S/A. (**www.licitacoes-e.com.br**) e no site do Sesc/DR-PE (**www.sescpe.org.br/sobre-o-sesc/licitacoes**).

6.6.5 – Após a publicação do **RESULTADO** do certame, será realizada a convocação do licitante vencedor e, caso possua, do(s) licitante(s) aderente(s) a praticar(em) o menor preço, para assinatura da Ata de Registro de Preços.

7. DO CRITÉRIO DE JULGAMENTO

7.1 – **A presente licitação é do tipo MENOR PREÇO, POR LOTE, PARA REGISTRO DE PREÇOS**, **sendo que na obtenção da proposta mais vantajosa o julgamento far-se-á vinculado ao atendimento das exigências contidas neste instrumento convocatório e seus anexos.**

7.1.1 – **Os preços unitários que compõem o lote cotado serão analisados individualmente, objetivando verificar a compatibilidade com os preços unitários praticados no mercado.**

7.2 – **PODERÃO SER DESCLASSIFICADAS AS PROPOSTAS DOS LICITANTES CUJAS ESPECIFICAÇÕES DO(S) ITEM(NS) SEJAM REPROVADAS APÓS ANÁLISE E PARECER DA ÁREA TÉCNICA DO SESC/DR-PE.**

8. DAS OBRIGAÇÕES E RESPONSABILIDADES DAS PARTES

8.1 – Sem prejuízo das obrigações inerentes à perfeita execução do objeto da licitação e demais disposições deste instrumento, constituem obrigações e responsabilidades das partes aquelas elencadas nas **CLÁUSULAS SÉTIMA** e **OITAVA da MINUTA DA ATA DE REGISTRO DE PREÇOS (ANEXO IV)** deste edital, além de outras que estejam relacionadas à perfeita execução do objeto licitado.

9. DA ATA DE REGISTRO DE PREÇOS

9.1 – Após a homologação pela autoridade competente, o licitante vencedor será convocado para assinatura da Ata de Registro de Preços no prazo de **até 01 (um) dia útil,** a contar da data da convocação, através de e-mail pela Unidade de Suprimentos (Coordenação de Compras) do Sesc/DR-PE.

9.1.1 – Para as empresas localizadas fora da Região Metropolitana do Recife o prazo para assinatura da Ata será de **até 02 (dois) dias úteis,** a contar da data da convocação.

9.1.2 - CRITÉRIOS PARA ASSINATURA DA ATA DE REGISTRO DE PREÇOS – Como critério para assinatura da Ata de Registro de Preços, a empresa signatária deverá apresentar as exigências constantes nas tabelas abaixo:

ITEM	EXIGÊNCIA (CONFORME TABELA LEGENDA DO CAMPO EXIGÊNCIA)
01	A, B, C
02	A, B, C

LEGENDA DO CAMPO EXIGÊNCIA	
A	Comprovação através de Carta do Fabricante (nominal ao processo) que sua empresa é revenda/distribuidor autorizado a comercializar os produtos;

B	Declaração do fabricante comprovando que possui em seu quadro funcional ao menos um profissional autorizado e com capacitação técnica para realizar treinamentos oficiais de implantação, configuração e operação da solução ofertada
C	Declaração do fabricante garantindo que o produto terá atualização e suporte pelo período mínimo de 36 (trinta e seis) meses

9.2 – **Caso o licitante vencedor não compareça para a assinatura, ou se recuse a tal, injustificadamente, terá seus preços invalidados e será penalizado com a suspensão do direito de licitar e contratar com o Sesc/DR-PE pelo prazo de até 03 (três) anos, além das demais penalidades previstas em lei e neste instrumento convocatório.**

9.2.1 – No caso do subitem anterior, poderá o Sesc/DR-PE convocar outro licitante, respeitada a ordem de classificação e atendidas as demais exigências deste edital e seus anexos.

9.3 – É permitido que outros licitantes habilitados venham a praticar o menor preço registrado, chamados na ordem de classificação, desde que atendam às exigências e condições estabelecidas neste edital, e assinem a Ata de Registro de Preços.

9.4 – A vigência inicial da ATA será de **12 (doze) meses**, com início a partir da data de sua assinatura, podendo ser prorrogada, desde que pesquisa de mercado demonstre que o preço registrado se mantém vantajoso, conforme o Artigo 45 da Resolução Sesc Nº 1.593/2024.

9.4.1 – **A Ata de Registro de Preços poderá ser prorrogada, além do prazo estipulado no subitem acima, até o limite máximo de 36 (trinta e seis) meses.**

9.4.2 – **Prorrogada a Ata de Registro de Preços, ficam restabelecidos os termos e as condições iniciais do referido instrumento vinculativo, inclusive quantitativos.**

9.5 – **As Atas de Registro de Preços poderão ser acrescidas em até 50% (cinquenta por cento) de seus quantitativos inicialmente registrados, mediante acordo entre as Partes.**

9.6 – A qualquer tempo, durante o período de vigência, os preços registrados poderão ser revistos em decorrência de eventual redução dos preços praticados no mercado ou de fato que eleve o custo dos serviços ou bens registrados, cabendo ao Sesc/DR-PE convocar a empresa fornecedora para promover as negociações necessárias, até que se defina o novo valor, conforme o entendimento da legislação vigente.

9.6.1 – Frustrada a negociação, a empresa fornecedora será liberada de seu compromisso e o Sesc/DR-PE convocará as demais empresas classificadas visando igual oportunidade de negociação.

9.7 – Quando o preço de mercado se tornar superior ao preço registrado na Ata de Registro de Preços e o fornecedor não puder arcar com seu compromisso, o Sesc/DR-PE poderá, após comprovação do fato, liberar a empresa sem a aplicação das penalidades previstas neste edital e convocar as demais empresas classificadas, pela ordem, visando igual oportunidade de negociação.

9.7.1 – Quando não houver êxito nas negociações, o Sesc/DR-PE deverá proceder ao cancelamento

da Ata de Registro de Preços, adotando as medidas cabíveis para obtenção da contratação mais vantajosa.

9.8 – Fica vedada a contratação dos produtos a preços excessivos ou manifestadamente inexequíveis, face à oferta de mercado no momento da necessidade do Sesc/DR-PE, devendo para tanto os preços registrados serem alvo de permanente vigilância pelo fiscal.

9.9 – **ESTE REGISTRO DE PREÇO PODERÁ SER OBJETO DE ADESÃO POR OUTRO DEPARTAMENTO REGIONAL DO SESC E POR OUTRO SERVIÇO SOCIAL AUTÔNOMO, NOS TERMOS DO DISPOSTO NOS ARTIGOS 52 AO 55 DA RESOLUÇÃO SESC Nº 1.593/2024.**

10. DO CANCELAMENTO DO REGISTRO DE PREÇOS

10.1 – O FORNECEDOR terá seu registro de preços cancelado quando:

a) Descumprir as condições estipuladas nas cláusulas da Ata de Registro de Preços, configurando-se inadimplemento parcial ou total das obrigações assumidas;

b) Não aceitar reduzir seu preço registrado, na hipótese deste se tornar superior àqueles praticados no mercado;

c) Justificadamente, não for mais de interesse do Sesc/DR-PE.

10.2 – O FORNECEDOR poderá solicitar o cancelamento do seu registro de preços, ocorrendo fato superveniente que venha comprometer a perfeita execução contratual, decorrente de caso fortuito ou de força maior, devidamente justificado e comprovado, e que tenha sido formulado com a antecedência de 30 (trinta) dias.

10.2.1 – Será considerada como descumprimento total das obrigações a solicitação de cancelamento que não atender aos pré-requisitos do subitem 10.2 deste edital.

10.3 – O cancelamento do registro de preços, nas hipóteses previstas, assegurados o contraditório e a ampla defesa, serão formalizados por despacho da autoridade competente do Sesc/DR-PE.

11. DO PAGAMENTO

11.1 – Sem prejuízo das obrigações inerentes à perfeita execução do objeto da licitação e demais disposições deste instrumento, a FORMA DE PAGAMENTO estão elencadas na CLÁUSULA NONA da MINUTA DA ATA DE REGISTRO DE PREÇOS (ANEXO IV) deste edital.

12. DAS PENALIDADES

12.1 – **Sem prejuízo das obrigações inerentes à perfeita execução do objeto da licitação e demais disposições deste instrumento, as penalidades previstas constituem-se aquelas elencadas na CLÁUSULA DÉCIMA da MINUTA DA ATA DE REGISTRO DE PREÇOS (ANEXO**

IV) deste edital.

12.2 – **Para fins de penalidade, o lance é considerado proposta.**

13. DOS ESCLARECIMENTOS, IMPUGNAÇÕES E RECURSOS

13.1 – **Até 02 (dois) dias úteis** à data e horário fixados para a **abertura das propostas**, qualquer interessado poderá enviar ao Pregoeiro(a) pedido de esclarecimentos referente ao processo licitatório, **exclusivamente, para o e-mail: licitacao@sescpe.com.br**.

13.1.1 – Não sendo feito nesse prazo, pressupõe-se que os elementos fornecidos são suficientemente claros e precisos, precluindo toda a matéria nele constante, não cabendo ao licitante o direito a qualquer reclamação posterior.

13.2 – **Até 02 (dois) dias úteis** anteriores à data de **abertura das propostas**, qualquer pessoa poderá impugnar o ato convocatório do Pregão Eletrônico, condicionado à entrega da documentação formal de impugnação no mesmo prazo, **exclusivamente, para o e-mail: licitacao@sescpe.com.br.** As respostas serão disponibilizadas a todos os licitantes, nos moldes do previsto no subitem 14.1 deste edital.

13.3 – **DECLARADO O VENCEDOR, qualquer licitante poderá, durante a sessão pública, de forma imediata e motivada, em campo próprio do sistema, manifestar sua intenção de recorrer no prazo de 24 (vinte e quatro) horas, quando lhe será concedido prazo de 02 (dois) dias úteis para apresentar as razões de recurso, para o e-mail: licitacao@sescpe.com.br, que será dirigido ao Diretor Regional do Sesc/DR-PE, ficando os demais licitantes, desde logo, intimados para, querendo, apresentar contrarrazões em igual prazo, que começará a contar do término do prazo do recorrente, sendo-lhes assegurado vista imediata dos elementos indispensáveis à defesa dos seus interesses, através da disponibilização dos documentos via e-mail: licitacao@sescpe.com.br.**

13.3.1 – A Proposta Comercial Ajustada e os documentos de Habilitação da empresa vencedora permanecerão com vista franqueada aos interessados, os quais poderão ser disponibilizados via Internet.

13.4 – A falta de manifestação imediata e motivada do licitante quanto à intenção de recorrer, nos termos do subitem 13.3, importará em decadência desse direito, ficando o Pregoeiro(a) autorizado a propor à autoridade competente a homologação do certame e a assinatura da Ata de Registro de Preços. Por outro lado, o acolhimento do recurso implicará na invalidação apenas dos atos insuscetíveis de aproveitamento.

13.5 – Impugnado ou não o recurso, a Comissão de Licitação/Pregoeiro(a) o apreciará, podendo, se necessário, realizar instruções complementares e decidirá, motivadamente, pela manutenção ou reforma do ato recorrido, submetendo a decisão final da autoridade competente, cujo resultado será publicado no site do Sistema *"Licitações-e"* do Banco do Brasil S/A.: **www.licitacoes-e.com.br** e no site do Sesc/DR-PE: **www.sescpe.org.br/sobre-o-sesc/licitacoes**.

13.5.1 – O provimento de recursos pela autoridade competente somente invalidará os atos

insuscetíveis de aproveitamento.

13.6 – Não será aceita a intenção de recursos sobre assuntos meramente protelatórios.

13.7 – Não caberá recurso da decisão da autoridade competente do Sesc/DR-PE que é a última instância de julgamento da Entidade.

13.8 – As solicitações de esclarecimentos, impugnações ou recursos devem ser apresentadas à Comissão de Licitação/Pregoeiro(a), **exclusivamente, para o e-mail: licitacao@sescpe.com.br,** nos prazos estabelecidos no item 13 deste edital, no horário das 8h às 12h e das 13h às 17h, de segunda a sexta-feira, em dias de funcionamento da Sede do Sesc/DR-PE.

14. DAS DISPOSIÇÕES GERAIS

14.1 – As decisões relativas a esta licitação serão publicadas no site do Sistema *"Licitações-e"* do Banco do Brasil S/A.: **www.licitacoes-e.com.br** e no site do Sesc/DR-PE: **www.sescpe.org.br/sobre-o-sesc/licitacoes**.

14.1.1 – **É DE RESPONSABILIDADE DOS LICITANTES O ACOMPANHAMENTO DE TODAS AS INFORMAÇÕES NOS REFERIDOS SÍTIOS, DURANTE O PROCESSO LICITATÓRIO, EXIMINDO O SESC/DR-PE DA OBRIGAÇÃO DE INFORMAR POR QUALQUER OUTRO MEIO DE COMUNICAÇÃO.**

14.2 – **A Comissão de Licitação/Pregoeiro(a) poderá, no interesse do Sesc/DR-PE em manter o caráter competitivo desta licitação, relevar omissões puramente formais nos documentos e propostas apresentadas pelos licitantes, desde que não comprometam a lisura do certame e possam ser sanadas em prazo fixado pela mesma. Poderá também pesquisar via internet, quando possível, para verificar a regularidade/validade de documentos ou fixar prazo para dirimir eventuais dúvidas. O resultado de tal procedimento será determinante para fins de classificação/habilitação**.

14.3 – A Comissão de Licitação/Pregoeiro(a) poderá, a seu exclusivo critério, em qualquer fase da licitação, solicitar por escrito aos licitantes informações adicionais sobre a documentação e as propostas apresentadas, com o propósito de esclarecer ou complementar a instrução do processo. O não atendimento da solicitação no prazo estabelecido poderá implicar a desclassificação do licitante.

14.4 – O FORNECEDOR e seus sucessores se responsabilizarão por todos e quaisquer danos e/ou prejuízos que, a qualquer título, venham causar à imagem do Sesc/DR-PE e/ou terceiros em decorrência da execução indevida do objeto desta licitação.

14.5 – Na contagem dos prazos estabelecidos no presente instrumento convocatório, excluir-se-á o dia do início e incluir-se-á o do vencimento, e serão considerados dias consecutivos, exceto quando for explicitamente disposto em contrário. Só se iniciam e vencem os prazos aqui referidos em dias de funcionamento do Sesc/DR-PE.

14.6 – Independentemente de declaração expressa, a apresentação da proposta comercial e dos documentos de habilitação, implica na aceitação plena e total das condições e exigências deste

instrumento convocatório, na veracidade e autenticidade das informações constantes na proposta comercial e nos documentos apresentados e, ainda, na inexistência de fato impeditivo à participação da empresa, bem como de que deverá declará-lo quando ocorrido.

14.7 – **O Sesc/DR-PE se reserva o direito de CANCELAR unilateralmente esta licitação, a qualquer momento, no todo ou em parte, antes da formalização da Ata de Registro de Preços ou documento equivalente (Pedido de Compra), não cabendo aos licitantes quaisquer direitos, vantagens ou reclamações a que título for, inclusive de reparação a eventuais perdas ou danos ou de lucros cessantes.**

14.8 – A Resolução Sesc Nº 1.593/2024, encontra-se à disposição dos licitantes no seguinte endereço: Casa do Comércio / Edifício Josias Albuquerque, situado à Avenida Visconde de Suassuna, 265, Santo Amaro, Recife/PE, CEP: 50.050-540, com a Comissão de Licitação/Pregoeiro(a), Telefone: (81) 3216-1739 e no site do Sesc/DR-PE: **www.sescpe.org.br/sobre-o-sesc/licitacoes.**

14.9 – Os interessados poderão baixar este edital no site do Sesc/DR-PE: **www.sescpe.org.br/sobre-o-sesc/licitacoes** ou no site do sistema *"Licitações-e",* do Banco do Brasil S/A.: **www.licitacoes-e.com.br**, **licitação número 1086030.**

14.10 – **Todas as referências a horário neste edital consideram o horário de Brasília-DF.**

14.11 – São partes integrantes deste instrumento convocatório:

ANEXO I – TERMO DE REFERÊNCIA;
ANEXO II – MODELO DE PROPOSTA COMERCIAL;
ANEXO III – MINUTA DA ATA DE REGISTRO DE PREÇOS.

Recife, 15 de janeiro de 2026.

Comissão de Licitação/Pregoeiro(a)
SESC - Departamento Regional em Pernambuco

Ana Elizabeth Tinoco de Souza Ferraz

Ana Teresa Soares Rodrigues

Norma da Silva Bezerra Neta

PREGÃO ELETRÔNICO SESC/DR-PE Nº 006/2026 – REGISTRO DE PREÇOS
Licitação número 1086030 (www.licitacoes-e.com.br)

ANEXO I – TERMO DE REFERÊNCIA

Está disponível junto a este edital, no site do Sesc/DR-PE (www.sescpe.org.br - Licitações) e no site do Sistema *"Licitações-e"* do Banco do Brasil S/A (www.licitacoes-e.com.br), TERMO DE REFERÊNCIA, no formato *"PDF"*, que deverá ser observado pelos licitantes interessados em participar do Pregão Eletrônico em questão.

SESC – Serviço Social do Comércio | Departamento Regional em Pernambuco | www.sescpe.org.br
Casa do Comércio/Edifício Josias Albuquerque | Avenida Visconde de Suassuna, nº 265, Santo Amaro - Recife-PE.
CEP: 50.050-540 TEL + 55 81 3216 1739

PREGÃO ELETRÔNICO SESC/DR-PE Nº 006/2026 – REGISTRO DE PREÇOS
Licitação número 1086030 (www.licitacoes-e.com.br)

ANEXO II – MODELO DE PROPOSTA COMERCIAL

AO
SERVIÇO SOCIAL DO COMÉRCIO – SESC/DR-PE
COMISSÃO DE LICITAÇÃO/PREGOEIRO(A)
RECIFE - PE

REFERÊNCIA: PREGÃO ELETRÔNICO SESC/DR-PE Nº 006/2026.

A empresa _____, inscrita no CNPJ sob o nº __.___.___/____-__, estabelecida na _____, telefone nº ( ) _____-_____, e-mail _____, propõe ao Sesc/DR-PE o abaixo referenciado:

I – DO OBJETO

A presente Proposta Comercial é baseada nas especificações, condições e prazos estabelecidos no edital do PREGÃO ELETRÔNICO SESC/DR-PE Nº 006/2026, destinado ao **REGISTRO DE PREÇO, PARA RENOVAÇÃO DE LICENÇAS DE ANTIVÍRUS, KASPERSKY ENDPOINT SECURITY, A FIM DE SUPRIR AS NECESSIDADES DO PARQUE TECNOLÓGICO DO SESC-DR/PE, COM UMA SOLUÇÃO DE SOFTWARE INTEGRADO DE SEGURANÇA E PROTEÇÃO CONTRA SPAM DE E-MAIL, VAZAMENTOS DE DADOS, TENTATIVAS DE PHISHING E HACKING, ANTIMALWARE - VÍRUS, RANSOMWARE, CAVALOS DE TRÓIA, ROOTKITS, BACKDOORS, COM CRIPTOGRAFIA DE DADOS, SEGURANÇA MÓVEL, SEGURANÇA DA PLATAFORMA OFFICE 365, GERENCIAMENTO DE DISPOSITIVOS MÓVEIS, GERENCIAMENTO DE SISTEMAS E TREINAMENTO DE EQUIPE TÉCNICA SESC/DR-PE, COM ATUALIZAÇÕES PARA 36 (TRINTA E SEIS) MESES, SERVIÇO DE IMPLANTAÇÃO E MANUTENÇÃO, A FIM DE GARANTIR A PROTEÇÃO LÓGICA DOS COMPUTADORES, SERVIDORES FÍSICOS E VIRTUAIS, MS OFFICE 365, BEM COMO, EQUIPAMENTOS MÓVEIS (LAPTOPS, SMARTPHONES, TABLETS) INTEGRADOS A REDE LÓGICA DE DADOS DO SESC-DR/PE E DEMAIS UNIDADES DA INSTITUIÇÃO, CONTRA A ENTRADA E ATUAÇÃO DE MALWARES E PROGRAMAS MALICIOSOS,** em conformidade com as especificações técnicas descritas no TERMO DE REFERÊNCIA (ANEXO I), observadas as demais condições estabelecidas no instrumento convocatório e seus anexos.

II – DAS ESPECIFICAÇÕES DOS EQUIPAMENTOS E DOS PREÇOS

Os produtos que constituem o objeto desta Proposta serão entregues, conforme especificações técnicas contidas no TERMO DE REFERÊNCIA (ANEXO I) do edital do PREGÃO ELETRÔNICO SESC/DR-PE Nº 006/2026 e no quadro a seguir:

LOTE ÚNICO						
ITEM	PRODUTO	DESCRIÇÃO	PREVISÃO PARA AQUISIÇÃO IMEDIATA	QUANTIDADE TOTAL A SER REGISTRADA (UND.)	VALOR (R$)	
					UNITÁRIO	TOTAL

SESC – Serviço Social do Comércio | Departamento Regional em Pernambuco | www.sescpe.org.br
Casa do Comércio/Edifício Josias Albuquerque | Avenida Visconde de Suassuna, nº 265, Santo Amaro - Recife-PE.
CEP: 50.050-540 TEL + 55 81 3216 1739

XX	*(Descrição completa do item, conforme ANEXO I)*		*XX*	*XX*	xx,xx *(extenso)*	xx,xx *(extenso)*
⋮	⋮		⋮	⋮	⋮	⋮
XX	*(Descrição completa do item, conforme ANEXO I)*		*XX*	*XX*	xx,xx *(extenso)*	xx,xx *(extenso)*
VALOR DO LOTE: R$ XX.XXX,XX.						

Declaro que no valor da proposta estão incluídas todas as despesas, tais como: impostos, taxas, encargos sociais, tributos, descontos, emolumentos, **fretes**, instalação, carga e descarga, despesas diretas e indiretas, tributos e demais encargos de qualquer natureza, incidentes sobre o objeto do edital do PREGÃO ELETRÔNICO SESC/DR-PE N° 006/2026.

DECLARAMOS QUE ESTAMOS DE PLENO ACORDO COM TODAS AS OBRIGAÇÕES E RESPONSABILIDADES, BEM COMO TODAS AS CONDIÇÕES ESTABELECIDAS NO TERMO DE REFERÊNCIA (ANEXO I) DO EDITAL E SEUS ANEXOS.

III – DA ASSINATURA DA ATA DE REGISTRO DE PREÇOS

Se vencedor, na qualidade de representante legal da empresa, assinará a Ata de Registro de Preços:
Sr.(a):_____
Estado Civil,Profissão/Cargo:_____
RG nº/Órgão Expedidor:_____ CPF/MF: _____
Residente e domiciliado em:_____

(Local), ____ de _____ de 20___.

_____
ASSINATURA E CARIMBO DO REPRESENTANTE LEGAL

OBSERVAÇÕES:

- **O LICITANTE DEVERÁ INDICAR, NA PROPOSTA COMERCIAL, O E-MAIL DO REPRESENTANTE LEGAL QUE ASSINARÁ A ATA DE REGISTRO DE PREÇOS, BEM COMO COMUNICAR POR ESCRITO QUALQUER ALTERAÇÃO POSTERIOR, NO ENDEREÇO ELETRÔNICO APRESENTADO, A FIM DE QUE O SESC/DR-PE POSSA ENVIAR O DOCUMENTO AOS SIGNATÁRIOS POR E-MAIL, COM O OBJETIVO DE OBTER AS ASSINATURAS ELETRÔNICAS.**

- **ESTE DOCUMENTO DEVERÁ SER CONFECCIONADO EM PAPEL TIMBRADO DO LICITANTE, COM O CARIMBO DA EMPRESA E ASSINATURA DE SEU REPRESENTANTE LEGAL.**

ANEXO III – MINUTA DA ATA DE REGISTRO DE PREÇOS

CLÁUSULA PRIMEIRA – DAS PARTES

1.1 – O **SERVIÇO SOCIAL DO COMÉRCIO – Sesc** (**GERENCIADOR**), Departamento Regional em Pernambuco, instituição de direito privado, sem fins lucrativos, instituído pelo Decreto-Lei nº 9.853, de 13 de setembro de 1946, com regulamento aprovado pelo Decreto Federal nº 61.836, de 05 de dezembro de 1967, inscrito no CNPJ/MF sob o nº 03.482.931/0001-61, , localizado na Casa do Comércio/ Edifício Josias Albuquerque, situado à Avenida Visconde de Suassuna, nº 265, Santo Amaro - Recife-PE, CEP: 50.050-540, neste ato representado de acordo com a Portaria "N" Sesc/PE nº XXX de XXX, pelo _____ do Sesc Pernambuco, o Sr. _____ *(nome)*, _____ *(nacionalidade),* _____ *(estado civil)*, Identidade nº. _____ *(Órgão exp.)*, CPF/MF nº _____-___, residente e domiciliado na _____/__ *(cidade/estado)*, e _____ *(razão social da empresa)* (**FORNECEDOR**), CNPJ: _____/____-__, estabelecida na _____ *(endereço)*, (*telefone*) _____-____, *(e-mail)* _____@_____, neste ato representado por _____ *(cargo na empresa)*, o(a) Sr.(a) _____ *(nome)*, _____ *(nacionalidade)*, _____ *(estado civil)*, _____ *(profissão),* Identidade nº. _____ *(Órgão exp.)*, CPF nº. _____-___, residente e domiciliado (a) em _____/__ *(cidade/estado)*, têm entre si justo e convencionado a presente **ATA DE REGISTRO DE PREÇOS**, oriunda do **PREGÃO ELETRÔNICO SESC/DR-PE Nº 006/2026** e das **Requisições de Compra nº 197805**, que se regerá pelas cláusulas e condições seguintes, obrigando as partes às condições adiante registradas, que mútua e reciprocamente, outorgam, estipulam, aceitam e se obrigam a cumprir por si e seus sucessores.

CLÁUSULA SEGUNDA – DO OBJETO

2.1 – Constitui objeto da presente Ata de Registro de Preços o **REGISTRO DE PREÇO, PARA RENOVAÇÃO DE LICENÇAS DE ANTIVÍRUS, KASPERSKY ENDPOINT SECURITY, A FIM DE SUPRIR AS NECESSIDADES DO PARQUE TECNOLÓGICO DO SESC-DR/PE, COM UMA SOLUÇÃO DE SOFTWARE INTEGRADO DE SEGURANÇA E PROTEÇÃO CONTRA SPAM DE E-MAIL, VAZAMENTOS DE DADOS, TENTATIVAS DE PHISHING E HACKING, ANTIMALWARE - VÍRUS, RANSOMWARE, CAVALOS DE TRÓIA, ROOTKITS, BACKDOORS, COM CRIPTOGRAFIA DE DADOS, SEGURANÇA MÓVEL, SEGURANÇA DA PLATAFORMA OFFICE 365, GERENCIAMENTO DE DISPOSITIVOS MÓVEIS, GERENCIAMENTO DE SISTEMAS E TREINAMENTO DE EQUIPE TÉCNICA SESC/DR-PE, COM ATUALIZAÇÕES PARA 36 (TRINTA E SEIS) MESES, SERVIÇO DE IMPLANTAÇÃO E MANUTENÇÃO, A FIM DE GARANTIR A PROTEÇÃO LÓGICA DOS COMPUTADORES, SERVIDORES FÍSICOS E VIRTUAIS, MS OFFICE 365, BEM COMO, EQUIPAMENTOS MÓVEIS (LAPTOPS, SMARTPHONES, TABLETS) INTEGRADOS A REDE LÓGICA DE DADOS DO SESC-DR/PE E DEMAIS UNIDADES DA INSTITUIÇÃO, CONTRA A ENTRADA E ATUAÇÃO DE MALWARES E PROGRAMAS MALICIOSOS,** em conformidade com as especificações técnicas descritas no **TERMO DE REFERÊNCIA (ANEXO I)** observadas as demais condições estabelecidas no instrumento

convocatório e seus anexos, do edital do **PREGÃO ELETRÔNICO SESC/DR-PE Nº 006/2026**, observadas as demais condições estabelecidas nesta Ata de Registro de Preços.

2.2 – Sendo Registro de Preços o GERENCIADOR não se obriga a adquirir o objeto desta Ata de Registro de Preços, podendo realizar contratação com terceiros, sempre que se mostre mais vantajosa para a entidade.

2.3 – **O quantitativo total, constante na CLÁUSULA QUARTA desta Ata de Registro de Preços é estimado e representa as previsões do GERENCIADOR durante o prazo de 12 (doze) meses.**

2.4 – **O FORNECEDOR deverá permanecer em condições de fornecer os produtos dentro dos prazos definidos pelo GERENCIADOR, durante o período de validade da Ata de Registro de Preços, não cabendo ao FORNECEDOR nenhum adicional além do que foi previsto inicialmente.**

2.5 – A qualquer tempo, durante o período de vigência de 12 (doze) meses, os preços registrados poderão ser revistos em decorrência de eventual redução dos preços praticados no mercado ou de fato que eleve o custo dos serviços ou bens registrados, cabendo ao GERENCIADOR convocar o FORNECEDOR para promover as negociações necessárias, até que se defina o novo valor, conforme o entendimento da legislação vigente.

CLÁUSULA TERCEIRA – DA VIGÊNCIA

3.1 – A vigência inicial da presente ATA será de **12 (doze) meses**, com início a partir da data de sua assinatura, podendo ser prorrogada, desde que pesquisa de mercado demonstre que o preço se mantém vantajoso, conforme o Artigo 45 da Resolução Sesc Nº 1.593/2024.

3.1.1 – **A presente Ata de Registro de Preços poderá ser prorrogada, além do prazo estipulado no subitem acima, até o limite máximo de 36 (trinta e seis) meses.**

3.1.2 – **No caso de prorrogação, ficam restabelecidos os termos e as condições iniciais da presente Ata de Registro de Preços, inclusive quantitativos.**

3.2 – Não haverá, ao final do período de vigência, no caso do não fornecimento total ou do fornecimento parcial do objeto, obrigação do GERENCIADOR no que diz respeito a ressarcimentos ou indenizações.

CLÁUSULA QUARTA – DAS ESPECIFICAÇÕES TÉCNICAS DOS PRODUTOS E QUANTITATIVOS

4.1 – Pelo fornecimento dos produtos, o GERENCIADOR pagará ao FORNECEDOR a importância do preço unitário dos itens, conforme a Proposta Comercial do FORNECEDOR, nas especificações contidas abaixo:

LOTE ÚNICO						
ITEM	PRODUTO	DESCRIÇÃO	PREVISÃO PARA AQUISIÇÃO IMEDIATA	QUANTIDADE TOTAL A SER REGISTRADA (UND.)	VALOR (R$)	
					UNITÁRIO	TOTAL

SESC – Serviço Social do Comércio | Departamento Regional em Pernambuco | www.sescpe.org.br
Casa do Comércio/Edifício Josias Albuquerque | Avenida Visconde de Suassuna, nº 265, Santo Amaro - Recife-PE.
CEP: 50.050-540 TEL + 55 81 3216 1739

XX	*(Descrição completa do item, conforme ANEXO I)*		*XX*	*XX*	xx,xx *(extenso)*	xx,xx *(extenso)*
⋮	⋮		⋮	⋮	⋮	⋮
XX	*(Descrição completa do item, conforme ANEXO I)*		*XX*	*XX*	xx,xx *(extenso)*	xx,xx *(extenso)*
VALOR DO LOTE: R$ XX.XXX,XX.						

4.2 – A presente Ata de Registro de Preços poderá ser acrescida em até 50% (cinquenta por cento) de seu(s) quantitativo(s) inicialmente registrado(s), mediante acordo entre as Partes.

4.3 – É permitido que outros licitantes habilitados venham a praticar o menor preço registrado, chamados na ordem de classificação, desde que assinem a Ata de Registro de Preços.

4.3.1 – A empresa _____, CNPJ _____/____-__, Endereço _____, Representante Legal _____, Identidade nº. _____ e CPF nº _____, aderiu ao menor preço registrado. (ou: não houve licitante que aderiu ao menor preço registrado).

4.4 – DETALHAMENTO E ESPECIFICAÇÃO TÉCNICA DA SOLUÇÃO

ITEM 1: LICENÇAS DE ANTIMALWARE

Servidor de administração e console administrativa

1. A console deverá ser acessada via WEB (HTTPS) ou MMC;
2. Console deverá ser baseada no modelo cliente/servidor;
3. Compatibilidade com Windows Failover Clustering ou outra solução de alta disponibilidade;
4. Deverá permitir a atribuição de perfis para os administradores da Solução de AntiMalware;
5. Deverá permitir incluir usuários do AD para logarem na console de administração;
6. Console deverá ser totalmente integrada com suas funções e módulos caso haja a necessidade no futuro de adicionar novas tecnologias tais como, criptografia, Patch management e MDM;
7. As licenças deverão ser por subscrição anual (12 meses), ou seja, expirado a validade do produto as funcionalidades de atualização e acesso ao serviço de inteligência de ameaças (Kaspersky Security Network) serão desativadas, sendo necessária a renovação para manter a proteção eficaz.
8. Capacidade de remover remotamente e automaticamente qualquer solução de AntiMalware (própria ou de terceiros) que estiver presente nas estações e servidores;
9. Capacidade de instalar remotamente a solução de AntiMalware nas estações e servidores Windows, através de compartilhamento administrativo, login script e/ou GPO de Active Directory;
10. Deverá registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria;
11. Deverá armazenar histórico das alterações feitas em políticas;
12. Deverá permitir voltar para uma configuração antiga da política de acordo com o histórico de alterações efetuadas pelo administrador apenas selecionando a data em que a política foi alterada;

13. Deverá ter a capacidade de comparar a política atual com a anterior, informando quais configurações foram alteradas;
14. A solução de gerência deverá permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas;
15. Através da solução de gerência, deverá ser possível verificar qual licença está aplicada para determinado computador;
16. Capacidade de instalar remotamente a solução de segurança em smartphones e tablets de sistema iOS, Android e Windows;
17. Capacidade de instalar remotamente qualquer app em smartphones e tablets de sistema iOS;
18. A solução de gerência centralizada deverá permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle;
19. Deverá ter a capacidade de criar regras para limitar o tráfego de comunicação cliente/servidor por subrede com os seguintes parâmetros: KB/s e horário;
20. Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux e Mac) protegidos pela solução AntiMalware;
21. Capacidade de gerenciar smartphones e tablets (Android e iOS) protegidos pela solução de segurança;
22. Capacidade de instalar atualizações em computadores de teste antes de instalar nos demais computadores da rede;
23. Capacidade de gerar pacotes customizados (auto executáveis) contendo a licença e configurações do produto;
24. Capacidade de atualizar os pacotes de instalação com as últimas vacinas;
25. Capacidade de fazer distribuição remota de qualquer software, ou seja, deverá ser capaz de remotamente enviar qualquer software pela estrutura de gerenciamento de AntiMalware para que seja instalado nas máquinas clientes;
26. A comunicação entre o cliente e o servidor de administração deverá ser criptografada;
27. Capacidade de desinstalar remotamente, através da console de gerenciamento, qualquer software instalado nas máquinas clientes;
28. Deverá permitir a realocação de máquinas novas na rede para um determinado grupo sem ter um agente ou endpoint instalado utilizando os seguintes parâmetros:

    a) Nome do computador;
    b) Nome do domínio;
    c) Range de IP;
    d) Sistema Operacional;
    e) Máquina virtual

29. Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas;
30. Deverá 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;
31. Capacidade de monitorar diferentes subnets de rede a fim de encontrar máquinas novas para serem adicionadas à proteção;
32. 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;
33. 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 AntiMalware instalado. Caso não possuir, deverá instalar o AntiMalware automaticamente;

34. Capacidade de agrupamento de máquina por características comuns entre as mesmas, por exemplo: agrupar todas as máquinas que não tenham o AntiMalware instalado, agrupar todas as máquinas que não receberam atualização nos últimos 2 dias, etc.;
35. 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;
36. Deverá fornecer as seguintes informações dos computadores:

a) Se o AntiMalware está instalado;
b) Se o AntiMalware está iniciado;
c) Se o AntiMalware está atualizado;
d) Minutos/horas desde a última conexão da máquina com o servidor administrativo;
e) Minutos/horas desde a última atualização de vacinas;
f) Data e horário da última verificação executada na máquina;
g) Versão do AntiMalware instalado na máquina;
h) Se é necessário reiniciar o computador para aplicar mudanças;
i) Data e horário de quando a máquina foi ligada;
j) Quantidade de vírus encontrados (contador) na máquina;
k) Nome do computador;
l) Domínio ou grupo de trabalho do computador;
m) Data e horário da última atualização de vacinas;
n) Sistema operacional com Service Pack;
o) Quantidade de processadores;
p) Quantidade de memória RAM;
q) Usuário (s) logado(s) naquele momento, com informações de contato (caso disponíveis no Active Directory);
r) Endereço IP;
s) Aplicativos instalados, inclusive aplicativos de terceiros, com histórico de instalação, contendo data e hora que o software foi instalado ou removido;
t) Atualizações do Windows Updates instaladas;
u) Informação completa de hardware contendo: processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de áudio, adaptadores de rede, monitores, drives de CD/DVD;
v) Vulnerabilidades de aplicativos instalados na máquina;

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

a) Alteração de Gateway Padrão;
b) Alteração de subrede;
c) Alteração de domínio;
d) Alteração de servidor DHCP;
e) Alteração de servidor DNS;
f) Alteração de servidor WINS;
g) Resolução de Nome;
h) Disponibilidade de endereço de conexão SSL;
i) Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet;

SESC – Serviço Social do Comércio | Departamento Regional em Pernambuco | www.sescpe.org.br
Casa do Comércio/Edifício Josias Albuquerque | Avenida Visconde de Suassuna, nº 265, Santo Amaro - Recife-PE.
CEP: 50.050-540 TEL + 55 81 3216 1739

39. Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes;
40. Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de AntiMalware;
41. Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos;
42. Capacidade de eleger qualquer computador cliente como repositório de vacinas e de pacotes de instalação, sem que seja necessária a instalação de um servidor administrativo completo, onde outras máquinas clientes irão atualizar-se e receber pacotes de instalação, a fim de otimizar tráfego da rede;
43. Capacidade de fazer deste repositório de vacinas um gateway para conexão com o servidor de administração, para que outras máquinas que não consigam conectar-se diretamente ao servidor possam usar este gateway para receber e enviar informações ao servidor administrativo;
44. Capacidade de exportar relatórios para os seguintes tipos de arquivos: PDF, HTML e XML;
45. Capacidade de gerar traps SNMP para monitoramento de eventos;
46. Capacidade de enviar e-mails para contas específicas em caso de algum evento;
47. Listar em um único local, todos os computadores não gerenciados na rede;
48. Deverá encontrar computadores na rede através de no mínimo três formas: Domínio, Active Directory e subredes;
49. Capacidade de baixar novas versões do AntiMalware direto pela console de gerenciamento, sem a necessidade de importá-los manualmente;
50. Deverá possuir documentação da estrutura do banco de dados para geração de relatórios a partir de ferramentas específicas de consulta (Crystal Reports, por exemplo).
51. Capacidade de ligar máquinas via Wake on Lan para realização de tarefas (varredura, atualização, instalação, etc.), inclusive de máquinas que estejam em subnets diferentes do servidor;
52. Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado intervalo de tempo);
53. Deverá através de opções de optimizações fazer com que o computador gerenciado conceda recursos à outras aplicações, mantendo o AntiMalware ativo, porém sem comprometer o desempenho do computador;
54. Deverá permitir a configuração de senha no endpoint e configurar quando que será necessário a utilizá-la, (ex: Solicitar senha quando alguma tarefa de scan for criada localmente no endpoint);
55. Permitir fazer uma verificação rápida ou detalhada de um dispositivo removível assim que conectado no computador, podendo configurar a capacidade máxima em GB da verificação;
56. Deverá ser capaz de configurar quais eventos serão armazenados localmente, nos eventos do Windows ou ainda se serão mostrados na tela para o colaborador, sejam estes eventos informativos, de alertas ou de erros;
57. Capacidade de realizar atualização incremental de vacinas nos computadores clientes;
58. Deverá armazenar localmente e enviar ao servidor de gerência a ocorrência de vírus com os seguintes dados, no mínimo:

    a) Nome do vírus;
    b) Nome do arquivo infectado;
    c) Data e hora da detecção;
    d) Nome da máquina ou endereço IP;
    e) Ação realizada.

59. Capacidade de reportar vulnerabilidades de softwares presentes nos computadores;
60. Capacidade de listar updates nas máquinas com o respectivo link para download;
61. Deverá criar um backup de todos arquivos deletados em computadores para que possa ser restaurado através de comando na Console de administração;
62. Deverá ter uma quarentena na própria console de gerenciamento, permitindo baixar um artefato ou enviar direto para análise do fabricante;
63. Capacidade de realizar inventário de hardware de todas as máquinas clientes;
64. Capacidade de realizar inventário de aplicativos de todas as máquinas clientes;
65. Capacidade de diferenciar máquinas virtuais de máquinas físicas.
66. Possuir as seguintes características de CRIPTOGRAFIA:

a) O acesso ao recurso criptografado (arquivo, pasta ou disco) deve ser garantido mesmo em caso o usuário tenha esquecido a senha, através de procedimentos de recuperação;
b) Utilizar, no mínimo, algoritmo AES com chave de 256 bits;
c) Capacidade de criptografar completamente o disco rígido da máquina, adicionando um ambiente de pré-boot para autenticação do usuário;
d) Capacidade de utilizar Single Sign-On para a autenticação de pré-boot;
e) Permitir criar vários usuários de autenticação pré-boot;
f) Capacidade de criar um usuário de autenticação pré-boot comum com uma senha igual para todas as máquinas a partir da console de gerenciamento; g)
g) Capacidade de criptografar drives removíveis de acordo com regra criada pelo administrador, com as opções:

i. Criptografar somente os arquivos novos que forem copiados para o disco removível, sem modificar os arquivos já existentes;
ii. Criptografar todos os arquivos individualmente;
iii. Criptografar o dispositivo inteiro, de maneira que não seja possível listar os arquivos e pastas armazenadas;
iv. Criptografar o dispositivo em modo portátil, permitindo acessar os arquivos em máquinas de terceiros através de uma senha;

h) Capacidade de selecionar pastas e arquivos (por tipo, ou extensão) para serem criptografados automaticamente. Nesta modalidade, os arquivos devem estar acessíveis para todas as máquinas gerenciadas pela mesma console de maneira transparente para os usuários;
i) Capacidade de criar regras de exclusões para que certos arquivos ou pastas nunca sejam criptografados;
j) Capacidade de selecionar aplicações que podem ou não ter acesso aos arquivos criptografados;
k) Verifica compatibilidade de hardware antes de aplicar a criptografia;
l) Possibilita estabelecer parâmetros para a senha de criptografia;
m) Bloqueia o reuso de senhas;
n) Bloqueia a senha após um número de tentativas pré-estabelecidas;
o) Capacidade de permitir o usuário solicitar permissão a determinado arquivo criptografado para o administrador mediante templates customizados;
p) Permite criar exclusões para não criptografar determinados discos rígidos através de uma busca por nome do computador ou nome do dispositivo;
q) Permite criptografar as seguintes pastas pré-definidas: meus documentos, Favoritos, Desktop, arquivos temporários e arquivos do outlook;

SESC – Serviço Social do Comércio | Departamento Regional em Pernambuco | www.sescpe.org.br
Casa do Comércio/Edifício Josias Albuquerque | Avenida Visconde de Suassuna, nº 265, Santo Amaro - Recife-PE.
CEP: 50.050-540 TEL + 55 81 3216 1739

r) Permite utilizar variáveis de ambiente para criptografar pastas customizadas;
s) Capacidade de criptografar arquivos por grupos de extensão, tais como: Documentos do office, Document, arquivos de áudio etc.;
t) Permite criar um grupo de extensões de arquivos a serem criptografados;
u) Capacidade de criar regra de criptografia para arquivos gerados por aplicações;
v) Permite criptografia de dispositivos móveis mesmo quando o endpoint não possuir comunicação com a console de gerenciamento;
w) Capacidade de deletar arquivos de forma segura após a criptografia;
x) Capacidade de criptografar somente o espaço em disco utilizado;
y) Deve ter a opção de criptografar arquivos criados a partir de aplicações selecionadas pelo administrador;
z) Capacidade de bloquear aplicações selecionadas pelo administrador de acessarem arquivos criptografados;
aa) Deve permitir criptografar somente o espaço utilizado em dispositivos removíveis tais como pendrives, HD externo, etc.;
bb) Capacidade de criptografar discos utilizando a criptografia BitLocker da Microsoft;
cc) Deve ter a opção de utilização de TPM para criptografia através do BitLocker;
dd) Capacidade de fazer Hardware encryption;

67 – Deverá possui as seguintes características para o gerenciamento do sistema:

a) Capacidade de detectar softwares de terceiros vulneráveis, criando assim um relatório de softwares vulneráveis;
b) Capacidade de corrigir as vulnerabilidades de softwares, fazendo o download centralizado da correção ou atualização e aplicando essa correção ou atualização nas máquinas gerenciadas de maneira transparente para os usuários;
c) Capacidade de gerenciar licenças de softwares de terceiros;
d) Capacidade de registrar mudanças de hardware nas máquinas gerenciadas;
e) Capacidade de gerenciar um inventário de hardware, com a possibilidade de cadastro de dispositivos (ex: router, switch, projetor, acessório, etc.), informando data de compra, local onde se encontra, service tag, número de identificação e outros;
f) Possibilita fazer distribuição de software de forma manual e agendada;
g) Suporta modo de instalação silenciosa;
h) Suporte a pacotes MSI, exe, bat, cmd e outros padrões de arquivos executáveis;
i) Possibilita fazer a distribuição através de agentes de atualização;
j) Utiliza tecnologia multicast para evitar tráfego na rede;
k) Possibilita criar um inventário centralizado de imagens;
l) Capacidade de atualizar o sistema operacional direto da imagem mantendo os dados do usuário;
m) Suporte a WakeOnLan para deploy de imagens;
n) Capacidade de atuar como servidor de atualização do Windows podendo fazer deploy de patches;
o) Suporta modo de teste, podendo atribuir alguns computadores para receberem as atualizações de forma automática para avaliação de alterações no comportamento;
p) Capacidade de gerar relatórios de vulnerabilidades e patches;

SESC – Serviço Social do Comércio | Departamento Regional em Pernambuco | www.sescpe.org.br
Casa do Comércio/Edifício Josias Albuquerque | Avenida Visconde de Suassuna, nº 265, Santo Amaro - Recife-PE.
CEP: 50.050-540 TEL + 55 81 3216 1739

q) Possibilita criar exclusões para aplicação de patch por tipo de sistema operacional, Estação de trabalho e Servidor ou por grupo de administração;
r) Permite iniciar instalação de patch e correções de vulnerabilidades ao reiniciar ou desligar o computador;
s) Permite baixar atualizações para o computador sem efetuar a instalação;
t) Permite o administrador instalar somente atualizações aprovadas, instalar todas as atualizações (exceto as bloqueadas) ou instalar todas as atualizações incluindo as bloqueadas;
u) Capacidade de instalar correções de vulnerabilidades de acordo com a Severidade;
v) Permite selecionar produtos a serem atualizados pela console de gerenciamento;
w) Permite selecionar categorias de atualizações para serem baixadas e instaladas, tais como: atualizações de segurança, ferramentas, drivers, etc.;
x) Capacidade de adicionar caminhos específicos para procura de vulnerabilidades e updates em arquivos;
y) Capacidade de instalar atualizações ou correções somente em computadores definidos, em grupos definidos ou em uma porcentagem de computadores conforme selecionado pelo administrador;
z) Capacidade de configurar o reinício do computador após a aplicação das atualizações e correções de vulnerabilidades;
aa) Deve permitir selecionar o idioma das aplicações que serão atualizadas;
bb) Permitir agendar o sincronismo entre a console de gerenciamento e os sites da Microsoft para baixar atualizações recentes;

68. Compatibilidade:

a) Microsoft Windows Server 2012 (Todas edições);
b) Microsoft Windows Server 2012 R2 (Todas edições);
c) Microsoft Windows Server 2016 x64 ou superior;
d) Microsoft Windows 10 todas as edições x32 e x64 ou superior;
e) Microsoft Windows 11 todas edições ou superior.

69. Suportar as seguintes plataformas virtuais:

a) Vmware: Workstation 12.x Pro ou superior, vSphere 5.5, vSphere 6 e vShere 6.5 ou superior;
b) Microsoft Hyper-V: 2008, 2008 R2, 2008 R2 SP1, 2012, 2012 R2, 2016;
c) Microsoft VirtualPC 6.0.156.0;
d) Parallels Desktop 7 e 11;
e) Oracle VM VirtualBox 4.0.4-70112 (Somente logon como convidado);
f) Citrix XenServer 6.2, 6.5, 7.0 e 7.2
g) Citrix XenDesktop 7.14
h) Citrix Provisioning Services 7.14 DOS SERVIDORES

SISTEMA OPERACIONAL WINDOWS:

1. Deve prover as seguintes proteções:

a) Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
b) Autoproteção contra-ataques aos serviços/processos do antivírus;
c) Firewall com IDS;

d) Controle de vulnerabilidades do Windows e dos aplicativos instalados;

2. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
3. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;
4. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

a) Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
b) Gerenciamento de tarefa (criar ou excluir tarefas de verificação);
c) Leitura de configurações;
d) Modificação de configurações;
e) Gerenciamento de Backup e Quarentena;
f) Visualização de relatórios;
g) Gerenciamento de relatórios;
h) Gerenciamento de chaves de licença;
i) Gerenciamento de permissões (adicionar/excluir permissões acima);

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

a) Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;
b) 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 à rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados;

6. Capacidade de, separadamente, selecionar o número de processos que irão executar funções de varredura em tempo real, o número de processos que executarão a varredura sob demanda e o número máximo de processos que podem ser executados no total;
7. Bloquear malwares tais como Cryptlockers mesmo quando o ataque vier de um computador sem antivírus na rede;
8. Capacidade de resumir automaticamente tarefas de verificação que tenham sido paradas por anormalidades (queda de energia, erros, etc);
9. Capacidade de automaticamente pausar e não iniciar tarefas agendadas caso o servidor esteja em rodando com fonte ininterrupta de energia (uninterruptible Power supply UPS);
10. Em caso de erros, deve ter capacidade de criar logs e traces automaticamente, sem necessidade de outros softwares;
11. Capacidade de configurar níveis de verificação diferentes para cada pasta, grupo de pastas ou arquivos do servidor;
12. Capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado no servidor;
13. Capacidade de criar uma lista de máquina que nunca serão bloqueadas mesmo quando infectadas;
14. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;

SESC – Serviço Social do Comércio | Departamento Regional em Pernambuco | www.sescpe.org.br
Casa do Comércio/Edifício Josias Albuquerque | Avenida Visconde de Suassuna, nº 265, Santo Amaro - Recife-PE.
CEP: 50.050-540 TEL + 55 81 3216 1739

15. 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;
16. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
17. 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;
18. Capacidade de verificar somente arquivos novos e alterados;
19. Capacidade de escolher qual tipo de objeto composto será verificado (ex: arquivos comprimidos, arquivos autodescompressores, .PST, arquivos compactados por compactadores binários, etc.);
20. Capacidade de verificar objetos usando heurística;
21. Capacidade de configurar diferentes ações para diferentes tipos de ameaças;
22. Capacidade de agendar uma pausa na verificação;
23. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;
24. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

    a) Perguntar o que fazer, ou;
    b) Bloquear acesso ao objeto;
    c) Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração preestabelecida pelo administrador);
    d) Caso positivo de desinfecção, restaurar o objeto para uso;
    e) Caso negativo de desinfecção, mover para quarentena ou apagar (de acordo com a configuração preestabelecida pelo administrador);

25. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
26. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;
27. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;
28. Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa;
29. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros;
30. Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning).
31. Compatibilidade:

    a) Microsoft Windows Storage Server SP2 Workgroup Edition;
    b) Microsoft Windows Server 2012 Essentials / Standard / Foundation / Datacenter;
    c) Microsoft Windows Server 2012 R2 Essentials / Standard / Foundation / Datacenter;
    d) Microsoft Windows Server 2012 Core Essentials / Standard / Foundation / Datacenter;
    e) Microsoft Windows Server 2012 R2 Core Essentials / Standard / Foundation / Datacenter;
    f) Microsoft Windows Storage Server 2012 (Todas edições);
    g) Microsoft Windows Storage Server 2012 R2 (Todas edições);
    h) Microsoft Windows Hyper-V Server 2012;

SESC – Serviço Social do Comércio | Departamento Regional em Pernambuco | www.sescpe.org.br
Casa do Comércio/Edifício Josias Albuquerque | Avenida Visconde de Suassuna, nº 265, Santo Amaro - Recife-PE.
CEP: 50.050-540 TEL + 55 81 3216 1739

i) Microsoft Windows Hyper-V Server 2012 R2 ou superior;
j) Windows Server 2016 Essentials/Standard/Datacenter/Core ou posterior;
k) Windows Storage Server 2016 ou posterior;
l) Windows Hyper-V Server 2016.

MS OFFICE 365

1. Características Gerais

1.1 A solução deve ser entregue no modelo de "Software as a Service", onde servidor e console administrativa são hospedados na nuvem.
1.2 Acesso a console administrativa via HTTPS.
1.3 A integração com o Office 365 deve ser realizada via API.
1.4 A autenticação da integração deve ser realizada via protocolo seguro OAuth 2.0.
1.5 A solução deve prover módulos de proteção para a suíte Microsoft Office 365 (Exchange Online, OneDrive, SharePoint e Teams).
1.6 A console deve prover painel de informações exibindo as informações principais da operação e do estado dos componentes de proteção.
1.7 Capacidade de geração de relatórios em no mínimo formato ".pdf".
1.8 Capacidade de geração de relatório instantâneo;
1.9 Capacidade de agendamento automático de relatórios.
1.10 A solução deve verificar o tráfego de e-mails inbound e outbound.
1.11 Deve possuir quarentena para armazenar artefatos detectados como maliciosos.
1.12 A quarentena deve possuir no mínimo as seguintes opções:

1.12.1 Exibir detalhes do item;
1.12.2 Excluir item;
1.12.3 Liberar item;
1.12.4 Filtrar itens;
1.12.5 Salvar item em disco;

1.13 A gestão da solução deve ser realizada por usuário com perfil de administrador.
1.14 Deve ser possível atribuir perfil de administrador para um usuário na console de administração.

2. Módulos de Proteção

2.1 Anti-malware

2.1.1 Deve proteger as caixas de correio contra vírus, worms, trojans, entre outras ameaças que podem ser enviadas via e-mail.
2.1.2 Análise das ameaças deve ser realizada por no mínimo as seguintes tecnologias:

2.1.2.1. Assinaturas;
2.1.2.2. Heurística;
2.1.2.3. Comportamento;
2.1.2.4. Consulta ao repositório de inteligência do fabricante.

SESC – Serviço Social do Comércio | Departamento Regional em Pernambuco | www.sescpe.org.br
Casa do Comércio/Edifício Josias Albuquerque | Avenida Visconde de Suassuna, nº 265, Santo Amaro - Recife-PE.
CEP: 50.050-540 TEL + 55 81 3216 1739

2.1.3 Capacidade de detectar ataques conhecidos e desconhecidos.
2.1.4 Ao detectar um malware, a solução deve tomar uma ou mais ações de acordo com a configuração do administrador, possibilitando no mínimo:

2.1.4.1. Excluir a mensagem e colocá-la em quarentena;
2.1.4.2. Excluir anexo infectado e colocá-lo em quarentena;
2.1.4.3. Colocar tag no assunto;
2.1.4.4. Substituir arquivo por mensagem personalizada;

2.1.5 Notificar ao administrador sobre novas ameaças encontradas
2.1.6 Notificar ao proprietário da caixa sobre mensagens excluídas.
2.1.7 Deve analisar arquivos nas seguintes aplicações:

2.1.7.1. Exchange Online
2.1.7.2. OneDrive
2.1.7.3. SharePoint
2.1.7.4. Teams

2.2 Anti-phishing

2.2.1 Deve proteger as caixas de correio contra phishing e links maliciosos enviados em mensagens de e-mail, evitando assim infecção por malware, roubo de dados pessoas e acesso a sites fraudulentos.
2.2.2 Deve validar o conteúdo das mensagens para detectar phishing, utilizando as seguintes tecnologias:

2.2.2.1. SPF (Sender Policy Framework)
2.2.2.2. DKIM (Domain-based Message Authentication)
2.2.2.3. DMARC (Domain-based Message Authentication, Reporting and Conformance)
2.2.2.4. Consulta ao repositório de inteligência do fabricante.

2.2.3 Capacidade de detectar ataques conhecidos e desconhecidos.
2.2.4 Ao detectar um link de phishing, a solução deve tomar uma ou mais ações de acordo com a configuração do administrador, possibilitando no mínimo:

2.2.4.1. Excluir a mensagem e coloca-la em quarentena;
2.2.4.2. Permitir;
2.2.4.3. Mover para pasta “Lixo eletrônico”;
2.2.4.4. Colocar tag no assunto;

2.2.5 Notificar ao administrador sobre novas mensagens encontradas.
2.2.6 Notificar ao proprietário da caixa sobre mensagens excluídas.
2.2.7 Permitir a criação de exclusões por e-mail completo ou máscara.

2.3 Anti-spam / Mass Mail

2.3.1 Deve proteger as caixas de correio contra e-mail não solicitados “SPAM” e e-mails enviados em massa.

2.3.2 A verificação deve ser realizada através dos seguintes métodos:

2.3.2.1. Verificação de cabeçalho, conteúdo, anexos e elementos de design;
2.3.2.2. Algoritmos linguísticos e heurísticos;
2.3.2.3. Consulta ao repositório de inteligência do fabricante;

2.3.3 Ao detectar um SPAM, a solução deve tomar uma ou mais ações de acordo com a configuração do administrador, possibilitando no mínimo:

2.3.3.1. Permitir;
2.3.3.2. Mover para a pasta “Lixo eletrônico”;
2.3.3.3. Colocar tag no assunto;

2.3.4 Notificar ao administrador sobre novas ameaças encontradas
2.3.5 Notificar ao proprietário da caixa sobre mensagens excluídas.
2.3.6 Permitir a criação de exclusões por e-mail completo ou máscara.

2.4 Filtro de conteúdo

2.4.1 Deve possibilitar a filtragem de anexos em mensagens de e-mail.
2.4.2 Capacidade de detectar anexos pelos seguintes parâmetros:

2.4.2.1. Formato do arquivo;
2.4.2.2. Nome completo do arquivo;
2.4.2.3. Nome do arquivo com máscara;
2.4.2.4. Arquivos MS Office com macro;

2.4.3 Ao detectar um anexo que se encaixe em uma das regras, a solução deve possibilitar as seguintes ações:

2.4.3.1. Excluir mensagem e coloca-la em quarentena;
2.4.3.2. Excluir anexo e colocá-lo em quarentena;
2.4.3.3. Permitir
2.4.3.4. Colocar tag no assunto;
2.4.3.5. Substituir arquivo por mensagem personalizada;

2.4.4 Notificar ao administrador sobre novas ameaças encontradas
2.4.5 Notificar ao proprietário da caixa sobre mensagens excluídas.
2.4.6 Permitir a criação de exclusões por e-mail completo ou máscara.

DOS SERVIDORES

SISTEMA OPERACIONAL LINUX:

1. Deve prover as seguintes proteções:

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

SESC – Serviço Social do Comércio | Departamento Regional em Pernambuco | www.sescpe.org.br
Casa do Comércio/Edifício Josias Albuquerque | Avenida Visconde de Suassuna, nº 265, Santo Amaro - Recife-PE.
CEP: 50.050-540 TEL + 55 81 3216 1739

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

a) Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
b) 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;
c) Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;
d) Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados;

3. Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares;
4. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
5. 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;
6. Capacidade de verificar objetos usando heurística;
7. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;
8. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;
9. Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).
10. Compatibilidade:

a) Plataforma 32-bits:

a.1) Red Hat Enterprise Linux 6.7;
a.2) Red Hat Enterprise Linux 6.8 ou posterior;
a.3) CentOS-6.7;
a.4) CentOS-6.8 ou posterior;
a.5) Ubuntu 14.04 LTS;
a.6) Ubuntu 16.04 LTS;
a.7) Ubuntu 16.10 LTS ou posterior;
a.8) Debian GNU/Linux 7.10;
a.9) Debian GNU/Linux 7.11;
a.10) Debian GNU/Linux 8.6;
a.11) Debian GNU/Linux 8.7 ou posterior;

b) Plataforma 64-bits:

b.1) Red Hat Enterprise Linux 6.7;
b.2) Red Hat Enterprise Linux 6.8;
b.3) Red Hat Enterprise Linux 7.2;

SESC – Serviço Social do Comércio | Departamento Regional em Pernambuco | www.sescpe.org.br
Casa do Comércio/Edifício Josias Albuquerque | Avenida Visconde de Suassuna, nº 265, Santo Amaro - Recife-PE.
CEP: 50.050-540 TEL + 55 81 3216 1739

b.4) Red Hat Enterprise Linux 7.3 ou posterior;
b.5) CentOS-6.7;
b.6) CentOS-6.8;
b.7) CentOS-7.2;
b.8) CentOS-7.3 ou posterior;
b.9) Ubuntu 14.04 LTS;
b.10) Ubuntu 16.04 LTS;
b.11) Ubuntu 16.10 LTS ou posterior;
b.12) Debian GNU/Linux 7.10;
b.13) Debian GNU/Linux 7.11;
b.14) Debian GNU/Linux 8.6;
b.15) Debian GNU/Linux 8.7 ou posterior;
b.16) OpenSUSE 42.2;
b.17) SUSE Linux Enterprise Server 12 ou posterior;
b.18) OracleLinux 7.3 ou posterior;
b.19) Novell Open Enterprise Server 11 SP3;
b.20) Novell Open Enterprise Server 2015 SP1 ou posterior;

DAS ESTAÇÕES DE TRABALHO

SISTEMA OPERACIONAL WINDOWS:

1. Deve prover as seguintes proteções:

a) AntiMalware de Arquivos residente (anti-spyware, anti-trojan, antimalware, etc) que verifique qualquer arquivo criado, acessado ou modificado; b) AntiMalware de Web (módulo para verificação de sites e downloads contra vírus);
b) AntiMalware de E-mail (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos);
c) AntiMalware de Mensagens Instantâneas;
d) O Endpoint deve possuir opção para rastreamento por linha de comando, parametrizável, com opção de limpeza;
e) Firewall com IDS;
f) Autoproteção (contra-ataques aos serviços/processos do AntiMalware);
g) Controle de dispositivos externos;
h) Controle de acesso a sites por categoria, ex: Bloquear conteúdo adulto, sites de jogos, etc;
i) Controle de acesso a sites por horário;
j) Controle de acesso a sites por usuários;
k) Controle de acesso a websites por dados, ex: Bloquear websites com conteúdos de vídeo e áudio;
l) Controle de execução de aplicativos;
m) Controle de vulnerabilidades do Windows e dos aplicativos instalados;

2. Capacidade de escolher quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
3. As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa);

4. Capacidade de detecção de presença de AntiMalware de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;
5. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do AntiMalware, (ex: Win32.Trojan.banker) para que qualquer objeto detectado com o veredicto escolhido seja ignorado;
6. Capacidade de adicionar aplicativos a uma lista de aplicativos confiáveis, onde as atividades de rede, atividades de disco e acesso ao registro do Windows não serão monitoradas;
7. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);
8. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
9. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O AntiMalware deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;
10. Ter a capacidade de fazer detecções por comportamento, identificando ameaças avançadas sem a necessidade de assinaturas;
11. Capacidade de verificar somente arquivos novos e alterados;
12. Capacidade de verificar objetos usando heurística;
13. Capacidade de agendar uma pausa na verificação;
14. Deve permitir a filtragem de conteúdo de URL avançada efetuando a classificação dos sites em categorias;
15. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;
16. O AntiMalware de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

    a) Perguntar o que fazer, ou;
    b) Bloquear acesso ao objeto;
    c) Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
    d) Caso positivo de desinfecção:
    e) Restaurar o objeto para uso;
    f) Caso negativo de desinfecção, mover para quarentena ou apagar (de acordo com a configuração pré- estabelecida pelo administrador);

17. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o AntiMalware deve realizar um backup do objeto;
18. Capacidade de verificar e-mails recebidos e enviados nos protocolos POP3, IMAP, NNTP, SMTP e MAPI;
19. Capacidade de verificar links inseridos em e-mails contra phishings;
20. Capacidade de verificar tráfego nos browsers: Internet Explorer, Firefox e Opera;
21. Capacidade de verificação de corpo e anexos de e-mails usando heurística;
22. O AntiMalware de e-mail, ao encontrar um objeto potencialmente perigoso, deve:

    a) Perguntar o que fazer, ou;
    b) Bloquear o e-mail;
    c) Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
    d) Caso positivo de desinfecção, restaurar o e-mail para o usuário;

e) Caso negativo de desinfecção, mover para quarentena ou apagar o objeto (de acordo com a configuração pré-estabelecida pelo administrador);

24. Caso o e-mail conter código que parece ser, mas não é definitivamente malicioso, o mesmo deve ser mantido em quarentena;
25. Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados;
26. Capacidade de filtrar anexos de e-mail, apagando-os ou renomeandoos de acordo com a configuração feita pelo administrador;
27. Capacidade de verificação de tráfego HTTP e qualquer script do Windows Script Host (JavaScript, Visual Basic Script, etc), usando heurísticas;
28. Deve ter suporte total ao protocolo Ipv6;
29. Capacidade de alterar as portas monitoradas pelos módulos de Web e E-mail;
30. Na verificação de tráfego web, caso encontrado código malicioso o programa deve:

a) Perguntar o que fazer, ou;
b) Bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio, ou;
c) Permitir acesso ao objeto;

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

a) Verificação on-the-fly, onde os dados são verificados enquanto são recebidos em tempo-real, ou;
b) Verificação de buffer, onde os dados são recebidos e armazenados para posterior verificação;

32. Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo AntiMalware de web;
33. Deve possuir módulo que analise as ações de cada aplicação em execução no computador, gravando as ações executadas e comparando-as com sequências características de atividades perigosas. Tais registros de sequências devem ser atualizados juntamente com as vacinas;
34. Deve possuir módulo que analise cada macro de VBA executada, procurando por sinais de atividade maliciosa;
35. Deve possuir módulo que analise qualquer tentativa de edição, exclusão ou gravação do registro, de forma que seja possível escolher chaves específicas para serem monitoradas e/ou bloqueadas;
36. Deve possuir módulo de bloqueio de Phishing, com atualizações incluídas nas vacinas, obtidas pelo Anti-Phishing Working Group (http://www.antiphishing.org/);
37. Capacidade de distinguir diferentes subnets e conceder opção de ativar ou não o firewall para uma subnet específica;
38. 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;
39. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:

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

b) 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.

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

a) Discos de armazenamento locais;
b) Armazenamento removível;
c) Impressoras;
d) CD/DVD;
e) Drives de disquete;
f) Modems;
g) Dispositivos de fita;
h) Dispositivos multifuncionais;
i) Leitores de smart card;
j) Dispositivos de sincronização via ActiveSync (Windows CE, Windows Mobile, etc);
k) Wi-Fi;
l) Adaptadores de rede externos;
m) Dispositivos MP3 ou smartphones;
n) Dispositivos Bluetooth;
o) Câmeras e Scanners.

41. 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;
42. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por usuário;
43. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por agendamento;
44. Capacidade de habilitar logging em dispositivos removíveis tais como Pendrive, Discos externos etc.
45. Capacidade de configurar novos dispositivos por Class ID/Hardware ID;
46. Capacidade de limitar a execução de aplicativos por hash MD5, nome do arquivo, versão do arquivo, nome do aplicativo, versão do aplicativo, fabricante/desenvolvedor, categoria (ex: navegadores, gerenciador de download, jogos, aplicação de acesso remoto, etc);
47. Capacidade de bloquear execução de aplicativo que está em armazenamento externo;
48. Capacidade de limitar o acesso dos aplicativos a recursos do sistema, como chaves do registro e pastas/arquivos do sistema, por categoria, fabricante ou nível de confiança do aplicativo;
49. Capacidade de, em caso de epidemia, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web;
50. Capacidade de, caso o computador cliente saia da rede corporativa, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web.
51. Compatibilidade:

a) Microsoft Windows 10 Pro / Enterprise x86 / x64;

SESC – Serviço Social do Comércio | Departamento Regional em Pernambuco | www.sescpe.org.br
Casa do Comércio/Edifício Josias Albuquerque | Avenida Visconde de Suassuna, nº 265, Santo Amaro - Recife-PE.
CEP: 50.050-540 TEL + 55 81 3216 1739

b) Microsoft Windows 11 todas as edições;
c) Microsoft Windows Server 2012 R2 Standard x64;
d) Microsoft Windows Server 2012 Foundation x64;
e) Microsoft Windows Server 2012 Standard x64;
f) Microsoft Small Business Server 2011 Standard x64;
g) Microsoft Windows Server 2008 R2 Standard/Enterprise x64 SP1;
h) Microsoft Windows Server 2008 Standard/Enterprise x86/x64 SP2;
i) Microsoft Windows Server 2016 Standard/Enterprise/datacenter 4 ou posterior;

SISTEMA OPERACIONAL MAC OS X:

1. Deve prover proteção residente para arquivos (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
2. Possuir módulo de web-AntiMalware para proteger contra ameaças durante navegação na internet com possibilidade de analisar endereços https; 3. Possuir módulo de bloqueio á ataques na rede;
4. Possibilidade de bloquear a comunicação entre a máquina atacante e os demais computadores por tempo definido pelo administrador;
5. Capacidade de criar exclusões para computadores que não devem ser monitorados pelo módulo de bloqueio à ataques na rede;
6. Possibilidade de importar uma chave no pacote de instalação;
7. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
8. A instalação e a primeira execução do produto deve ser feita sem a necessidade de reinicialização do computador, de modo que, o produto funcione com toda sua capacidade;
9. Deve possuir suportes a notificações utilizando o Growl;
10. As vacinas devem ser atualizadas pelo fabricante e disponibilizadas aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa);
11. Capacidade de voltar para a base de dados de vacina anterior;
12. Capacidade de varrer a quarentena automaticamente após cada atualização de vacinas;
13. 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 AntiMalware, (ex: Win32.Trojan.banker) para que qualquer objeto detectado com o veredicto escolhido seja ignorado;
14. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);
15. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O AntiMalware deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;
16. Capacidade de verificar somente arquivos novos e alterados;
17. Capacidade de verificar objetos usando heurística;

a) Capacidade de agendar uma pausa na verificação;
b) O AntiMalware de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
c) Perguntar o que fazer, ou;
d) Bloquear acesso ao objeto;
e) Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);

f) Caso positivo de desinfecção, restaurar o objeto para uso;

18. Caso negativo de desinfecção, mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);
19. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o AntiMalware deve realizar um backup do objeto;
20. Capacidade de verificar arquivos de formato de email;
21. Possibilidade de trabalhar com o produto pela linha de comando, com no mínimo opções para atualizar as vacinas, iniciar uma varredura, para o AntiMalware e iniciar o AntiMalware pela linha de comando;
22. Capacidade de ser instalado, removido e administrado pela mesma console central de gerenciamento.
23. Compatibilidade:

a) Mac OS X 10.11 (El Capitan);
b) Mac OS X 10.10 (Yosemite);
c) Mac OS X 10.9 (Mavericks);
d) Mac OS X 10.8 (Mountain Lion);
e) Mac OS X 10.7 (Lion);
f) Mac OS Sierra 10.12;

SISTEMA OPERACIONAL LINUX:

1. Deve prover as seguintes proteções:

a) AntiMalware de arquivos residente (anti-spyware, anti-trojan, antimalware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
b) As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;
c) Capacidade de configurar a permissão de acesso às funções do AntiMalware;
d) Capacidade de criar exclusões por local, máscara e nome da ameaça;
e) Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
f) 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;
g) Dectectar aplicações que possam ser utilizadas como vetor de ataque por hackers;
h) Fazer detecções através de heurística utilizando no mínimo as seguintes opções de nível:

h.1) Alta;
h.2) Média;
h.3) Baixa;
h.4) Recomendado;

i) Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;
j) Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados.

k) Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares;
l) Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
m) Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O AntiMalware deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;

GERENCIAMENTO DE SISTEMAS:

1. Capacidade de criar imagens de sistema operacional remotamente e distribuir essas imagens para computadores gerenciados pela solução e para computadores bare-metal;
2. Deve possibilitar a utilização de servidores PXE na rede para deploy de imagens;
3. Capacidade de detectar softwares de terceiros vulneráveis, criando assim um relatório de softwares vulneráveis;
4. Capacidade de corrigir as vulnerabilidades de softwares, fazendo o download centralizado da correção ou atualização e aplicando essa correção ou atualização nas máquinas gerenciadas de maneira transparente para os usuários;
5. Capacidade de gerenciar licenças de softwares de terceiros;
6. Capacidade de registrar mudanças de hardware nas máquinas gerenciadas;
7. Capacidade de gerenciar um inventário de hardware, com a possibilidade de cadastro de dispositivos (ex: router, switch, projetor, acessório, etc), informando data de compra, local onde se encontra, service tag, número de identificação e outros;
8. Possibilita fazer distribuição de software de forma manual e agendada;
9. Suporta modo de instalação silenciosa;
10. Suporte a pacotes MSI, exe, bat, cmd e outros padrões de arquivos executáveis;
11. Possibilita fazer a distribuição através de agentes de atualização;
12. Utiliza tecnologia multicast para evitar tráfego na rede;
13. Possibilita criar um inventário centralizado de imagens;
14. Capacidade de atualizar o sistema operacional direto da imagem mantendo os dados do usuário;
15. Suporte a WakeOnLan para deploy de imagens;
16. Capacidade de atuar como servidor de atualização do Windows podendo fazer deploy de patches;
17. Suporta modo de teste, podendo atribuir alguns computadores para receberem as atualizações de forma automática para avaliação de alterações no comportamento;
18. Capacidade de gerar relatórios de vulnerabilidades e patches;
19. Possibilita criar exclusões para aplicação de patch por tipo de sistema operacional, Estação de trabalho e Servidor ou por grupo de administração;
20. Permite iniciar instalação de patch e correções de vulnerabilidades ao reiniciar ou desligar o computador;
21. Permite baixar atualizações para o computador sem efetuar a instalação;
22. Permite o administrador instalar somente atualizações aprovadas, instalar todas as atualizações (exceto as bloqueadas) ou instalar todas as atualizações incluindo as bloqueadas;
23. Capacidade de instalar correções de vulnerabilidades de acordo com a severidade;
24. Permite selecionar produtos a serem atualizados pela console de gerenciamento;
25. Permite selecionar categorias de atualizações para serem baixadas e instaladas, tais como: atualizações de segurança, ferramentas, drivers, etc;

26. Capacidade de adicionar caminhos específicos para procura de vulnerabilidades e updates em arquivos;
27. Capacidade de instalar atualizações ou correções somente em computadores definidos, em grupos definidos ou em uma porcentagem de computadores conforme selecionado pelo administrador;
28. Capacidade de configurar o reinício do computador após a aplicação das atualizações e correções de vulnerabilidades;
29. Deve permitir selecionar o idioma das aplicações que serão atualizadas;
30. Permitir agendar o sincronismo entre a console de gerenciamento e os sites da Microsoft para baixar atualizações recentes;

a) Capacidade de verificar objetos usando heurística;
b) Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;
c) Deve possuir função para? escolha da pasta? onde arquivos restaurados de backup deverão ser salvos em local definido pelo cliente; de administração remota através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).

31. Compatibilidade:

a) Plataforma 32-bits:

a.1) Red Hat Enterprise Linux 6.7;
a.2) Red Hat Enterprise Linux 6.8;
a.3) CentOS-6.7;
a.4) CentOS-6.8;
a.5) Ubuntu 14.04 LTS;
a.6) Ubuntu 16.04 LTS;
a.7) Ubuntu 16.10 LTS;
a.8) Debian GNU/Linux 7.10;
a.9) Debian GNU/Linux 7.11;
a.10) Debian GNU/Linux 8.6;
a.11) Debian GNU/Linux 8.7.

b) Plataforma 64-bits:

b.1) Red Hat Enterprise Linux 6.7;
b.2) Red Hat Enterprise Linux 6.8;
b.3) Red Hat Enterprise Linux 7.2;
b.4) Red Hat Enterprise Linux 7.3 e versões superiores;
b.5) CentOS-6.7;
b.6) CentOS-6.8;
b.7) CentOS-7.2;
b.8) CentOS-7.3 e versões superiores;
b.9) Ubuntu 14.04 LTS;
b.10) Ubuntu 16.04 LTS;
b.11) Ubuntu 16.10 LTS e versões superiores;
b.12) Debian GNU/Linux 7.10;
b.13) Debian GNU/Linux 7.11;

SESC – Serviço Social do Comércio | Departamento Regional em Pernambuco | www.sescpe.org.br
Casa do Comércio/Edifício Josias Albuquerque | Avenida Visconde de Suassuna, nº 265, Santo Amaro - Recife-PE.
CEP: 50.050-540 TEL + 55 81 3216 1739

b.14) Debian GNU/Linux 8.6;
b.15) Debian GNU/Linux 8.7 e versões superiores;
b.16) OpenSUSE 42.2 e versões superiores;
b.17) SUSE Linux Enterprise Server 12 e versões superiores;
b.18) OracleLinux 7.3 e versões superiores;
b.19) Novell Open Enterprise Server 11 SP3 e versões superiores;
b.20) Novell Open Enterprise Server 2015 SP1 e versões superiores

DOS DISPOSITIVOS MÓVEIS TABLETS E SMARTPHONES:

1. **Deve prover as seguintes proteções:**

a) Proteção em tempo real do sistema de arquivos do dispositivo e interceptação e verificação de:

a.1) Proteção contra adware e autodialers;
a.2) Todos os objetos transmitidos usando conexões wireless (porta de infravermelho, Bluetooth) e mensagens EMS, durante sincronismo com PC e ao realizar download usando o browser;
a.3) Arquivos abertos no smartphone;
a.4) Programas instalados usando a interface do smartphone;
a.5) Verificação dos objetos na memória interna do smartphone e nos cartões de expansão sob demanda do usuário e de acordo com um agendamento;
a.6) Deverá isolar em área de quarentena os arquivos infectados;
a.7) Deverá atualizar as bases de vacinas de modo agendado;
a.8) Deverá bloquear spams de SMS através de Black lists;
a.9) Deverá ter função de bloqueio do aparelho caso o SIM CARD for trocado para outro não autorizado com mensagem de aviso ao utilizador do dispositivo;
a.10) Capacidade de desativar por política:
a.11) Wi-fi;
a.12) Câmera;
a.13) Bluetooth.

b) Deverá ter função de limpeza de dados pessoais a distância, em caso de roubo, por exemplo;
c) Capacidade de requerer uma senha para desbloquear o dispositivo e personalizar a quantidade de caracteres para esta senha;
d) Deverá ter firewall pessoal (Android);
e) Capacidade de tirar fotos quando a senha for inserida incorretamente;
f) Possibilidade de instalação remota utilizando o Microsoft System Center Mobile Device Manager 2008 SP1;
g) Capacidade de enviar comandos remotamente de:

g.1) Localizar;
g.1) Bloquear.

h) Capacidade de detectar Jailbreak em dispositivos iOS;
i) Capacidade de bloquear o acesso a site por categoria em dispositivos;
j) Capacidade de bloquear o acesso a sites phishing ou malicioso;

SESC – Serviço Social do Comércio | Departamento Regional em Pernambuco | www.sescpe.org.br
Casa do Comércio/Edifício Josias Albuquerque | Avenida Visconde de Suassuna, nº 265, Santo Amaro - Recife-PE.
CEP: 50.050-540 TEL + 55 81 3216 1739

k) Capacidade de criar containers de aplicativos, separando dados corporativos de dados pessoais;
l) Capacidade de bloquear o dispositivo quando o cartão ?SIM? for substituído;
m) Capacidade de configurar White e blacklist de aplicativos;
n) Capacidade de localizar o dispositivo quando necessário;
o) Permitir atualização das definições quando estiver em roaming;
p) Capacidade de selecionar endereço do servidor para buscar a definição de vírus;
q) Deve permitir verificar somente arquivos executáveis;
r) Deve ter a capacidade de desinfectar o arquivo se possível;
s) Capacidade de agendar uma verificação;
t) Capacidade de enviar URL de instalação por e-mail;
u) Capacidade de fazer a instalação através de um link QRCode;
v) Capacidade de executar as seguintes ações caso a desinfecção falhe:

v.1) Deletar;
v.2) Ignorar;
v.3) Quarentena;
v.4) Perguntar ao usuário.

2. Compatibilidade:

a) Apple iOS 9.0-10.3 ou superior;
b) Android 4.1 ? 7.1.1 ou superior;

ITEM 2: AQUISIÇÃO DE LICENÇAS DO ANTIMALWARE EM AMBIENTE FÍSICO E VIRTUALIZADO

SERVIDOR DE ADMINISTRAÇÃO E CONSOLE ADMINISTRATIVA

1. **Requerimentos Gerais**

a. O software de segurança para ambientes virtuais deve incluir:

a.1) Software AntiMalware sem agente para ambientes virtuais;
a.2) Software AntiMalware baseado em agente para ambientes virtuais;
a.3) Gerenciamento, monitoramento e atualização de software e vacinas centralizados;
a.4) Capacidade de atualizar definições de vírus e padrões de ataques;
a.5) Documentação do administrador;
a.6) Compatibilidade com a rede a ser protegida.

2. **Requerimentos para o AntiMalware sem agente:**

a) O software de AntiMalware sem agente para ambientes virtualizados deve funcionar com as seguintes versões do VMWARE:

a.1) VMWARE ESXi Hypervisor 6.0 update 2;
a.2) VMWARE ESXi Hypervisor 5.5 update 3b;
a.3) VMWARE NSX para Vsphere 6.2.4;

SESC – Serviço Social do Comércio | Departamento Regional em Pernambuco | www.sescpe.org.br
Casa do Comércio/Edifício Josias Albuquerque | Avenida Visconde de Suassuna, nº 265, Santo Amaro - Recife-PE.
CEP: 50.050-540 TEL + 55 81 3216 1739

a.4) VMWARE vCenter 6.0.0a Server ou superior;
a.5) VMWARE vCenter 6.0 Update 2 ou superior;
a.6) VMWARE vCenter 5.5. update 3e;
a.7) VMWARE vShield Endpoint do VMware vCloud Networking and Security 5.5.4.3 suite;
a.8) VMWARE vShield Manager do VMware vCloud Networking and Secruity 5.5.4.3 suite;

b) Requerimentos para o componente de integração ao Servidor:

b.1) Windows Server 2016 Datacenter / Standard x64 ou superior;
b.2) Windows Server 2012 R2 Datacenter / Standard x64;
b.3) Windows Server 2012 R2 Essentials x64;
b.4) Windows Server 2012 Datacenter x64;
b.5) Windows Server 2012 Essentials x64;
b.6) Windows Server 2008 R2 Datacenter / Enterprise / Standard Service Pack 1 x64;
b.7) b.7) Windows Server 2008 Datacenter / Enterprise / Standard Service Pack 2 x86 e x64;

c) Software de AntiMalware sem agente para ambientes virtuais deve proteger os seguintes sistemas operacionais para desktops:

c.1) Windows 10 32/64 bits ou superior;
c.2) Windows 11 todas as edições.

d) Software de AntiMalware sem agente para ambientes virtuais deve proteger os seguintes sistemas operacionais para servidores:

d.1) Windows Server 2008 R2 (x64);
d.2) Windows Server 2012 R2;
d.3) Windows Server 2012 sem ReFS (Resilient File system) suporte (x64);
d.4) Windows Server 2012 R2 (x64) quando utilizado com o VMware vSphere 5.5 update 2 ou posterior;
d.5) Windows Server 2016 Datacenter x64 ou superior;

3. **O AntiMalware sem agente para ambientes virtuais deve prover as seguintes funcionalidades:**

a) Proteção contra malware em tempo real e durante a verificação agendada sem a necessidade de qualquer agente instalado no computador convidado;
b) Integração com a tecnologia Vmware vShield Manager para proteger o sistema de arquivos do computador;
c) Integração com a tecnologia Vmware Network Extensibility SDK para prover proteção no nível de rede, implementado para monitorar e bloquear atividade maliciosa na rede bem como endereços de URL com a habilidade de notificar o usuário sobre os bloqueios efetuados;
d) Possuir integração com Vmware NSX;
e) Deve possuir IPS;
f) Possuir integração com as etiquetas de segurança NSX;
g) Adicionar automaticamente novas máquinas virtuais ao escopo de proteção, sem a necessidade de qualquer instalação adicional;

h) Deve automatizar a instalação se baseando em políticas de segurança identificadas pelo VMware NSX;
i) Fazer scan em máquinas virtuais mesmo desligadas;
j) Verificar os dispositivos removíveis tais como (Pendrive, Cartões, etc);
k) O produto deve permitir parar o scan após x (minutos) da inicialização da verificação;
l) O produto deve ser capaz de ser configurado até três níveis de segurança sendo eles: Recomendado, alto ou baixo;
m) Provê as seguintes opções caso encontre uma ameaça:

m.1) Escolher a ação automaticamente;
m.2) Desinfectar ou bloquear caso a desinfecção falhe;
m.3) Desinfectar ou deletar caso a desinfecção falhe;
m.4) Deletar ou bloquear caso a deleção falhe;
m.5) Bloquear;

n) A solução deve permitir configurar um tamanho máximo de um arquivo para ser verificado. Ex: Caso o arquivo compactado tenha mais de 10 MB não verificar;
o) Permitir configurar o tempo máximo de scan em um arquivo;
p) Verificar os malwares do tipo trojans, auto-dialers, adware, etc;
q) Permitir verificar drives de rede;
r) Permitir verificar todos os arquivos do sistema com a exceção dos arquivos selecionados pelo administrador;
s) Fazer a verificação dos arquivos que possuem somente as extensões definidas pelo administrador;
t) Permitir a criação de exceções por pastas ou arquivos podendo incluir subpastas;
u) Permitir a criação de perfis de políticas diferentes para cada grupo de máquinas virtuais;
v) Possuir a integração com SNMP;
w) Capacidade de bloquear ataques vindos pela rede;
x) Verificar os endereços da web por possíveis ameaças;
y) Permitir a criação de exceções para URLs que não devem ser verificadas;
z) Permitir enviar uma mensagem de bloqueio caso colaborador acesse um site malicioso;
aa) Proteção baseada em nuvem contra novas ameaças, permitindo a aplicação se comunicar com a fabricante do software para poder dar um veredito a um arquivo tanto na proteção em tempo real como na verificação agendada;
bb) Atualizações centralizadas no sistema com a proteção especializada para virtualização sem a necessidade de distribuir atualizações para cada máquina convidada;
cc) Possibilidade de verificação sob demanda ou manual nas máquinas virtuais selecionadas;
dd) Verificação de: arquivos selecionados, pastas ou todo o sistema na verificação agendada de todas as máquinas virtuais;
ee) Capacidade de implementar a solução de segurança sem a necessidade de reiniciar o Hypervisor ou entrar no modo de manutenção; ff) Tecnologia que previne a verificação do mesmo arquivo mais de uma vez;
gg) Prevenir múltipla verificação em arquivos iguais mesmo que estejam em máquinas virtuais diferentes;
hh) Bloquear, isolar e remover os vírus notificando o usuário e o administrador;
ii) Possuir uma única console de gerenciamento para todos os componentes de proteção;
jj) Uma única console de gerenciamento tanto para o ambiente virtual como para o ambiente físico;
kk) Capacidade de ver a estrutura de administração tanto física como lógica assim como é apresentado no Vmware vCenter;
ll) Informações detalhadas sobre os eventos e tarefas de implementação nas máquinas virtuais;

SESC – Serviço Social do Comércio | Departamento Regional em Pernambuco | www.sescpe.org.br
Casa do Comércio/Edifício Josias Albuquerque | Avenida Visconde de Suassuna, nº 265, Santo Amaro - Recife-PE.
CEP: 50.050-540 TEL + 55 81 3216 1739

mm) Capacidade de aplicar configurações de segurança diferentes para cada grupo de máquinas virtuais;
nn) Criar exceções pelo nome do arquivo, pelo endereço dos arquivos e pela máscara dos arquivos;
oo) Permitir exportar e importar listas com exceções;
pp) Criar listas com exceções frequentes de acordo com as recomendações da Microsoft;
qq) Permitir verificar drives de rede conectados na máquina virtual se necessário;
rr) Capacidade de excluir drives de rede do escopo de proteção;
ss) Suporta o Vmware vMotion, se uma máquina é transferida de um ESXi para outro a proteção não é interrompida; tt) Criar backup de arquivos deletados pela proteção;
uu) Suportar esquema de licenciamento pela quantidade de máquinas virtuais protegidas e de acordo com o número de CPU cores;
vv) Componente dedicado para integração centralizada com o ambiente virtual para evitar carga no Vmware vCenter e impedir chamadas de soluções de AntiMalware; ww) Suporte para ativar o software utilizando um código sob subscrição; xx) Providenciar informações sobre números de objetos verificados; yy) Providenciar informações sobre detalhes da definição de AntiMalware;
zz) Suportar verificação de certificados SSL para comunicação entre o mecanismo de antimalware, servidor de gerenciamento e Componentes de infraestrutura do VMware;
aaa) Importar ou exportar a lista de exclusões e verificações nas tarefas de verificação e perfis de proteção.

4. Requerimentos para AntiMalware em ambientes virtualizados baseado em agente (conector);

a) Para ser instalado em uma infraestrutura virtualizada, um dos seguintes hypervisors devem ser instalados:

a.1) Vmware ESXi 5.1 com os últimos updates;
a.2) Vmware ESXi 5.5 com os últimos updates;
a.3) Vmware ESXi 6.0 com os últimos updates;
a.4) Vmware ESXi 6.5 com os últimos updates;
a.5) Vmware vCenter 5.1, 5.5, 6.0 ou 6.5 com todos os patches instalados;
a.6) Microsoft Windows Server 2012 R2 Hyper-V (no modo instalação completa ou modo core) com todos os updates disponíveis;
a.7) Microsoft Windows Server 2016 Hyper-V (no modo instalação completa ou core) com todos os updates disponíveis;
a.8) Citrix XenServer 6.5 SP1;
a.9) Citrix XenServer 7;
a.10) Citrix XenDesktop 7.9 ou 7.11;
a.11) Citrix Provisioning Services 7.9 ou 7.11;
a.12) Vmware Orizon View 7
a.13) KVM (Kernel-based Virtual Machine) executando sistema operacional Ubuntu Server 14.04 LTS;
a.14) KVM CentOS 7.2;
a15) Red Hat Enterprise Linux Server 7 patch 1

b) O AntiMalware baseado em agente deve prover proteção para as máquinas virtuais no Vmware hypervisor nos seguintes sistemas operacionais para Desktop:

b.1) Windows 10 Pro/Enterprise/Enterprise LTSB/RS1 x86/x64;

SESC – Serviço Social do Comércio | Departamento Regional em Pernambuco | www.sescpe.org.br
Casa do Comércio/Edifício Josias Albuquerque | Avenida Visconde de Suassuna, nº 265, Santo Amaro - Recife-PE.
CEP: 50.050-540 TEL + 55 81 3216 1739

b.2) Windows 11 todas as edições.

c) O AntiMalware baseado em agente deve prover proteção para máquinas virtuais no Vmware Hypervisor com os seguintes sistemas operacionais para servidores:

c.1) Windows Server 2008 Service Pack 2 Todas edições x64;
c.2) Windows Server 2008 R2 SP1 Todas edições x64;
c.3) Windows Server 2012 R2 Todas edições (X64);
c.4) Windows Server 2012 Todas edições (x64);
c.5) Windows Server 2016 todas edições x64.

d) A Suite VMware tools deve ser instalada para prover integração entre o Hypervisor, máquinas virtuais e o conector;

e) O AntiMalware baseado em agente deve prover proteção para máquinas virtuais no Microsoft Hyper-V Hypervisor com os seguintes sistemas operacionais para Desktop;

e.1) Windows 10 Pro/Enterprise x86/x64;
e.2) Windows 11 todas as edições

f) O AntiMalware baseado em agente deve prover proteção para máquinas virtuais no Microsoft Hyper-V Hypervisor com os seguintes sistemas operacionais para Servidores;

f.1) Windows Server 2012 R2 x64;
f.2) Windows Server 2012 x64;
f.3) Windows Server 2008 R2 todas edições SP1 x64;
f.4) Windows Server 2008 SP2 Todas edições;
f.5) Windows Server 2016 Todas edições x64.
f.6) Um serviço de integração deve ser instalado na máquina virtual executada pelo Microsoft Hyper-V

g) O AntiMalware baseado em agente deve prover proteção para máquinas virtuais no Citrix Hypervisor com os seguintes sistemas operacionais para Desktop:

g.1) Microsoft Windows 10 Pro/Enterprise x86/x64;
g.2) Microsoft Windows 11 todas as edições.

h) O AntiMalware baseado em agente deve prover proteção para máquinas virtuais no Citrix Hypervisor com os seguintes sistemas operacionais para Servidores;

h.1) Windows Server 2012 R2 x64;
h.2) Windows Server 2012 x64;
h.3) Windows Server 2008 R2 Todas edições SP1 x64;
h.4) Windows Server 2016 Todas edições x64;

i) O AntiMalware baseado em agente deve suportar a proteção das seguintes máquinas virtuais Linux:

i.1) Debian GNU/Linux 8.5 32/64 bits;

SESC – Serviço Social do Comércio | Departamento Regional em Pernambuco | www.sescpe.org.br
Casa do Comércio/Edifício Josias Albuquerque | Avenida Visconde de Suassuna, nº 265, Santo Amaro - Recife-PE.
CEP: 50.050-540 TEL + 55 81 3216 1739

i.2) Ubuntu Server 14.04 LTS 32/64 bits;
i.3) Ubuntu Server 16.04 LTS x64;
i.4) CentOS 6.8 x64;
i.5) CentOS 7.2 x64;
i.6) Red hat Enterprise Linux Server 6.7 x64;
i.7) Red Hat Enterprise Linux Server 7.2 x64;
i.8) SUSE Linux Enterprise Server 12 SP1 x64;

j) O AntiMalware baseado em agente deve ser compatível com as soluções usadas para criar e gerenciar um a infraestrutura de máquinas virtuais VDI:

j.1) Citrix Provisioning Services 7.1;
j.2) Citrix XenDesktop 7.5

k) O AntiMalware baseado em agente deve prover proteção para máquinas virtuais no KVM Hypervisor com os seguintes sistemas operacionais Linux:

k.1) Ubuntu Server 14.04 LTS;
k.2) CentOS 7;

l) O AntiMalware baseado em agente deve prover proteção para máquinas virtuais no KVM com os seguintes sistemas operacionais para servidores:

l.1) Windows Server 2012 R2 x64;
l.2) Windows Server 2012 x64;
l.3) Windows Server 2008 R2 Standard SP1 x64;
l.4) Ubuntu Server 14.04 LTS;
l.5) CentOS 7;

m) O AntiMalware baseado em agente deve prover as funcionalidades abaixo;

m.1) AntiMalware e monitoramento residente;
m.2) Proteção contra rootkits e auto dialers a sites pagos;
m.3) Verificação por heurística para detectar e bloquear malwares desconhecidos;
m.4) Transferir a verificação de malware e as tarefas intensivas para uma única máquina virtual responsável pela proteção;
m.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;
m.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;
m.7) Deve atender HIPPA e SOX;
m.8) Proteção de e-mail contra malwares verificando tráfego de entrada e saída nos protocolos IMAP, SMTP, POP3, MAPI e NNTP independente do cliente de e-mail;
m.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;
m.10) Bloqueia banners e pop-ups nas páginas web;

SESC – Serviço Social do Comércio | Departamento Regional em Pernambuco | www.sescpe.org.br
Casa do Comércio/Edifício Josias Albuquerque | Avenida Visconde de Suassuna, nº 265, Santo Amaro - Recife-PE.
CEP: 50.050-540 TEL + 55 81 3216 1739

m.11) Capacidade de detectar e bloquear sites de phishing;
m.12) Proteção contra ameaças não conhecidas baseadas no comportamento;
m.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;
m.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;
m.15) O Firewall deve permitir a criação de regras para pacotes de rede em protocolos específicos (TCP, UDP) e portas;
m.16) Permitir a criação de regras de rede para programas específicos;
m.17) Proteção contra-ataques de hackers utilizando o firewall com IDS/IPS e regras de atividade de rede para as aplicações mais conhecidas;
m.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;
m.19) Não carregar nenhum módulo de segurança na máquina virtual e sim no appliance virtual;
m.20) Permitir a verificação em máquinas linux;
m.21) Deve ser capaz de usar o Microsoft System Center Virtual Machine Manager (SCVMM) para fazer deploy dos appliances virtuais;
m.22) Os virtuais appliances responsáveis pela verificação devem ser baseados em Linux;
m.23) Capacidade de desativar a interface local na inicialização do sistema para diminuir consumo de memória;
m.24) Permitir selecionar a forma de conexão ao appliance virtual de três formas diferentes:

i. Utilizando Multicast;
ii. Selecionando Servidor de integração;
iii. Utilizando uma lista de appliances virtuais

m.25) Deve ser capaz de verificar vírus, worms, trojans, toolkits, adware, autodialers e outros tipos de ameaças em máquinas Linux;
m.26) Deve ser capaz de criar exclusões em máquinas linux por nome ou pasta;
m.27) Capacidade de verificar arquivos por formato ou extensão em máquinas Linux;
m.28) Permitir configurar limite de tempo de verificação em um arquivo tanto para máquinas Linux como Windows;
m.29) Permitir alterar o modo de scan para no mínimo três opções diferentes:

i. Verificação automática;
ii. Verificar os arquivos no acesso ou na modificação;
iii. Somente no acesso;

m.30) 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;
m.31) Capacidade de garantir privilégios na utilização de dispositivos externos para usuários específicos do AD;

SESC – Serviço Social do Comércio | Departamento Regional em Pernambuco | www.sescpe.org.br
Casa do Comércio/Edifício Josias Albuquerque | Avenida Visconde de Suassuna, nº 265, Santo Amaro - Recife-PE.
CEP: 50.050-540 TEL + 55 81 3216 1739

m.32) 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);
m.33) Capacidade de controlar acesso na internet por horário e por usuário do AD;
m.34) Atualizações centralizadas permitindo que parte do banco de dados de definições seja armazenado na máquina de proteção (SVM);
m.35) Habilidade de executar tarefas de detecção de vulnerabilidades em aplicações instaladas nos computadores incluindo opção de submeter um relatório de qualquer vulnerabilidade encontrada;
m.36) Integração com o Windows Update para instalar patches de acordo com as vulnerabilidades encontradas;
m.37) Capacidade de instalar e distribuir remotamente componentes do antivirus em todas as máquinas protegidas sem utilização de ferramentas de terceiros;
m.38) Armazenar as informações de arquivos verificados para evitar um novo scan sobre o arquivo e aumentar consumo de recursos;
m.39) Bloquear, neutralizar e remover os malwares com a opção de notificar os administradores;
m.40) Console de gerenciamento única para todos os componentes de proteção;
m.41) Console de gerenciamento única tanto para ambientes físicos como virtuais;
m.42) Console única para administração de máquinas virtuais Linux e Windows;
m.43) Provê informações detalhadas sobre os eventos e execução de tarefas;
m.44) Capacidade de aplicar configurações de segurança diferentes para cada grupo de máquinas virtuais;
m.45) Salvar o backup dos arquivos deletados;

5. Suporta as seguintes tecnologias Vmware: vMotion, Distributed resource Scheduler;
6. Suporta as seguintes tecnologias Citrix: Virtual User Drive, Citrix Receiver, Multi-stream ICA, XenMotion Live Migration, Automated VM protection and recovery, Dynamic memory control;
7. Suportar as seguintes tecnologias Hyper-V: Live migration, Cluster shared volumes, Dynamic memory, Live backup;
8. Suportar rollback do banco de dados de definições;
9. Suportar o esquema de licença de acordo com o número de máquinas virtuais protegidas e de acordo com o número de hardware CPU cores;
10. Requerimentos para administração centralizada, monitoramento e update do software para ambientes virtualizados:

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

a.1) Microsoft Windows 10 Education RS1;
a.2) Microsoft Windows 10 Education 32/64 bits;
a.3) Microsoft Windows 10 Enterprise RS1 e Professional RS1 32/64 bits;
a.4) Microsoft Windows 10 Enterprise e Professional 32/64 bits;
a.5) Microsoft Windows 11 todas as edições;
a.6) Microsoft Windows Small Business Server 2008 Standard x64;
a.7) Microsoft Windows Small Business Server 2008 Premium x64;
a.8) Microsoft Windows Server 2008 Todas edições 32/64 bits;
a.9) Microsoft Windows Server 2008 R2 Todas edições 32/64 bits;

a.10) Microsoft Windows Server 2012 Todas edições 32/64 bits;
a.11) Microsoft Windows Server 2012 R2 Todas edições 32/64 bits;
a.12) Microsoft Windows Server 2016 x64;

11. Banco de dados Suportados pela console de administração centralizada:

a) Microsoft SQL Server Express 2008;
b) Microsoft SQL Server Express 2008 R2;
c) Microsoft SQL Server Express 2008 R2 Service Pack 2;
d) Microsoft SQL Server 2005;
e) Microsoft SQL Server 2008;
f) Microsoft SQL Server 2008 R2;
g) Microsoft SQL Server 2012;
h) Microsoft SQL Server 2014 Todas as edições x64
i) MySQL Enterprise versions 5.0.67, 5.0.77, 5.0.85, 5.087 Service Pack 1, 5.091;
j) MySQL Enterprise versions 5.0.60 Service Pack 1, 5.0.70, 5.0.82 Service Pack 1, 5.0.90;

12. Requerimentos Console de administração instalada em ambientes virtualizados:

a) Vmware: Workstation 9.x, Workstation 10.x;
b) Microsoft Hyper-V: 2008, 2008 R2, 2012, 2012 R2
c) Microsoft Virtual PC 2007 (6.0.156.0)
d) Parallels Desktop 7;
e) Citrix XenServer 6.1 e 6.2;
f) Oracle VM VirtualBox 4.0.4-70112

13. O console de administração centralizada deve prover as seguintes funcionalidades:

a) Deve ser compatível com Microsoft SCVMM;
b) Capacidade de desativar a interface local do agente (conector) para diminuir uso de memória;
c) Instalação do AntiMalware a partir de uma única distribuição;
d) Seleção de instalação dependendo do número de pontos protegidos;
e) Capacidade de ler informações do AD para obter dados que some com as contas dos computadores na organização;
f) Capacidade de fazer a instalação automática através dos grupos gerenciados;
g) Capacidade de realocar computadores de acordo com endereço IP, tipo do sistema operacional e localização no AD;
h) Instalação centralizada;
i) Remoção centralizada (manual ou automática) de aplicações incompatíveis através do servidor de administração;
j) Capacidade de instalar o AntiMalware de diferentes formas: RPC, GPO, agente de administração;
k) Capacidade de atualizar pacotes de instalação com as últimas atualizações;
l) Atualizar de forma automática a versão do AntiMalware e as definições;
m) Procurar automaticamente por vulnerabilidades nas aplicações e sistemas operacionais presentes da rede;
n) Capacidade de proibir instalação/execução de aplicações;
o) Capacidade de gerenciar I/O de dispositivos externos;
p) Gerenciar a atividade do usuário na internet;
q) Capacidade de testar as atualizações antes de aplicar para o ambiente;

SESC – Serviço Social do Comércio | Departamento Regional em Pernambuco | www.sescpe.org.br
Casa do Comércio/Edifício Josias Albuquerque | Avenida Visconde de Suassuna, nº 265, Santo Amaro - Recife-PE.
CEP: 50.050-540 TEL + 55 81 3216 1739

r) Capacidade de executar instalações automáticas baseado no sistema de proteção dedicado, tais como: Vmware ESXi, Microsoft Hyper-V, Citrix XenServer virtualization ou hypervisor;
s) Criar os usuários baseados em RBAC;
t) Criar a hierarquia dos servidores de administração e tem capacidade de gerenciar cada um deles através de uma única console de gerenciamento;

ITEM 3: KASPERSKY MANAGED DETECTION AND RESPONSE BRAZILIAN EDITION

a. **Detecção e Resposta Gerenciada**

a.1. Do monitoramento, identificação e investigação dos eventos de segurança cibernética

a.1.1. O serviço de monitoramento deverá utilizar informações extraídas de registros gerados pelos sistemas monitorados.
a.1.2. Deverá ser instalado agentes específicos nos servidores e desktops, objetivando coletar informações mais detalhadas para o serviço de monitoramento, desde que seja plenamente compatível com o sistema onde será instalado e não afete o desempenho dos serviços.
a.1.3. A análise das informações correlacionadas deve ser realizada com auxílio de bases globais de inteligência cibernética em conjunto com a expertise dos profissionais do fabricante, com vistas a reduzir ao máximo os falsos positivos.
a.1.4. É obrigatório que a comunicação entre equipamentos e soluções do fabricante instalados nos dispositivos e qualquer infraestrutura onde esses dados sejam processados ocorra de forma segura, utilizando algoritmos criptográficos para preservar o sigilo das informações.
a.1.5. Deverá ser feita a investigação e a classificação dos eventos monitorados, aplicando os principais frameworks de gestão de incidentes de segurança cibernética bem como boas práticas de mercado na detecção e triagem dos eventos de segurança, objetivando minimizar a presença de falsos positivos na abertura de incidentes de segurança.
a.1.6. O serviço de monitoramento deverá ser capaz de coletar e realizar a correlação de eventos dos sistemas e ativos monitorados, permitindo uma visão mais abrangente do alcance das ações maliciosas, bem como de possível movimentação lateral do atacante dentro da rede.
a.1.7. O monitoramento deverá ser capaz de identificar as principais ameaças, bem como táticas, técnicas e procedimentos de ataque descritos na base de conhecimento MITRE ATT&CK, sem prejuízo do uso de outras bases de conhecimento ou serviços de inteligência de ameaças, para complementação da capacidade de identificação de atividades maliciosas.
a.1.8. Deverá monitorar e avaliar criticamente os serviços, traçando curvas de comportamento, definindo a volumetria média e identificando comportamentos anômalos, visando antecipar a identificação de incidentes de segurança.
a.1.9. A solução deverá prover inteligência de proteção contra ataques cibernéticos a nível global, sendo responsável por pesquisar novos tipos de ataques, vírus, malwares, botnets, vulnerabilidades e afins com intuito de melhoria contínua de detecção e mitigação destes males dentro dos serviços e ativos de segurança monitorados.
a.1.10. O fabricante deverá utilizar solução para registro de incidente de segurança, acessível pela equipe técnica do GERENCIDOR, para indicar ações de contenção,

SESC – Serviço Social do Comércio | Departamento Regional em Pernambuco | www.sescpe.org.br
Casa do Comércio/Edifício Josias Albuquerque | Avenida Visconde de Suassuna, nº 265, Santo Amaro - Recife-PE.
CEP: 50.050-540 TEL + 55 81 3216 1739

comunicar à equipe do GERENCIADOR sobre o andamento do tratamento dos incidentes.

b. **Compatibilidade:**

b.2. É suportada por qualquer um dos seguintes navegadores:

b.2.1. Apple Safari versões mais recentes
b.2.2. Google Chrome versões mais recentes
b.2.3. Microsoft Edge
b.2.4. Mozilla Firefox versões mais recentes

c. **Requisitos de rede:**

c.1. Em condições médias de carga: um canal full-duplex com largura de banda de pelo menos 1,7 Kbps para cada ativo.
c.2. Em condições de carga máxima: um canal full-duplex com largura de banda de pelo menos 2,7 Kbps para cada ativo.
c.3. Compatibilidade de sensor de endpoint
c.4. O agente de endpoint deve ser compatível com os seguintes sistemas operacionais, para no mínimo a coleta e envio dos dados/telemetria ao SOC do fabricante:
c.5. Microsoft Windows 7 e superiores;
c.6. macOS 10.14-11;
c.7. CentOS 6.7 ou superior;
c.8. Debian GNU / Linux 9.4 ou superior;
c.9. Linux Mint 19 ou superior;
c.10. Oracle Linux 7.3 ou superior;
c.11. Red Hat Enterprise Linux 6.7 ou superior;
c.12. SUSE Linux Enterprise Server 12 SP5 ou superior;
c.13. Ubuntu 18.04 LTS ou superior.

d. **Capacidades técnicas**

d.1. Deve possuir console web própria do serviço, além de integração nativa com a console do “software de segurança e antivírus para servidores físicos, microcomputadores e smartphones/tablets”
d.2. A console deve possuir dashboards com as informações principais, apresentando no mínimo:
d.3. Número de incidentes e status
d.4. Quantidade de dispositivos monitorados
d.5. Deve possuir mecanismo de notificações, com no mínimo as seguintes opções:
d.6. E-mail
d.7. Telegram
d.8. Deve permitir o envio de relatórios.
d.9. O agente deve enviar a telemetria em tempo real para o SoC do fabricante;
d.10. O serviço deve compreender monitoramento dos dados enviados e alertas gerados em um regime 24x7x365.

d.11. O envio e armazenamento da telemetria, devem respeitar as principais legislações de proteção de dados, como GDPR e LGPD.
d.12. O SoC do fabricante deve possuir datacenters em pelo menos duas localidades em diferentes países.
d.13. O SoC do fabricante deve possuir equipes de analistas em pelo menos 3 regiões (países) incluindo Brasil.
d.14. Os dados coletados devem passar por no mínimo:
d.15. Modelos de Machine Learning/Inteligência Artificial;

e. **Análise humana;**

e.1. Correlação com IoA's (indicadore de ataque);
e.2. Emulação em sandbox (quando necessário);
e.3. Após análise, informações sobre atividades potencialmente maliciosas, devem ser apresentadas no portal como "Incidentes"
e.4. O Incidente deve possuir no mínimo as seguintes informações:
e.5. Resumo
e.6. Prioridade (Baixa, Média e Alta)
e.7. Recomendação
e.8. Data de criação e data de atualização
e.9. Correlacionamento com táticas/técnicas do Framewok MITRE ATT&CK
e.10. Dispositivos afetados
e.11. IoC's de host e de rede
e.12. Descrição completa em linha do tempo

f. **O incidente pode receber ações de resposta recomendada disparadas pela equipe de SoC, compreendendo no mínimo as seguintes ações:**

f.1. Transferir arquivo para o SoC;
f.2. Isolar um dispositivo;
f.3. Desabilitar isolamento de dispositivo;
f.4. Deletar chave de registro;
f.5. Dump de memória;
f.6. As ações devem ser aprovadas no portal por profissional do gerenciador, com a opção de habilitar aprovação automática.
f.7. Deve possuir console mult-tenant com a possibilidade de separar ativos.
f.8. Deve possuir campos para o mult-tenant para melhor visualização: f.9. Name;
f.10. Status;
f.11. Descrição;
f.12. Criado em;
f.13. Agente de endpoint

g. **As funcionalidades relacionadas a detecção e resposta solicitadas nesse item, devem ser operadas na mesma console de gerenciamento da solução de endpoint;**

g1. A solução deve oferecer módulo focado em capacidades de EDR "Endpoint Detection and Response", incluindo no mínimo as seguintes capacidades:
g2. O agente deve ter capacidade de coletar e processar dados relacionadas ao veredito e ao contexto da ameaça;

g3. Deve fornecer graficamente a visualização da cadeia do ataque;
g4. Deve possuir a capacidade de varredura, para identificar a presença de um artefato detectado em outros dispositivos na rede, através de indicadores de comprometimento (IoC).
g5. A varredura deve oferecer opções de resposta automatizada (sem intervenção do administrador), para serem executadas caso o IoC seja encontrado em outro dispositivo, com no mínimo as seguintes opções:

i. Isolar o host;
ii. Iniciar uma varredura nas áreas críticas;
iii. Quarentenar o objeto;

h. **A solução deve criar um report detalhado sobre o incidente, tendo a capacidade de incluir no mínimo os seguintes dados:**

h.1. Detecções provenientes da solução de endpoint;
h.2. Processos;
h.3. Alterações de registro;
h.4. Conexões remotas;
h.5. Criação de arquivos;
h.6. Varredura por todos os dispositivos executada a partir de indicador de comprometimento (IoC) gerado através da solução e importado pelo administrador.
h.7. Possibilidade de exportar os indicadores de comprometimento (IoC) gerados a partir da solução.

i. **A solução deve oferecer no mínimo as seguintes opções de resposta:**

i.1. Prevenir a execução de um arquivo;
i.2. Quarentenar um arquivo;
i.3. Iniciar uma varredura por IoC;
i.4. Parar um processo;
i.5. Executar um processo;

j. **Ferramenta que possibilite o isolamento do host infectado com no mínimo as características abaixo:**

j.1. A opção de isolamento deve estar disponível junto a visualização do incidente;
j.2. Na configuração padrão, o isolamento deve ser feito de forma granular, permitindo o controle do dispositivo pela console administrativa mesmo após ativação da regra;

CLÁUSULA QUINTA – DA MANUTENÇÃO DO EQUILÍBRIO ECONÔMICO-FINANCEIRO E DO REAJUSTE

5.1 – A qualquer tempo, durante o período de vigência, os preços registrados poderão ser revistos (podendo ser aplicado reajuste, repactuação ou reequilíbrio econômico-financeiro, conforme for o caso) em decorrência de eventual redução dos preços praticados no mercado ou de fato que eleve o custo dos serviços ou bens registrados, cabendo ao GERENCIADOR convocar o FORNECEDOR para promover as negociações necessárias, até que se defina o novo valor, conforme previsto no Artigo 51 da Resolução Sesc Nº 1.593/2024.

SESC – Serviço Social do Comércio | Departamento Regional em Pernambuco | www.sescpe.org.br
Casa do Comércio/Edifício Josias Albuquerque | Avenida Visconde de Suassuna, nº 265, Santo Amaro - Recife-PE.
CEP: 50.050-540 TEL + 55 81 3216 1739

5.2 – DA MANUTENÇÃO DO EQUILÍBRIO ECONÔMICO-FINANCEIRO

5.2.1 – É assegurada a manutenção do equilíbrio econômico-financeiro desta Ata na hipótese de ajustes do mercado, devidamente comprovados pelo FORNECEDOR e conferidos e aprovados pelo GERENCIADOR, mediante Termo Aditivo a Ata de Registro de Preços.

5.2.2 – A solicitação do reequilíbrio econômico-financeiro **não suspende** a obrigação do fornecimento do objeto no prazo contratado, sem prejuízo de outras condições contratuais, a não ser que o GERENCIADOR não se pronuncie sobre à respectiva solicitação no prazo de até 30 (trinta) dias contados do seu protocolo formal, nos termos da CLÁUSULA DÉCIMA TERCEIRA desta Ata de Registro de Preços.

5.2.3 – Frustrada a negociação, o FORNECEDOR será liberado do compromisso assumido e o GERENCIADOR convocará as demais empresas classificadas, visando igual oportunidade de negociação.

5.2.4 – Quando os preços de mercado se tornarem superiores aos preços registrados na presente Ata de Registro de Preços e o FORNECEDOR não puder arcar com seu compromisso, o GERENCIADOR poderá, após comprovação do fato, liberar o FORNECEDOR sem a aplicação das penalidades previstas nesta Ata de Registro de Preços e convocar as demais empresas classificadas, pela ordem, visando igual oportunidade de negociação.

5.2.5 – Não havendo êxito nas negociações, o GERENCIADOR deverá proceder ao cancelamento desta Ata de Registro de Preços, adotando as medidas cabíveis para a obtenção da contratação mais vantajosa.

5.2.6 – Fica vedado o fornecimento dos produtos a preços excessivos ou manifestadamente inexequíveis, face à oferta de mercado no momento da necessidade do GERENCIADOR, devendo necessariamente os preços registrados serem alvo de permanente vigilância pelo fiscal.

5.3 – DO REAJUSTE

5.3.1 – O valor contratual poderá ser reajustado, obedecida à periodicidade mínima permitida legalmente, com base na variação do IGPM-FGV (Índice Geral de Preços do Mercado) da Fundação Getúlio Vargas, ou outro índice que vier a substituí-lo, considerando-se como índice inicial o do último mês anterior ao do início da vigência e como índice final o do último mês anterior ao do que o reajuste seja devido.

5.3.2 – Quando o índice final não for conhecido na data de emissão da fatura, este será estimado com base na última variação disponível, procedendo-se ao correto reajuste na fatura do mês subsequente.

5.3.3 – Nada impede que as Partes possam acordar um percentual de reajuste menor do que o referido índice.

5.3.4 – Caso ocorram mudanças nas condições econômicas atuais que venham a alterar o equilíbrio contratual ou o índice adotado não reflita a real variação dos custos do FORNECEDOR, os valores constantes desta Ata de Registro de Preços serão renegociados entre as Partes.

SESC – Serviço Social do Comércio | Departamento Regional em Pernambuco | www.sescpe.org.br
Casa do Comércio/Edifício Josias Albuquerque | Avenida Visconde de Suassuna, nº 265, Santo Amaro - Recife-PE.
CEP: 50.050-540 TEL + 55 81 3216 1739

5.3.5 – Os valores não pagos na data do vencimento deverão ser corrigidos, desde então, até a data do efetivo pagamento, pela variação do IGPM, ou outro índice que vier a substituí-lo, ocorrida no período e juros de 1% (um por cento) ao mês.

CLÁUSULA SEXTA – DAS CONDIÇÕES DE ENTREGA, DISPOSIÇÕES GERAIS, TREINAMENTO E INFORMAÇÕES COMPLEMENTARES

6.1 – O FORNECEDOR se compromete a fornecer os produtos constantes na CLÁUSULA QUARTA desta Ata de Registro de Preços, pelos preços registrados na presente Ata, durante o período de sua vigência.

6.2 – O FORNECEDOR deverá cumprir rigorosamente os prazos estabelecidos nesta Ata de Registro de Preços e atender a todas as normas de segurança, responsabilizando-se exclusivamente, civil e criminalmente, sem custo adicional ao GERENCIADOR, por todos e quaisquer eventos que ocorrerem no **LOCAL DE ENTREGA**, conforme abaixo:

UTD (UNIDADE DE TECNOLOGIA DIGITAL) DO SESC/PE
Edifício Casa do Comércio/Edifício Josias Albuquerque,
Endereço: Avenida Visconde de Suassuna, 1º andar, n° 265, Santo Amaro, Recife.
CEP: 50.050-540.
Responsável pelo recebimento: Diego Lilioso ou Anselmo William
Telefone: (081) 3216-1683

6.3 – Havendo a possibilidade de obter a solução de AntiMalware via download, deverá o FORNECEDOR realizar os procedimentos de instalação juntamente com o cliente.

6.4 – A **entrega dos produtos** deverá ocorrer conforme a necessidade do GERENCIADOR em **até 10 (dez) dias úteis**, contados da data do recebimento do pedido de compra, emitido pelo GERENCIADOR. A entrega deverá ser previamente agendada com o responsável técnico designado pelo GERENCIADOR para esse fim, sem custo adicional.

6.5 – A entrega das licenças deverá ocorrer em **até 10 (dez) dias úteis**, conforme as necessidades do GERENCIADOR, após a emissão do Pedido de Compras (PC) pela Coordenação de Compras do GERENCIADOR. A entrega deverá ser previamente agendada com o responsável técnico designado pelo GERENCIADOR para esse fim, sem custo adicional.

6.6 – O início do processo de **instalação** deverá ocorrer **em até 05 (cinco) dias úteis** após solicitação formal da Unidade de Tecnologia Digital (UTD) do GERENCIADOR.

6.7 – DISPOSIÇÕES GERAIS / INFORMAÇÕES COMPLEMENTARES

6.7.1 – Requisitos gerais de garantia e suporte

6.7.1.1 – O FORNECEDOR deverá fornecer garantia e suporte para todos os serviços que envolvem o funcionamento e uso da solução, sem que isso gere qualquer ônus para a GERENCIADOR.

6.7.1.2 – O FORNECEDOR deverá fornecer garantia e suporte para todos os serviços que envolvem o funcionamento e uso da solução, sem que isso gere qualquer ônus para a GERENCIADOR.

6.7.1.3 – O FORNECEDOR deverá garantir a atualização de versões do software e base de dados que compõem a solução, as quais incorporam correções de erros ou problemas registrados e melhorias nas funcionalidades implementadas pela Fabricante da Solução. Os procedimentos de atualização têm por finalidade assegurar a devida atualização da solução durante o período de suporte dos produtos.

6.7.2 – Requisitos gerais de tecnologia

6.7.2.1. Requisitos de arquitetura tecnológica (Requisitos de projeto e implementação)

i. Em até **10 (dez) dias úteis** após o recebimento do PC, o FORNECEDOR deverá elaborar e disponibilizar para equipe técnica de fiscalização do GERENCIADOR, o Projeto de Implantação da Solução de Segurança e Proteção AntiMalware, de acordo com o ambiente tecnológico disponível no GERENCIADOR. O projeto deverá prever a implantação, em suas respectivas fases, agrupando as atividades conforme cada uma das etapas e/ou subetapas, com detalhamento do cronograma, definições dos marcos de entrega, contemplando as fases de validação, aprovação e início de produção das etapas e/ou subetapas até que a solução esteja completamente operante no GERENCIADOR. A entrega deverá ser feita na forma arquivo digital e impressa, editável, devidamente encadernada, descrevendo cada uma das etapas e/ou subetapas, pré-requisitos, resultados previstos, cronograma e demais artefatos comuns em projetos de Tecnologia, Informação e Comunicação;

ii. Após a implantação de toda a solução, devidamente validadas e aprovadas em todas as etapas pela equipe técnica do GERENCIADOR, responsável pela fiscalização da Ata), o FORNECEDOR deverá elaborar e disponibilizar o Projeto em sua versão final, de acordo com o que fora executado. A entrega deverá ser feita no arquivo digital e impressa, editável, devidamente encadernada, descrevendo cada uma das etapas e/ou subetapas, pré-requisitos, resultados previstos e alcançados, cronograma e demais artefatos comuns em projetos de Tecnologia, Informação e Comunicação;

iii. Tendo em vista que a solução atenderá a todo o parque tecnológico do GERENCIADOR, esta deverá manter a compatibilidade com as seguintes distribuições de sistemas operacionais de 32 bits e 64 bits, devendo atender, também, com versões superiores destas distribuições:

a) GNU Linux e seus derivados;
b) Windows 10 ou superior;
c) Windows server 2008;
d) Windows server 2012;
e) Windows server 2016 ou superior
f) MAC OS X 10.4 ou superior;

iv. SISTEMAS OPERACIONAIS X SERVIDORES FÍSICOS E VIRTUAIS

SISTEMA OPERACIONAL	SERVIDORES FÍSICAS	SERVIDORES VIRTUAIS	QUANTIDADE
Windows Server 2008 R2		X	1
Windows Server 2008 R2	X		2

SESC – Serviço Social do Comércio | Departamento Regional em Pernambuco | www.sescpe.org.br
Casa do Comércio/Edifício Josias Albuquerque | Avenida Visconde de Suassuna, nº 265, Santo Amaro - Recife-PE.
CEP: 50.050-540 TEL + 55 81 3216 1739

Windows Server 2012 Standard		X	1
Windows Server 2012 Standard	X		1
Windows Server 2012 R2	X		3
Windows Server 2012 R2		X	12
Windows Server 2012 R2 Standard		X	2
Windows Server 2012 R2 Standard	X		1
Windows Server 2012 Datacenter		X	1
Windows Server 2016 Standard	X		16
Windows Server 2016 Standard		X	70
Windows Storage Server 2012 R2 Standard		X	1

v. SISTEMAS OPERACIONAIS X DESKTOPS

SISTEMA OPERACIONAL	QUANTIDADE DESKTOPS
Windows 10 Professional	907
Windows 11	175

vi. A solução deverá ser capaz de bloquear atividades de malware, explorando vulnerabilidades em software de terceiros;

vii. A solução deverá ser capaz de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina

viii. A solução deverá ser capaz de identificar processo malicioso de criptografia não autorizado antes de ser iniciado, realizando backup dos dados automaticamente e possibilitando volta ao estado inicial;

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

x. A solução deverá ser capaz de habilitar automaticamente uma política, sempre que ocorrer uma epidemia na rede, baseado em quantidade de malware encontrados em determinado intervalo de tempo;

xi. A solução deverá ser capaz de, em caso de epidemia, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e regras de acesso à internet;

xii. A solução deverá ser capaz de gerenciar todos os recursos da solução através de uma única console;

6.7.2.2. Requisitos Gerais do Suporte Técnico

i. Deverá funcionar em regime de horário **24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, inclusive feriados, para chamados de Nível 1 (Serviços Indisponíveis/Epidemia)**. Casos excepcionais serão estabelecidos pela UTD. **Para chamados de Nível 2 e Nível 3, o suporte poderá ocorrer em regime de horário administrativo, das 08:00 às 17:00 horas, de segunda à sexta.**

ii. Os métodos para abertura de chamado deverão ser via telefone ou portal Web;

iii. A equipe de suporte deverá prestar toda assistência remota necessária até a resolução dos problemas, tais como:

I. Nível 1: Serviços Indisponíveis

a) Interrupção dos negócios ou rede inoperante;
b) Epidemia de vírus por toda a rede;
c) Serviços críticos gravemente afetados;
d) Servidores que não estão se comunicando com a console de gerenciamento;
e) Ou similar;

II. Nível 2: Serviços Parcialmente Indisponíveis

a) Detecção de falsos positivos que afetam serviços críticos;
b) Suporte para upgrade de versões e releases do software;
c) Ou similar;

III. Nível 3: Serviços disponíveis com ocorrência de falhas ou alertas

a) Máquinas que não estão se comunicando com a console de gerenciamento;
b) Análise e correção de eventos relacionados à segurança e à performance do software e do ambiente;
c) Ou similar;

Níveis de Severidade	
Nível	**Descrição**
1	Serviços indisponíveis
2	Serviços parcialmente indisponíveis ou com degradação dos serviços.
3	Serviços disponíveis com ocorrência de falhas ou alertas. Dúvidas geral sobre equipamentos

iv. Para efeito dos atendimentos técnicos aos chamados, o FORNECEDOR deverá observar os níveis de severidade e respectivos prazos máximos fixados:

Prazo máximo para Início de Atendimento		
Tipo	**Prazo**	**Nível de Severidade**

SESC – Serviço Social do Comércio | Departamento Regional em Pernambuco | www.sescpe.org.br
Casa do Comércio/Edifício Josias Albuquerque | Avenida Visconde de Suassuna, nº 265, Santo Amaro - Recife-PE.
CEP: 50.050-540 TEL + 55 81 3216 1739

		1	2	3
Remoto	Tempo	2 horas	6 horas	24 oras

v. O FORNECEDOR arcará com todas as despesas decorrentes dos serviços de garantia e suporte técnico.
vi. Após a prestação de cada serviço de garantia/suporte técnico, o FORNECEDOR deverá emitir o relatório correspondente, no qual deverão constar todos os dados relevantes sobre a data e hora do chamado, do diagnóstico, o nome do técnico que realizou os serviços, a hora de início e de término do atendimento.

6.8 - TREINAMENTO HANDS-ON DA SOLUÇÃO E SUPORTE - DETALHAMENTO E ESPECIFICAÇÃO

6.8.1 - SERVIDOR DE ADMINISTRAÇÃO E CONSOLE ADMINISTRATIVA

1. A capacitação deverá contemplar, no mínimo, os seguintes tópicos:

a) Criação de pacotes de instalação;
b) Configuração de AntiMalware;
c) Configuração de proteção para arquivos compactados, e-mails navegação e discos removíveis.
d) Gerenciamento centralizado das funções via console;
e) Atualização de softwares e vacinas.
f) Instalação e atualização em ambientes físicos (servidores, estações de trabalho, laptops, smartphones, tablet) e virtuais (servidores);
g) Instalação e atualização em sistemas virtuais e operacionais windows, linux, android, iOS;
h) Criação de pacotes de instalação;

2. O FORNECEDOR deverá transmitir conhecimento à equipe da UTD do SESC-PE, contemplando o uso da solução objeto deste Termo.
3. O treinamento será feito para a equipe técnica da UTD, com vistas a capacitá-los para o uso das funcionalidades da solução, com carga horária de 16 horas, para até 15 (quinze) técnicos, no formato remoto.
4. O instrutor do FORNECEDOR deverá possuir pleno conhecimento no uso de todas as ferramentas que integram a referida solução.
5. O instrutor do FORNECEDOR deverá possuir certificado fornecido por centro de treinamento oficial do Fabricante que o credencie a ministrar a capacitação da solução.

6.8 .1.1 - INFORMAÇÕES SOBRE OS TREINAMENTOS

6.8.1.1.1 - Treinamento da solução implementada - Hands-on (para todos os itens constantes na tabela de especificações):

a) A vencedora fica responsável em ofertar treinamento (Hands-on) sobre a instalação, configuração e gerenciamento da solução de antivirus / antimalware, com carga horária mínima de 24hs, a ser realizada na sede do Sesc-DR/PE (podendo ser on-line), utilizando o ambiente da solução ofertada e instalada, provendo este treinamento prático para equipe composta de até 10 (dez) colaboradores indicados pela UTD do Sesc-DR/PE.

a.1) A exigência apresentada na alínea anterior está subordinada ao pedido mínimo (acumulativo) de 1.000 (mil) licenças para o item 01 e uma licença do item 02 do unico lote.
a.2) O treinamento HANDS-ON deverá ocorrer juntamente com a instalação e configuração dos produtos (itens 01 e 02 constantes no item 3 deste Termo de Referência).
a.3) A contratada deverá ser responsável por todos os custos, referente a este treinamento.

6.8.1.1.2 - Treinamento Oficial para o AntiMalware ofertado:

a) A vencedora fica responsável em ofertar treinamento presencial em Centro de Treinamento Oficial do AntiMalware ofertado, para 03 (três) funcionários da UTD do SESC-PE.

a.1) O treinamento deverá ser presencial e possuir o conteúdo programático oficial, contendo no mínimo: instalação e configuração em desktops e servidores; e gerenciamento em servidores.
a.2) O treinamento deverá ter carga horária mínima de 20 (vinte) horas. A Contratada deverá arcar com todo o ônus e custos dos mesmos, tais como material didático, translados, hospedagem, treinamento.
a.3) A exigência apresentada na alínea anterior está subordinada ao pedido mínimo (acumulativo) de 1.500 (hum mil e quinhentas) licenças para o item 01 e 100 (cem) licenças do item 02 do único lote.
a.4) O prazo máximo de realização do treinamento presencial Oficial para o AntiMalware será de até 90 (noventa) dias, contados a partir do Pedido de Compra (PC) que totalize os quantitativos mínimos estabelecidos.

6.8.2 – SUPORTE

SERVIDOR DE ADMINISTRAÇÃO E CONSOLE ADMINISTRATIVA

Nível 1: Serviços indisponíveis

a) Interrupção de serviços ou rede inoperante causado por vírus;
b) Epidemia de vírus por toda a rede;
c) Serviços críticos gravemente afetados;
d) Servidores que não estão se comunicando com a console de gerenciamento;

Nível 2: Serviços parcialmente indisponíveis

a) Detecção de falsos positivos que afetam serviços críticos;
b) Suporte para upgrade de versões e releases do software;

Nível 3: Serviços disponíveis com ocorrência de falhas ou alertas

a) Máquinas que não estão se comunicando com a console de gerenciamento;
b) Análise e correção de eventos relacionados à segurança e à performance do software e do ambiente;
c) O suporte inicial se dará de forma remota, em casos mais graves que o suporte remoto não seja suficiente, será realizado o atendimento de forma presencial.

6.9 – AVALIAÇÃO DA QUALIDADE E TERMO DE ACEITE

6.9.1 – O Gerenciamento Técnico desta Ata será de responsabilidade da equipe de fiscalização da Ata designada pela GERENCIADOR, que estará acompanhando e avaliando a execução dos serviços prestados pelo FORNECEDOR. Será utilizada como metodologia de avaliação da qualidade e aceite dos serviços o cumprimento a todas as exigências, obrigações e especificações descritas nesta Ata e demais anexos e conteúdos que integrarem o Edital do Pregão Eletrônico Sesc/DR-PE nº 006/2026, durante a execução desta Ata.

6.9.2 – O recebimento provisório ou definitivo não exclui a responsabilidade civil, nem a ético-profissional pela perfeita execução do objeto desta Ata, dentro dos limites estabelecidos pela lei.

6.10 – EXECUÇÃO DAS ATIVIDADES

6.10.1 – O início da execução dos serviços deverá ser realizado mediante a emissão do PC. Serão emitidas solicitações para as atividades de TREINAMENTO. O envio das solicitações será realizada pelo Gestor da Ata, por meio dos instrumentos formais de comunicação.

6.10.2 – A obrigação de execução dos serviços por parte do FORNECEDOR iniciará declarada na autorização de fornecimento ou documento equivalente. O FORNECEDOR deverá apresentar justificativa prévia e formal sobre eventuais atrasos ou paralisação dos serviços, cabendo ao Gestor acatar ou não a justificativa. A fiscalização promoverá a avaliação da qualidade dos serviços realizados e justificativas, de acordo com os Critérios de Aceitação e demais requisitos definidos nesta Ata.

6.11 – MANUTENÇÃO DE SIGILO E NORMAS DE SEGURANÇA

6.11.1 – O FORNECEDOR deverá manter sigilo, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto de interesse do GERENCIADOR ou de terceiros de que tomar conhecimento em razão da execução da Ata, respeitando todos os critérios estabelecidos, aplicáveis aos dados, informações, documentos, entre outros pertinentes.

6.11.2 – O FORNECEDOR deverá manter sigilo absoluto sobre quaisquer dados e informações, que venha a ter conhecimento durante a prestação dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo GERENCIADOR a tais documentos.

6.12 – FISCALIZAÇÃO

6.12.1 – A fiscalização desta Ata será realizada pela equipe técnica a ser designada pela UTD – Unidade de Tecnologia Digital do GERENCIADOR.

6.12.2 – O GERENCIADOR designará uma comissão de servidores para acompanhamento e fiscalização da execução do objeto deste Ata, que registrará, em relatório, todas as ocorrências relacionadas com sua execução, determinando o que for necessário à regularização das falhas ou defeitos observados, bem como a emissão de documentos de atesto, validações e aprovações.

6.12.3 – Os esclarecimentos solicitados pela fiscalização do GERENCIADOR deverão ser prestados imediatamente, salvo quando implicarem em indagações de caráter técnico, hipótese em que serão respondidos no prazo máximo de 8 (oito) horas úteis.

6.13 – A desobediência aos prazos e condições estabelecidos acarretará a aplicação, ao FORNECEDOR, das sanções estabelecidas nesta Ata de Registro de Preços ou documento equivalente (Pedido de Compra), no que couber.

6.13 – É facultado ao GERENCIADOR, quando o licitante convocado não aceitar realizar a entrega do(s) produto(s) no prazo e condições estabelecidos, convocar o(s) licitante(s) remanescente(s), na ordem de classificação, para fazê-lo em igual prazo e nas mesmas condições propostas pelo primeiro classificado, ou cancelar a Ata de Registro de Preços, independentemente das cominações que à empresa serão impostas.

CLÁUSULA SÉTIMA – DAS OBRIGAÇÕES DO FORNECEDOR

7.1 – Executar fielmente a Ata, de acordo com as cláusulas avençadas. A ação ou omissão, total ou parcial do GERENCIADOR não eximirá o FORNECEDOR de total responsabilidade quanto à execução dos serviços.

7.2 – Fornecer o objeto desta Ata dentro dos padrões e requisitos estabelecidos e realizar entrega dos itens, estritamente de acordo com as especificações.

7.3 – Manter, durante toda a execução da Ata, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na contratação.

7.4 – Assumir a responsabilidade por todos os encargos previdenciários e obrigações sociais previstos na legislação social e trabalhista em vigor, obrigando-se a saudá-los na época própria, uma vez que os seus empregados não manterão nenhum vínculo empregatício com o GERENCIADOR.

7.5 – Assumir a responsabilidade por todas as providências e obrigações estabelecidas na legislação específica de acidentes de trabalho, quando, em ocorrência da espécie, forem vítimas os seus empregados quando da execução do serviço ou em conexão com ele, ainda que acontecido em dependência do GERENCIADOR, inclusive por danos causados a terceiros.

7.6 – Assumir todos os encargos de possível demanda trabalhista, cível ou penal, relacionados à execução do serviço, originariamente ou vinculada por prevenção, conexão ou contingência, incluindo atendimento às normas regulamentadoras da Medicina e Segurança do Trabalho.

7.7 – Promover a execução do serviço dentro dos parâmetros e rotinas estabelecidos, em observância às normas legais e regulamentares aplicáveis e às recomendações aceitas pela boa técnica.

7.8 – Responder integralmente pelos danos causados, direta ou indiretamente, ao patrimônio da União em decorrência de ação ou omissão de seus empregados ou prepostos, não se excluindo ou reduzindo essa responsabilidade em razão da fiscalização ou do acompanhamento realizado pelo GERENCIADOR.

7.9 – Providenciar que seus empregados portem crachá de identificação quando da execução do serviço em ambiente do GERENCIADOR.

7.10 – Atender às solicitações do GERENCIADOR, por intermédio de funcionários ou técnicos por ele credenciados, relacionados com a execução dos serviços.

SESC – Serviço Social do Comércio | Departamento Regional em Pernambuco | www.sescpe.org.br
Casa do Comércio/Edifício Josias Albuquerque | Avenida Visconde de Suassuna, nº 265, Santo Amaro - Recife-PE.
CEP: 50.050-540 TEL + 55 81 3216 1739

7.11 – Comunicar ao GERENCIADOR qualquer ocorrência que venha a interferir na execução dos serviços.

7.12 – Respeitar, durante a execução dos serviços, todas as leis, normas e posturas Federais, Estaduais, Distritais e Municipais pertinentes e vigentes.

7.13 – Atender às solicitações do GERENCIADOR, de acordo com as especificações técnicas, procedimentos de controle administrativo e cronogramas físicos que venham a ser estabelecidos, ou quaisquer outras solicitações inerentes ao objeto da Ata.

7.14 – Facilitar à equipe de fiscalização o pleno exercício de suas funções, prestando-lhe todos os esclarecimentos e informações administrativas e/ou técnicas que lhe forem solicitadas, exibindo-lhe todos os documentos e dados de interesse para acompanhamento e fiscalização da execução do instrumento contratual ou instrumento equivalente.

7.15 – O exercício das funções da equipe de fiscalização não desobriga o FORNECEDOR de sua própria responsabilidade, quanto à adequada, pronta e fiel execução do objeto desta Ata.

7.16 – Ter pleno conhecimento de todas as condições e peculiaridades inerentes ao objeto não podendo invocar posteriormente desconhecimento para cobrança de serviços extras.

7.17 – Proibir a veiculação de publicidade ou qualquer outra informação acerca do objeto da Ata, salvo se houver prévia autorização da Administração do GERENCIADOR.

7.18 – Executar os serviços por intermédio de profissionais qualificados, com experiência e conhecimento compatíveis com os serviços a serem realizados.

7.19 – O FORNECEDOR é responsável por realizar a supervisão e acompanhamento da qualidade e dos níveis de serviço alcançados com vistas a efetuar eventuais ajustes e correções para o atendimento dos níveis de serviço.

7.20 – Durante a fase da execução do serviço a interrupção na prestação do serviço, em desacordo com a Ata, sujeita o FORNECEDOR às penalidades previstas no Edital e seus anexos, salvo por motivo formalmente encaminhado ao GERENCIADOR, justificado e aceito por esta.

7.21 – Se o GERENCIADOR houver disponibilizado recursos (documentos, equipamentos ou outros) ao FORNECEDOR, estes deverão ser devolvidos ao GERENCIADOR durante a transição contratual.

7.22 – O FORNECEDOR deverá reparar, corrigir, remover ou reconstruir, às suas expensas, no total ou em parte, os serviços efetuados referentes ao objeto em que se verifiquem vícios, defeitos ou incorreções resultantes da execução, ou ainda aqueles que não satisfaçam aos níveis de qualidade previstos.

7.23 – Solicitar, previamente e formalmente, autorização à equipe de fiscalização sempre que necessitar executar atividades especiais ou não previstas.

7.24 – Cumprir todas as obrigações e exigências previstas nesta Ata e em seus anexos.

SESC – Serviço Social do Comércio | Departamento Regional em Pernambuco | www.sescpe.org.br
Casa do Comércio/Edifício Josias Albuquerque | Avenida Visconde de Suassuna, nº 265, Santo Amaro - Recife-PE.
CEP: 50.050-540 TEL + 55 81 3216 1739

7.25 – Não é permitido a utilização de qualquer trabalho do menor de dezesseis anos, exceto na condição de aprendiz para os maiores de quatorze anos; nem a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre.

7.26 – Os serviços excepcionais realizados em horário noturno, e aos sábados, domingos e feriados no ambiente do GERENCIADOR ou do FORNECEDOR não implicarão em nenhuma forma de acréscimo ou majoração nos valores dos serviços e produtos, razão pela qual será improcedente a reivindicação de restabelecimento de equilíbrio econômico-financeiro.

7.27 – O representante do FORNECEDOR deverá apresentar, na reunião inicial, carta de formalização do PREPOSTO, contendo indicação de nome e contato do funcionário que exercerá as atividades de preposto do FORNECEDOR, no âmbito da Ata.

7.28 – Prestar todos os esclarecimentos que forem solicitados pela fiscalização do GERENCIADOR acerca da situação dos serviços contratados, em até 8 (oito) horas úteis, a contar do encaminhamento formal do pedido.

7.29 – O FORNECEDOR deverá entregar junto com a solução de AntiMalware:

7.29.1 – Todos os manuais necessários à instalação do software de AntiMalware e seus componentes em mídia digital;

7.29.2 – Todas as licenças de utilização definitivas para os softwares fornecidos, em suas últimas versões disponíveis considerando a data de entrega do software, em nome do SESC PERNAMBUCO. As licenças do software deverão ser ofertadas na modalidade de licenciamento perpétua;

7.30 – O FORNECEDOR deverá possibilitar a conferência das características da Solução descrita neste Termo, através dos canais de comercialização do fabricante no Brasil (site, folder, dentre outros meios).

7.31 – **O FORNECEDOR deverá indicar o e-mail do representante legal que assinará esta Ata de Registro de Preços, bem como comunicar por escrito qualquer alteração posterior, no endereço eletrônico apresentado, a fim de que o GERENCIADOR possa enviar o documento aos signatários por e-mail, com o objetivo de obter as assinaturas eletrônicas.**

CLÁUSULA OITAVA – OBRIGAÇÕES DO GERENCIADOR

8.1 – Acompanhar e fiscalizar a execução da Ata, atestar as notas fiscais/faturas relativo à entrega do objeto e o seu aceite.

8.2 – Efetuar o pagamento ao FORNECEDOR de acordo com o preço, os prazos e as condições estipuladas na Ata;

8.3 – Rejeitar, no todo ou em parte, serviço ou fornecimento realizado em desacordo com esta Ata de Registro de Preços;

8.4 – Informar ao FORNECEDOR toda e qualquer irregularidade constatada na execução do objeto, ou problemas que venham a interferir, direta ou indiretamente, na execução desta Ata de Registro de Preços;

SESC – Serviço Social do Comércio | Departamento Regional em Pernambuco | www.sescpe.org.br
Casa do Comércio/Edifício Josias Albuquerque | Avenida Visconde de Suassuna, nº 265, Santo Amaro - Recife-PE.
CEP: 50.050-540 TEL + 55 81 3216 1739

8.5 – Providenciar o acesso do FORNECEDOR aos locais necessários para o levantamento das informações que a execução dos serviços requeira;

8.6 – Permitir o acesso dos técnicos da empresa FORNECEDORA, para execução dos serviços previstos, desde que previamente identificados e credenciados, assim como acompanhá-los na execução dos serviços quando ocorrer in loco;

8.7 – Assegurar que os preços contratados estão compatíveis com aqueles praticados no mercado;

8.8 – Serão permitidas subcontratações desde que haja autorização/anuência do GERENCIADOR;

8.9 – Documentar as ocorrências decorrentes de sua fiscalização, verificar o cumprimento das obrigações do FORNECEDOR, aplicando-lhe as penalidades cabíveis quando do descumprimento daquelas, ressalvados os casos de força maior, justificados e aceitos pela Administração;

8.10 – Proporcionar todas as condições e prestar as informações necessárias para que o FORNECEDOR possa cumprir com suas obrigações, dentro das normas e condições contratuais.

8.11– Notificar o FORNECEDOR sobre qualquer irregularidade encontrada no fornecimento dos produtos.

8.10– Registrar e oficializar ao FORNECEDOR, as ocorrências de desempenho ou comportamento insatisfatório, irregularidades, falhas, insuficiências, erros e omissões constatados, durante a execução da Ata, para as devidas providências.

8.11 – Rejeitar, no todo ou em parte, o objeto em desacordo com as especificações estabelecidas na CLÁUSULA QUARTA desta Ata de Registro de Preços e com as obrigações assumidas pelo FORNECEDOR.

CLÁUSULA NONA – DO PAGAMENTO

9.1 – Em nenhuma hipótese o GERENCIADOR efetuará pagamento antecipado ao FORNECEDOR.

9.2 – O pagamento será realizado em até 30 (trinta) dias uteis, preferencialmente, através do pagamento de boleto bancário emitido pelo FORNECEDOR, ou de depósito bancário na conta do FORNECEDOR, mediante apresentação da Nota Fiscal, após a aceitação dos bens na Nota Fiscal ou "Nota Fiscal Fatura", atestada pela fiscalização do GERENCIADOR.

9.2.1 – A Nota Fiscal deverá conter a descrição completa dos equipamentos entregues, bem como os seus preços unitários e totais, e deverá ser emitida quando da entrega realizada, com o respectivo CNPJ da Unidade do GERENCIADOR onde será entregue o objeto licitado.

9.2.2 – Para depósito de que trata o subitem 9.2, os dados bancários do FORNECEDOR deverão estar indicados no corpo da Nota Fiscal, assim como, o número do Pedido de Compra correspondente. No caso de depósitos em conta corrente que não seja na Caixa Econômica Federal ou no Banco do Brasil S/A., será descontado o valor referente às despesas bancárias.

SESC – Serviço Social do Comércio | Departamento Regional em Pernambuco | www.sescpe.org.br
Casa do Comércio/Edifício Josias Albuquerque | Avenida Visconde de Suassuna, nº 265, Santo Amaro - Recife-PE.
CEP: 50.050-540 TEL + 55 81 3216 1739

9.2.3 – Boletos bancários serão aceitos, desde que não sejam registrados em Cartório de Protesto.

9.2.4 – Em caso de boleto bancário, o mesmo deverá ser encaminhado anexado à Nota Fiscal no ato da entrega, não sendo aceitos boletos bancários enviados posteriormente.

9.3 – Enquanto houver pendência de liquidação de qualquer obrigação financeira, em virtude de penalidade, inadimplência contratual ou se o produto apresentar irregularidades ou desconformidades no ato da entrega, não será efetuado nenhum pagamento ao FORNECEDOR referente à parcela inadimplida.

9.4 – Nenhuma fatura poderá ser negociada com Instituição de Crédito.

9.5 – As irregularidades porventura constatadas após a entrega dos equipamentos deverão ser sanadas, sem nenhum ônus adicional, devendo o FORNECEDOR comunicar por escrito a solução do problema.

9.5.1 – O pagamento ficará retido até que seja sanada a pendência, ocorrendo o pagamento, nos moldes do subitem 9.2 desta Ata de Registro de Preços, a partir da data da solução do problema, sem nenhum ônus para o GERENCIADOR.

9.6 – Não haverá pagamento sem que ocorra a efetiva entrega do objeto contratado, podendo ocorrer, contudo, excepcionalmente, se for do interesse do GERENCIADOR, o pagamento correspondente à fração do objeto contratual que tenha sido recebido parcialmente, mediante autorização da Administração.

9.7 – Os valores apresentados nas faturas são considerados completos e abrangem todos os tributos (impostos, taxas, licenças, emolumentos, contribuições fiscais e parafiscais), fornecimento de mão de obra especializada, fretes, leis sociais, seguros, administração, lucros e ferramental, transporte de material e de pessoal e qualquer despesa, acessória ou necessária.

9.8 – Em caso de incidência de tributos, o GERENCIADOR se reservará ao direito de efetuar as respectivas retenções na fonte incidentes sobre os valores da Nota Fiscal, fatura ou recibo.

9.9 – DAS GLOSAS

9.9.1 - O não cumprimento dos serviços/fornecimento de produtos descritos neste instrumento obrigacional, independentemente das sanções administrativas previstas, implicará em redutor na fatura mensal do serviço/produto, nos seguintes casos:

9.9.1.1 - Para o atraso na prestação dos serviços/entrega dos produtos:

a) glosa de 1% (um por cento), calculada sobre o valor correspondente aos produtos não entregues ou serviços não prestados no prazo acordado, por dia útil de atraso, limitada a 2 (dois) dias úteis de atraso.

9.9.1.2 - PARA O ATRASO NA SOLUÇÃO DAS VALIDAÇÕES DE RELATÓRIOS, MEDIÇÕES, PROJETOS E SERVIÇOS SIMILARES:

SESC – Serviço Social do Comércio | Departamento Regional em Pernambuco | www.sescpe.org.br
Casa do Comércio/Edifício Josias Albuquerque | Avenida Visconde de Suassuna, nº 265, Santo Amaro - Recife-PE.
CEP: 50.050-540 TEL + 55 81 3216 1739

a) glosa de 0,5% (meio por cento), calculada sobre o valor da parcela inadimplida, para cada dia útil de atraso na solução das validações, limitada até 03 (três) dias úteis de atraso.

9.9.2 - Nos casos em que os atrasos forem superiores aos limites previstos nas alíneas anteriores, além da aplicação das glosas previstas, a cada ocorrência o GERENCIADOR poderá aplicar sanções administrativas à FORNECEDOR previstas neste contrato/ata de registro de preços.

9.9.3 - A aplicação da glosa servirá ainda como indicador de desempenho do FORNECEDOR na execução dos serviços.

9.9.4 - No caso de aplicação de glosa referente à demora na entrega dos produtos ou na conclusão dos serviços, durante 3 (três) meses consecutivos, ou 5 (cinco) meses intervalados durante os últimos 12 (doze) meses, serão aplicadas as sanções administrativas previstas neste instrumento.

9.9.5 - No caso de discordância das glosas aplicadas, o FORNECEDOR deverá apresentar impugnação que será analisada pela área administrativa.

9.9.6 - Se a decisão da Administração for favorável à impugnação do FORNECEDOR, esta deverá emitir nota de cobrança adicional para que seja efetuado o pagamento referente ao valor glosado.

9.9.7 - A nota de cobrança emitida pelo FORNECEDOR deverá ser atestada pelo fiscal do contrato/ata de registro de preços e encaminhada para a área financeira para efetuar o pagamento, acompanhada da documentação comprobatória das glosas.

9.9.8 – Poderá o GERENCIADOR, após efetuar a análise das notas fiscais, realizar glosas dos valores cobrados indevidamente.

9.9.9 – O FORNECEDOR poderá apresentar impugnação à glosa, no prazo de 3 (três) dias úteis, contados da data do recebimento da notificação.

9.9.10 – Caso o FORNECEDOR não apresente a impugnação, ou caso o GERENCIADOR não acolha as razões da impugnação, o valor será deduzido da respectiva nota fiscal.

9.9.11 – O prazo de pagamento será interrompido nos casos em que haja necessidade de regularização do documento fiscal, o que será devidamente apontado pelo GERENCIADOR.

9.9.12 – A contagem do prazo previsto para pagamento será iniciada a partir da respectiva regularização.

9.9.13 – O depósito bancário com valor integral produzirá os efeitos jurídicos da quitação da prestação devida.

9.9.14 – Quando houver glosa parcial dos produtos ou serviços, o GERENCIADOR deverá comunicar à empresa para que emita a nota fiscal ou fatura com o valor incontroverso exato dimensionado, evitando, assim, efeitos tributários sobre o valor glosado pelo GERENCIADOR.

CLÁUSULA DÉCIMA – DAS PENALIDADES

SESC – Serviço Social do Comércio | Departamento Regional em Pernambuco | www.sescpe.org.br
Casa do Comércio/Edifício Josias Albuquerque | Avenida Visconde de Suassuna, nº 265, Santo Amaro - Recife-PE.
CEP: 50.050-540 TEL + 55 81 3216 1739

10.1 – O descumprimento dos prazos e condições estipulados sujeitará o FORNECEDOR às penalidades abaixo mencionadas, a critério do GERENCIADOR, desde que observadas as formalidades previstas na CLÁUSULA DÉCIMA TERCEIRA desta Ata de Registro de Preços.

a) Advertência/Notificação por escrito, na ocorrência de qualquer descumprimento desta Ata de Registro de Preços;

b) Multa de 15% (quinze por cento), sobre o saldo remanescente do respectivo Pedido de Compra, quando houver descumprimento de prazo, até o limite de 10% (dez por cento) do valor total do Pedido de Compra ou documento equivalente;

c) Multa de 5% (cinco por cento), sobre o valor do Pedido de Compra - PC, que estejam em desconformidade com a qualidade dos serviços contratados/prestados. Esta multa poderá ser acrescida de mais 5% (cinco por cento) caso não realize a substituição do(s) serviço(s) ou correção das irregularidades no(s) serviço(s) apontado(s) pelo GERENCIADOR, em até 10 (dez) dias corridos, limitada ao máximo de 10% (dez por cento) sobre o valor nominal total de cada item, contados da notificação feita pelo GERENCIADOR;

d) Multa de 0,5% (meio por cento), sobre o valor total do Pedido de Compra ou documento equivalente, pela não substituição da nota fiscal, que porventura contenha erros, no prazo de até 03 (três) dias corridos, contados da notificação por escrito ou por e-mail do GERENCIADOR.

10.2 – As multas de que tratam o subitem 10.1 desta Ata, poderão ser descontadas dos pagamentos a que o FORNECEDOR fizer jus, ou, se for o caso, recolhidas diretamente na tesouraria do GERENCIADOR, a juízo da Administração, no prazo de **até 10 (dez) dias corridos**, a partir da notificação que vier a ser feita.

10.3 – A aplicação das penalidades será precedida da concessão do contraditório e ampla defesa ao FORNECEDOR, que deverá protocolar a defesa/justificativa no prazo de 48 (quarenta e oito) horas contados a partir do dia útil seguinte ao recebimento da notificação e/ou comunicação realizada através de Carta com Aviso de Recebimento (AR) e/ou e-mail, conforme o previsto na CLÁUSULA DÉCIMA TERCEIRA desta Ata.

10.3.1 – Caso não sejam aceitas as justificativas apresentadas pelo FORNECEDOR, será aplicada a multa prevista no subitem 10.1 desta Ata de Registro de Preços, conforme o caso.

10.4 – É facultado ao GERENCIADOR exigir ainda, do FORNECEDOR que não cumprir as obrigações assumidas, restituição das perdas e danos de qualquer natureza, nos termos do artigo 389, do Código Civil, sem prejuízo de outras penalidades previstas em lei, especialmente as da Lei nº 8.078, de 12.09.90.

10.5 – A critério do GERENCIADOR, as sanções poderão ser cumulativas.

10.6 – **DA NOTIFICAÇÃO EXTRAPROCESSUAL PARA CIÊNCIA E ADEQUAÇÃO**

10.6.1. Constatada qualquer irregularidade, desconformidade ou descumprimento contratual, o FORNECEDOR poderá, a seu critério, notificar ao GERENCIDOR de forma extraprocessual, por meio de comunicação escrita enviada ao e-mail cadastrado, para fins de imediato ciência e promessa de

regularização.

10.6.2. O GERENCIADOR terá o prazo de **48 (quarenta e oito) horas**, contadas do recebimento da notificação, para comunicar formalmente ao GERENCIADOR as medidas tomadas para sanar a falha ou apresentar justificativa preliminar.

10.6.3. O descumprimento do disposto nesta cláusula ou a insuficiência da resposta poderão resultar na instauração de processo administrativo para apuração de infração e aplicação de penalidade, nos termos do artigo seguinte.

10.7 – DO PROCESSO ADMINISTRATIVO SANCIONADOR

10.7.1 - Para a aplicação das penalidades previstas nesta Ata, será instaurado processo administrativo específico, garantindo-se ao GERENCIADOR o exercício do contraditório e da ampla defesa.

10.7.2 - O FORNECEDOR será formalmente citada para apresentar defesa no prazo de **05 (cinco) dias úteis**, contados da ciência regular, podendo alegar e comprovar a ocorrência de caso fortuito, força maior que possam configurar excludentes de sua responsabilidade.

10.7.3 - A decisão final, proferida pela autoridade competente do GERENCIADOR, será fundamentada e comunicada ao FORNECEDOR, constituindo título executivo extrajudicial

10.8 – **O inadimplemento total ou parcial das obrigações assumidas dará ao GERENCIADOR o direito de cancelar unilateralmente esta Ata de Registro de Preços, sem prejuízo de outras penalidades previstas nesta Ata, que as partes declaram conhecer, inclusive a de suspensão do direito de licitar com o GERENCIADOR por prazo não superior a 03 (três) anos, conforme disposições contidas no artigo 40 da Resolução SESC Nº 1.593/2024.**

10.9 –**O FORNECEDOR é responsável pela fidelidade e legitimidade das informações prestadas e dos documentos apresentados em qualquer fase da licitação. A falsidade de qualquer documento apresentado ou a inverdade das informações nele contidas dará ao GERENCIADOR o direito de cancelar unilateralmente a Ata de Registro de Preços ou documento equivalente (Pedido de Compra), sem prejuízo de outras penalidades previstas nesta Ata.**

10.10 –**Após a declaração do vencedor não cabe desistência da proposta, salvo por motivo justo decorrente de fato superveniente aceito pelo GERENCIADOR, sendo que o inadimplemento desta cláusula implica nas penalidades estabelecidas para o inadimplemento total da Ata de Registro de Preços.**

10.10.1 – As hipóteses previstas no artigo **41 da Resolução SESC Nº 1.593/2024,** ensejarão impedimento do direito de licitar e terão abrangência nacional, por **prazo mínimo de 4 (quatro) e máximo de 6 (seis) anos,** nos seguintes casos:

I - Apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação ou a execução da ata;

II – Fraudar a licitação ou praticar ato fraudulento na execução da ata;

III - Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

SESC – Serviço Social do Comércio | Departamento Regional em Pernambuco | www.sescpe.org.br
Casa do Comércio/Edifício Josias Albuquerque | Avenida Visconde de Suassuna, nº 265, Santo Amaro - Recife-PE.
CEP: 50.050-540 TEL + 55 81 3216 1739

IV – Praticar atos ilícitos com vistas a frustrar os objetivos da licitação.

10.10.2 - A instrução do processo será de competência do gerenciador e a documentação deverá ser encaminhada ao Departamento Nacional para aplicação da pena, **conforme disposições contidas no parágrafo único da Resolução SESC Nº 1.593/2024**

CLÁUSULA DÉCIMA PRIMEIRA – DO TERMO DE RESPONSABILIDADE E ANTICORRUPÇÃO

11.1 – As PARTES declaram conhecer as normas de prevenção à corrupção previstas na legislação brasileira, dentre elas o Código Penal Brasileiro, Código de Ética do Sesc/PE, a Lei de Improbidade Administrativa (Lei nº. 8.429/1992) e a Lei nº. 12.846/2013, e seus regulamentos e, se comprometem a cumpri-las fielmente, por si e por seus representantes legais, gestores e colaboradores, bem como exigir seu cumprimento pelos terceiros por ela contratados.

CLÁUSULA DÉCIMA SEGUNDA – DO CANCELAMENTO DA ATA DE REGISTRO DE PREÇOS

12.1 – O FORNECEDOR terá seu registro de preços cancelado quando:

a) Descumprir as condições estipuladas nas cláusulas desta Ata de Registro de Preços, configurando-se inadimplemento parcial ou total das obrigações assumidas;

b) Não aceitar reduzir seu preço registrado, na hipótese deste se tornar superior àqueles praticados no mercado;

c) Justificadamente, não for mais de interesse do GERENCIADOR.

12.2 – O FORNECEDOR poderá solicitar o cancelamento do seu registro de preços, ocorrendo fato superveniente que venha comprometer a perfeita execução contratual, decorrente de caso fortuito ou de força maior, devidamente justificado e comprovado, e que tenha sido formulada a solicitação com a antecedência de 30 (trinta) dias.

12.2.1 – Será considerada como descumprimento total das obrigações a solicitação de cancelamento que não atender aos pré-requisitos do subitem 12.2 acima.

12.3 – O cancelamento do registro de preços, nas hipóteses previstas, assegurados o contraditório e a ampla defesa, serão formalizados por despacho da autoridade competente do GERENCIADOR.

CLÁUSULA DÉCIMA TERCEIRA – DA COMUNICAÇÃO

13.1 – As comunicações (solicitações/notificações/defesas/justificativas etc.) entre as partes somente terão validade e legitimidade se realizadas por e-mails, com aviso de leitura, enviados para os endereços físicos e/ou Eletrônicos indicados na qualificação da presente Ata de Registro de Preços ou de Carta com Aviso de Recebimento (AR), ou entregues diretamente no Setor de Documentação (SEDOC), caso seja possível.

13.2 – Caso as comunicações sejam realizadas diretamente na sede do GERENCIADOR, na SEDOC, deverão ser protocoladas durante o horário do expediente ordinário (**8h às 12h e de 13h às 17h**).

13.2.1 – Caso haja alteração extraordinária parcial ou total do horário previsto no *caput* do subitem

SESC – Serviço Social do Comércio | Departamento Regional em Pernambuco | www.sescpe.org.br
Casa do Comércio/Edifício Josias Albuquerque | Avenida Visconde de Suassuna, nº 265, Santo Amaro - Recife-PE.
CEP: 50.050-540 TEL + 55 81 3216 1739

13.2 da presente cláusula, por motivos administrativos ou não, a vigência ou início dos prazos serão adiados automaticamente para o dia útil seguinte, inclusive na hipótese de recesso administrativo do GERENCIADOR.

13.3 – As partes deverão comunicar por escrito quaisquer alterações dos dados destacados na qualificação das Partes na presente Ata de Registro de Preços, sob pena de ser consideradas como recebidas e protocoladas quaisquer comunicações realizadas para os endereços físicos e eletrônicos indicados.

CLÁUSULA DÉCIMA QUARTA – DA PROTEÇÃO DOS DADOS

14.1 – O FORNECEDOR se compromete a firmar Termo de Compromisso com a Proteção de Dados, com o objetivo de atuar em concordância com a legislação vigente sobre a proteção de dados pessoais e às determinações dos Órgãos Reguladores/Fiscalizadores sobre a matéria, em especial as disposições da Lei 13.709/2018 (“Lei Geral de Proteção de Dados”), bem como das demais leis, normas e políticas corporativas de proteção de dados pessoais.

14.2 – O FORNECEDOR ficará sujeita à proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados pessoais divergentes ao objeto da Ata de Registro de Preços firmada com o GERENCIADOR.

14.3 – Fica assegurado ao GERENCIADOR, nos termos da lei, o direito de regresso em face do FORNECEDOR diante de eventuais danos causados por esta em decorrência do descumprimento das obrigações aqui assumidas em relação à Proteção dos Dados.

CLÁUSULA DÉCIMA QUINTA – DO USO DE IMAGEM

15.1 – Pelo presente instrumento, o GERENCIADOR fica plenamente autorizado e capacitado a registrar a imagem e/ou voz dos funcionários, sócios, prestadores de serviços, subcontratados e afins do FORNECEDOR que venham a atuar no fornecimento e/ou prestação de serviço para o GERENCIADOR, captadas durante a vigência desta Ata de Registro de Preços para fins de utilização em obras audiovisuais e/ou obras impressas e outras, produzidas, editadas e/ou publicadas pelo GERENCIADOR, que se destinarão a toda e qualquer forma de comunicação audiovisual e impressa.

15.2 – O GERENCIADOR poderá utilizar-se da imagem dos funcionários, sócios, prestadores de serviços, subcontratados e afins do FORNECEDOR, para fins de divulgação das atividades, podendo reproduzi-la e/ou divulgá-la pelos diversos meios de comunicação à disposição do GERENCIADOR, sem qualquer retribuição pecuniária em favor dos funcionários, sócios, prestadores de serviços, subcontratados e afins do FORNECEDOR.

15.3 – A presente autorização é concedida em caráter gratuito, não cabendo aos funcionários, sócios, prestadores de serviços, subcontratados e afins do FORNECEDOR, qualquer pagamento, remuneração ou compensação, a qualquer tempo e título.

15.4 – A presente autorização de uso de imagem e/ou voz estará vigente pelo prazo de até 24 (vinte e quatro) meses após o término da Ata de Registro de Preços.

15.5 – As obras audiovisuais e/ou obras impressas e outras, produzidas, editadas e/ou publicadas durante o prazo indicado no parágrafo segundo, estarão sob a proteção de propriedade autoral,

SESC – Serviço Social do Comércio | Departamento Regional em Pernambuco | www.sescpe.org.br
Casa do Comércio/Edifício Josias Albuquerque | Avenida Visconde de Suassuna, nº 265, Santo Amaro - Recife-PE.
CEP: 50.050-540 TEL + 55 81 3216 1739

conforme estabelecido pela Lei nº 9.610/98.

15.6 – Fica vedado a captura de imagem e som dentro das instalações e/ou da programação do GERENCIADOR pelos funcionários, sócios, prestadores de serviços, subcontratados e afins do FORNECEDOR, sem a prévia autorização do GERENCIADOR, mediante requerimento justificado.

15.7 – A empresa fornecedora e/ou prestadora de serviços, se obriga a ter junto a seus funcionários, terceirizados, parceiros e/ou empresas subcontratadas, se for o caso, que venham a participar da execução da Ata ora celebrada junto ao GERENCIADOR, compromisso de uso de imagem para cobrir eventuais registros de imagem e áudio realizados a fim de prevenir possíveis demandas por uso não autorizado destes registros.

CLÁUSULA DÉCIMA SEXTA – DA VALIDADE E VERACIDADE DO DOCUMENTO

16.1 – As Partes reconhecem a veracidade, autenticidade, integridade, validade e eficácia desta Ata de Registro de Preços, nos termos do art. 219 do Código Civil, em formato eletrônico e/ou assinado pelas Partes por meio de certificados eletrônicos, ainda que sejam certificados eletrônicos não emitidos pela ICP-Brasil, nos termos do art. 10, § 2º, da Medida Provisória nº 2.220-2, de 24 de agosto de 2001 (“MP nº 2.220- 2”), como, por exemplo, por meio do upload e existência desta Ata de Registro de Preços, bem como a aposição das respectivas assinaturas eletrônicas nesta Ata de Registro de Preços, na plataforma Clicksign/Adobe Sign.

16.2 – Adicionalmente, as Partes expressamente anuem, autorizam, aceitam e reconhecem como válida qualquer forma de comprovação de autoria das Partes signatárias desta Ata de Registro de Preços por meio de suas respectivas assinaturas nesta Ata de Registro de Preços por meio de certificados eletrônicos, ainda que sejam certificados eletrônicos não emitidos pela ICP-Brasil, nos termos do art. 10, § 2º, da MP nº 2.220-2, como, por exemplo, por meio da aposição das respectivas assinaturas eletrônicas nesta Ata de Registro de Preços na plataforma de ClickSign/Adobe Sign, sendo certo que quaisquer de tais certificados será suficiente para a veracidade, autenticidade, integridade, validade e eficácia desta Ata de Registro de Preços, bem como a respectiva vinculação das Partes aos seus termos.

16.3 – Por fim, nos termos do art. 220 do Código Civil, as Partes expressamente anuem e autorizam que, eventualmente, as assinaturas das Partes não precisam necessariamente serem postas na mesma página de assinaturas desta Ata de Registro de Preços.

16.3.1 – Caso seja necessária a substituição da página de assinaturas, esta poderá ser assinada manualmente e escaneada em formato eletrônico, e será tão válida e produzirá os mesmos efeitos que a assinatura original de cada parte posta nesta Ata de Registro de Preços.

CLÁUSULA DÉCIMA SÉTIMA – DA GESTÃO E DA FISCALIZAÇÃO DA ATA DE REGISTRO DE PREÇOS

17.1 – DAS COMPETÊNCIAS:

17.1.1 – Ao gestor deste Contrato ou Ata de Registro de Preços cumpre:

a) Realização dos trâmites para efetuação dos Termos Aditivos tais como: prorrogação, reequilíbrio econômico-financeiro, reajuste, repactuação; além de notificações, eventual aplicação de sanções,

SESC – Serviço Social do Comércio | Departamento Regional em Pernambuco | www.sescpe.org.br
Casa do Comércio/Edifício Josias Albuquerque | Avenida Visconde de Suassuna, nº 265, Santo Amaro - Recife-PE.
CEP: 50.050-540 TEL + 55 81 3216 1739

cancelamento das atas de registro de preços, extinção dos contratos ou atas de registro de preços, atestados de capacidade técnica, entre outros;

b) Análise e elaboração das solicitações de autorização dos Termos de Contratos ou atas de registro de preços e seus respectivos Aditivos, bem como a condução dos processos de assinatura;

c) Elaboração de processos administrativos de apuração; e

d) Controle de vigência de contratos e atas de registro de preços.

17.1.2 – Aos fiscais (setoriais ou técnicos) desta Ata de Registro de Preços cumpre:

a) Conhecer os termos das cláusulas e das documentações relativas ao contrato ou atas de registro de preços;

b) Conhecer as obrigações contratuais que irá fiscalizar no decorrer da execução contratual;

c) Fiscalizar diretamente o cumprimento da execução contratual, realizando o controle e o acompanhamento de todas as ações atinentes ao contrato ou ata de registro de preços, em conformidade com o previsto no edital, na proposta da contratada, no contrato, na ata de registro de preços, bem como seus aditivos. Manter o gestor do contrato ou da ata de registro de preços devidamente informados quanto a sua execução;

d) Comunicar formalmente à Contratada/Fornecedora, no prazo máximo de 2 (dois) dias úteis a partir da identificação da irregularidade, por meio de carta ou e-mail informado no processo ou contrato, sobre as ocorrências de infrações contratuais. Conceder um prazo de até 2 (dois) dias úteis, contados a partir do primeiro dia útil seguinte ao recebimento da comunicação, para que a Contratada/Fornecedora regularize a situação e apresente, por escrito, a justificativa ou defesa das infrações cometidas;

e) Caso não seja atendida a solicitação de regularização da infração, verificar junto ao Gestor de Contratos a possibilidade de notificação ou aplicação de sanções à contratada, se for o caso, de acordo com as regras previstas no edital/contrato/ata de registro de preços e na legislação pertinente;

f) Acompanhar a correção e a readequação das inconformidades contratuais cometidas pela contratada ou fornecedora quanto à documentação, obrigações e outros aspectos administrativos do contrato ou ata de registro de preços;

g) Acompanhar e avaliar a qualidade dos serviços realizados ou dos bens entregues;

h) Enviar ao gestor do contrato os documentos necessários aos pedidos de reajuste, repactuação, reequilíbrio, entre outros;

i) Solicitar assessoramento técnico caso seja necessário ao acompanhamento da execução contratual;

j) Efetuar o Termo de Recebimento Definitivo do objeto contratado, exceto para obras, através de atesto de que os serviços prestados, os bens ou materiais fornecidos atendem aos requisitos estabelecidos no contrato ou na ata de registro de preços; e

SESC – Serviço Social do Comércio | Departamento Regional em Pernambuco | www.sescpe.org.br
Casa do Comércio/Edifício Josias Albuquerque | Avenida Visconde de Suassuna, nº 265, Santo Amaro - Recife-PE.
CEP: 50.050-540 TEL + 55 81 3216 1739

k) Após o término do contrato ou da ata de registro de preços, manter arquivados, no arquivo central, os registros de ocorrências e demais documentações julgadas úteis, pelo tempo mínimo previsto em normativo do Sesc/DR-PE.

CLÁUSULA DÉCIMA OITAVA – DAS DISPOSIÇÕES FINAIS

18.1 – Qualquer tolerância entre as partes não importará em novação de qualquer uma das CLÁUSULAS ou condições estatuídas neste contrato, as quais permanecerão íntegras.

18.2 – O GERENCIADOR não aceitará, sob nenhum pretexto, a transferência de responsabilidade para terceiros.

CLÁUSULA DÉCIMA NONA – DO FORO

19.1 – Fica eleito o foro da cidade de Recife/PE, como competente para dirimir quaisquer questões oriundas da aplicação do presente instrumento, com exclusão de qualquer outro, por mais privilegiado que seja.

E, por estarem de acordo, as partes assinam a presente Ata de Registro de Preços, juntamente com as testemunhas abaixo, para que produza seus jurídicos e legais efeitos, cientes de que ao GERENCIADOR é aplicável o disposto no artigo 150, inciso VI, alínea “c”, da Constituição Federal, no artigo 5º do Decreto-Lei nº 9.853, de 13 de setembro de 1946 e nos artigos 12 e 13 da Lei nº 2613, de 23 de setembro de 1955.

Recife, ____ de _____ de 20____.

_____
GERENCIADOR

_____
FORNECEDOR

TESTEMUNHAS:

_____
NOME:
CPF:

_____
NOME:
CPF:

SESC – Serviço Social do Comércio | Departamento Regional em Pernambuco | www.sescpe.org.br
Casa do Comércio/Edifício Josias Albuquerque | Avenida Visconde de Suassuna, nº 265, Santo Amaro - Recife-PE.
CEP: 50.050-540 TEL + 55 81 3216 1739