PREGÃO ELETRÔNICO SRP Nº 11/2022

DOCUMENTO DE ORIGEM: SIGED 2933/2022-29

SÍNTESE DO OBJETO E PROCEDIMENTOS

A PRODAM – Processamento de Dados Amazonas S.A, com base na Lei nº 13.303, de 30.06.2016, Decreto nº 10.024, de 20.09.2019 Decreto Estadual nº 39.032, de 24.05.2018, Lei nº 10.520, de 17.07.2002, Lei Complementar nº 123, de 14.12.2006, Decreto Estadual nº 21.178, de 27.09.2000, Decreto Estadual nº 24.818, de 27.01.2005, e alterações e RILC - Regulamento Interno de Licitações e Contratos da PRODAM, torna público a realização de processo licitatório, na modalidade de **PREGÃO ELETRÔNICO**, processado através do Sistema de Registro de Preços, no critério de julgamento **MENOR PREÇO GLOBAL**, modo de disputa **ABERTO**, a ser realizada na forma abaixo:

1. DO OBJETO

1.1 Contratação de Empresa Especializada para o fornecimento de Solução de Segurança Avançada para Endpoints e Servidores, com proteção integrada contra ataques complexos, direcionados e descoberta avançada de ameaças em nível de rede, com capacidade de respostas automatizadas a incidentes, bem como serviços de instalação, configuração, treinamento, serviços de consultoria e suporte técnico em sistemas de segurança na solução fornecida para prevenção de vírus de computador, spyware, APT e outras ameaças por um período de 36 meses, conforme especificações detalhadas no Termo de Referência, constante do Anexo I, deste Instrumento convocatório.

2. DO LOCAL, DA DATA E HORÁRIO

2.1 O pregão eletrônico será realizado conforme local, data e horários a seguir:

2.1.1 Endereço Eletrônico: https://www.gov.br/compras;
UASG: 927131 – PROCESSAMENTO DE DADOS AMAZONAS – PRODAM – PREGÃO ELETRÔNICO Nº 11/2022
2.1.2 Recebimento das propostas: de 09/11/2022 a 30/11/2022;
2.1.3 Abertura das propostas: dia 30/11/2022 às 10h, de Brasília;
2.1.4 Início da sessão de disputa de preços: dia 30/11/2022 às 10h30h, de Brasília;

2.2 Todas as referências de tempo no Instrumento convocatório, no Aviso e durante a Sessão pública do Pregão observarão obrigatoriamente o horário de **Brasília – DF** e, dessa forma, serão registradas no sistema eletrônico e na documentação relativa ao certame.

3. ORIGEM DE RECURSOS FINANCEIROS

3.1 A despesa com o pagamento do referido objeto será custeada com recursos próprios da PRODAM – Processamento de Dados Amazonas S.A.

4. DOS PRAZOS DE PEDIDO DE ESCLARECIMENTO, IMPUGNAÇÃO E RECURSO.

4.1 Para os pedidos de Esclarecimento: Deverão ser encaminhados ao e-mail: licitacoes@prodam.am.gov.br até 03 (três) dias úteis antes da data fixada para a abertura das propostas, devendo a PRODAM responder aos pedidos de esclarecimentos no prazo de 2 (dois) dias úteis;

4.2 Para a impugnação do Instrumento convocatório: Deverá ser encaminhada ao e-mail licitacoes@prodam.am.gov.br até 03 (três) dias úteis antes da data inicial fixada para abertura das propostas. A impugnação não possui efeito suspensivo e caberá ao pregoeiro, auxiliado pelos responsáveis pela elaboração do edital e dos anexos, decidir sobre a impugnação no prazo de 03 (três) dias úteis, contado da data de recebimento da impugnação. A concessão de efeito suspensivo à impugnação é medida excepcional e deverá ser motivada pelo pregoeiro, nos autos do processo de licitação.

4.3 Recurso:

4.3.1 Ao final da sessão pública, verificada a documentação do arrematante, o Pregoeiro irá declarar o licitante vencedor e abrirá o período para registro de manifestações de recurso dentro de **30 (trinta) minutos**. O proponente que desejar recorrer contra decisões do Pregoeiro poderá fazê-lo, manifestando a intenção de recurso com registro da síntese de suas razões no espaço previsto no próprio sistema eletrônico, sendo necessário juntar memoriais no prazo de 03 (três) dias úteis. Os interessados ficam, desde logo, intimados a apresentar contrarrazões em igual número de dias, que começarão a correr do término do prazo do recorrente.

4.3.2 A falta de manifestação, imediata e motivada, importará à preclusão do direito de recurso.

4.3.3 Não será concedido prazo para recursos sobre assuntos meramente protelatórios ou quando não justificada a intenção de interpor o recurso pelo proponente.

4.3.4 Os recursos contra decisões do Pregoeiro não terão efeito suspensivo.

4.4 Os recursos e contrarrazões de recurso deverão ser preenchidos em campo específico no próprio sistema e encaminhados ao e-mail licitacoes@prodam.am.gov.br, podendo também, ser protocolados junto à PRODAM, localizada na Rua Jonathas Pedrosa, 1937, Praça 14 de Janeiro, Manaus, Amazonas, CEP 69020-110, em dias úteis, no horário de 08:30 às 17 horas informando o número da licitação – **PREGÃO ELETRÔNICO SRP Nº 11/2022-PRODAM**.

5. DO CREDENCIAMENTO

5.1 Os interessados em participar deste pregão deverão dispor de registro cadastral no SICAF – Sistema De Cadastro Unificado De Fornecedores

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

5.2 O credenciamento junto ao provedor do sistema implica a responsabilidade do licitante ou de seu representante legal e a presunção de sua capacidade técnica para realização

das transações inerentes a este Pregão.

5.3 O uso da senha de acesso pelo LICITANTE é de sua responsabilidade exclusiva, incluindo qualquer transação efetuada diretamente ou por seu representante, não cabendo ao provedor do sistema ou à PRODAM, responsabilidade por eventuais danos decorrentes do uso indevido da senha, ainda que por terceiros

5.4 O credenciamento junto ao provedor do sistema implica a responsabilidade legal da LICITANTE e a presunção de sua capacidade técnica para realização das transações inerentes ao Pregão na forma eletrônica.

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

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

6. DAS CONDIÇÕES PARA PARTICIPAÇÃO

6.1. Poderão participar deste processo os interessados que atenderem a todas as exigências contidas neste Instrumento convocatório e seus Anexos.

6.2. Não poderão participar deste pregão os interessados que se enquadrarem em uma ou mais das situações relacionadas no art. 38 da Lei 13.303/16:

6.2.1. Cujo administrador ou sócio detentor de mais de 5% (cinco por cento) do capital social seja diretor ou empregado da empresa pública ou sociedade de economia mista contratante;

6.2.2. Suspensa pela empresa pública ou sociedade de economia mista;

6.2.3. Declarada inidônea pela União, por Estado, pelo Distrito Federal ou pela unidade federativa a que está vinculada a empresa pública ou sociedade de economia mista, enquanto perdurarem os efeitos da sanção;

6.2.4. Constituída por sócio de empresa que estiver suspensa, impedida ou declarada inidônea;

6.2.5. Cujo administrador seja sócio de empresa suspensa, impedida ou declarada inidônea;

6.2.6. Constituída por sócio que tenha sido sócio ou administrador de empresa suspensa, impedida ou declarada inidônea, no período dos fatos que deram ensejo à sanção;

6.2.7. Cujo administrador tenha sido sócio ou administrador de empresa suspensa, impedida ou declarada inidônea, no período dos fatos que deram ensejo à sanção;

6.2.8. Que tiver, nos seus quadros de diretoria, pessoa que participou, em razão de vínculo de mesma natureza, de empresa declarada inidônea.

6.3. É vedada também:

6.3.1 À contratação do próprio empregado ou dirigente, como pessoa física, bem como à participação dele em procedimentos licitatórios, na condição de licitante;

6.3.2 A quem tenha relação de parentesco, até o terceiro grau civil, com:

6.3.2.1 Dirigente de empresa pública ou sociedade de economia mista;

6.3.2.2 Empregado de empresa pública ou sociedade de economia mista cujas atribuições envolvam a atuação na área responsável pela licitação ou contratação;

6.3.2.3 Autoridade do ente público a que a empresa pública ou sociedade de economia mista esteja vinculada.

6.3.3 Cujo proprietário, mesmo na condição de sócio, tenha terminado seu prazo de gestão ou rompido seu vínculo com a respectiva empresa pública ou sociedade de economia mista promotora da licitação ou contratante há menos de 6 (seis) meses.

6.4. As condições de não participação e vedações serão consultadas na etapa de habilitação.

7. DA PARTICIPAÇÃO

7.1. A participação no certame se dará através de prévio credenciamento junto ao provedor do sistema, no site https://www.gov.br/compras, observando a data e os horários limites estabelecidos no **subitem 2.1** deste Instrumento convocatório.

7.2. Os licitantes deverão utilizar o certificado digital para acesso ao sistema.

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

7.4. No caso de desconexão com o Pregoeiro no decorrer da etapa competitiva do Pregão, o sistema eletrônico poderá permanecer acessível aos licitantes para a recepção dos lances, retornando o Pregoeiro, quando possível, sua atuação no certame, sem prejuízo dos atos realizados.

7.5. Quando a desconexão persistir por tempo superior a 10 (dez) minutos, a sessão do Pregão será suspensa e terá reinício somente após comunicação expressa aos participantes através do envio de mensagens pelo próprio sistema, marcando a sessão para continuidade do Pregão, havendo interstício de pelo menos 24 (vinte e quatro) horas entre os mesmos.

8. REGULAMENTO OPERACIONAL DO CERTAME

8.1. O certame será conduzido pelo Pregoeiro designado que terá, em especial, as seguintes atribuições:

I - conduzir a sessão pública;

II - receber, examinar e decidir as impugnações e os pedidos de esclarecimentos ao edital e aos anexos, além de poder requisitar subsídios formais aos responsáveis pela elaboração desses documentos;

III - verificar a conformidade da proposta em relação aos requisitos estabelecidos no edital;

IV - coordenar a sessão pública e o envio de lances;

V - verificar e julgar as condições de habilitação;

VI - sanar erros ou falhas que não alterem a substância das propostas, dos documentos de habilitação e sua validade jurídica;
VII - receber, examinar e decidir os recursos e encaminhá-los à autoridade competente quando mantiver sua decisão;
VIII - indicar o vencedor do certame;
IX - adjudicar o objeto, quando não houver recurso;
X - conduzir os trabalhos da equipe de apoio; e
XI - encaminhar o processo devidamente instruído à autoridade competente e propor a sua homologação.

Parágrafo único. O pregoeiro poderá solicitar manifestação técnica da assessoria jurídica ou de outros setores do órgão ou da entidade, a fim de subsidiar sua decisão.

9. DO ENVIO DAS PROPOSTAS DE PREÇOS

9.1 O encaminhamento de proposta pressupõe o pleno conhecimento e atendimento às exigências de habilitação previstas no Instrumento convocatório e seus Anexos. O fornecedor será responsável por todas as transações que forem efetuadas em seu nome no sistema eletrônico, assumindo como firmes e verdadeiras suas propostas e lances.

9.2 As propostas de preços terão seus valores definidos conforme os itens no Anexo 3 – Minuta da Ata de Registro de Preços.

9.3 Ao apresentar sua proposta e ao formular lances, o licitante concorda especificamente com as seguintes condições:

9.3.1 O objeto ofertado deverá atender a todas as especificações constantes do Anexo I do Instrumento convocatório.

9.4 O prazo de validade da proposta não poderá ser inferior a **90 (noventa)** dias contados da data da Sessão Pública do Pregão.

9.5 Da entrega: Por se tratar de um Pregão pelo Sistema de Registro de Preços – SRP, a Prodam não se obriga a adquirir o objeto licitado, só o fazendo quando houver necessidade, ocasião em que serão formalizados os instrumentos de contratos para atendimento da demanda, conforme especificado no Anexo 1 – Termo de Referência deste instrumento convocatório.

9.5.1 Os preços deverão ser cotados em moeda corrente nacional, sendo neles inclusos todas e quaisquer despesas consideradas para composição dos preços, tais como, transportes, impostos, seguros, tributos diretos e indiretos incidentes sobre o fornecimento do objeto.

9.5.2 A cotação apresentada e levada em conta para efeito de julgamento será da exclusiva e total responsabilidade do licitante, não lhe cabendo o direito de pleitear quaisquer alterações, seja para mais ou para menos.

9.5.3 Local de faturamento: Indicar o Município e o Estado onde será efetuado o faturamento.

9.6 No caso de fornecimento de materiais:

9.6.1 **Diferencial de ICMS -** Para efeito de comprovação da incidência do Imposto Sobre Circulação de Mercadorias e Serviços (ICMS), a PRODAM está enquadrada como contribuinte do ICMS, nas operações interestaduais, com a

alíquota de **18%. Para todo material adquirido fora do Estado será recolhido o diferencial de alíquota ao Estado do Amazonas.**

9.6.2 **Forma de apresentação dos preços**: Os licitantes de outros Estados deverão computar aos preços ofertados o percentual diferencial de alíquota de ICMS, **somente para efeito de julgamento**, correspondente a complementação de alíquota que será recolhida pela PRODAM ao Estado do Amazonas (Conforme Anexo 01-A – Modelo de Proposta de Preços). **Quando do envio de sua proposta final este percentual deverá ser expurgado.**

9.6.3 Os licitantes não abrangidos na área da Zona Franca de Manaus, não deverão incluir no seu preço o PIS e COFINS, em virtude da Lei Federal nº 10.996/2004, modificada pela Lei nº 11.945/2009, que estabelece que as vendas de mercadorias para as Zonas de Livre Comércio terão isenção tributária de PIS/COFINS. E ainda a isenção tributária do Imposto sobre produtos Industrializados – IPI, em conformidade com o Decreto 7.212/2010.

10. ABERTURA DAS PROPOSTAS E DISPUTA

10.1 Conforme previsto no Instrumento convocatório, antes do horário da disputa de lances, o Pregoeiro fará a abertura das propostas apresentadas para análise das mesmas e avaliar a aceitabilidade das propostas de preços. Havendo necessidade a licitante deverá informar a marca e o modelo do material ofertado. Desclassificará aquelas que não se adequarem ao disposto no Instrumento convocatório desta licitação.

10.2 Em seguida, a partir do horário previsto no sistema, terá início à sessão pública do Pregão Eletrônico, com a divulgação das propostas de preços recebidas pelo ***sistema*** e não desclassificadas, passando o Pregoeiro a receber os lances das licitantes.

10.3 Aberta a etapa competitiva, os representantes dos licitantes deverão estar conectados ao sistema para participar da sessão de lances. A cada lance ofertado o participante será imediatamente informado de seu recebimento e respectivo horário de registro e valor.

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

10.4 Durante o transcurso da sessão pública, os participantes serão informados, em tempo real, do valor do menor lance registrado. O sistema não divulgará o autor dos lances aos demais participantes. Os licitantes serão representados por seus códigos.

10.5 A etapa de lances da sessão pública terá duração de dez minutos e, após isso, será prorrogada automaticamente pelo sistema quando houver lances ofertados nos últimos dois minutos do período de duração da sessão pública.

10.6 O sistema informará a proposta de menor preço imediatamente após o encerramento da etapa de lances no período adicional de tempo.

10.7 Encerrada a etapa de lances da sessão pública, o Pregoeiro ratificará a proposta vencedora e poderá solicitar da licitante que envie os documentos descritos no **Anexo 2 – Documentos para habilitação**, para comprovar a regularidade de situação do autor da proposta, e solicitará a proposta comercial, contendo as especificações detalhadas do objeto licitado (preço unitário, preço total, e validade da proposta) atualizada em conformidade com o último lance, ambas no prazo máximo de 2h (duas horas) a contar da solicitação do pregoeiro; documentação essa avaliada conforme

este instrumento convocatório. O Pregoeiro verificará, também, o cumprimento às demais exigências para habilitação contidas nos Anexos deste Instrumento convocatório.

11. JULGAMENTO DAS PROPOSTAS

11.1 O Pregoeiro efetuará o julgamento das propostas pelo critério de **MENOR PREÇO,** podendo encaminhar, pelo sistema eletrônico, contraproposta diretamente ao licitante que tenha apresentado o lance de menor valor, para que seja obtido preço melhor, bem como decidir sobre sua aceitação, observados prazos para fornecimento, especificações técnicas e demais condições definidas neste Instrumento convocatório. O próprio sistema acusará quando houver empate técnico em se tratando de ME/EPP.

11.2 Após a sessão de lances, analisando a aceitabilidade ou não, o Pregoeiro analisará a documentação do arrematante.

11.3 Se a proposta ou lance de menor valor não atender as especificações técnicas e as condições mínimas de habilitação, o Pregoeiro examinará a proposta ou o lance subsequente, verificando a sua aceitabilidade e procedendo à sua habilitação, na ordem de classificação, e assim sucessivamente, até a apuração de uma proposta ou lance que atenda ao Instrumento convocatório.

11.3.1 Ocorrendo a situação a que se refere o subitem anterior, o Pregoeiro poderá negociar com o licitante para que seja obtido preço melhor para a PRODAM.

11.4 A proposta deverá ser apresentada em 01 (uma) via original, na língua portuguesa corrente no Brasil, salvo quanto às expressões técnicas impressas através de edição eletrônica de textos em papel timbrado do proponente, bem como ser redigida de forma clara, legível, sem rasuras, emendas ou entrelinhas.

11.5 Constatado o atendimento das exigências fixadas no Instrumento convocatório, a licitante será declarada vencedora do certame pelo Pregoeiro, desde que não haja a manifestação da intenção de interposição de recurso pelas licitantes, sendo adjudicado o objeto.

11.6 Caso seja declarada pelas licitantes a intenção de interpor recurso, estando devidamente motivado, conforme item 4.3 e acatada pelo Pregoeiro, será aberto o prazo legal para recebimento do recurso.

11.7 Se o adjudicatário, convocado dentro do prazo de validade da sua proposta, não apresentar situação regular, estará sujeito às penalidades previstas no **item 19**. Neste caso, o Pregoeiro examinará as ofertas subsequentes, e a habilitação dos proponentes observadas à ordem de classificação, até a apuração de uma que atenda ao Instrumento convocatório, sendo o respectivo proponente convocado para negociar redução do preço ofertado.

12. HOMOLOGAÇÃO

12.1 Não sendo declarada a intenção de interposição de recurso pelas licitantes, caberá ao Pregoeiro a adjudicação do objeto ao vencedor e Ao Diretor Presidente da PRODAM deliberar sobre a homologação do objeto ao vencedor do Pregão.

12.2 Havendo recurso, o Diretor-Presidente da PRODAM, após deliberar sobre o mesmo, adjudicará o objeto ao licitante vencedor, homologando também o processo.

12.3 Por se tratar de um pregão para registro de preços, a homologação do resultado desta licitação não implicará em direito à contratação.

13. DA ATA DE REGISTRO DE PREÇOS

13.1 Homologado o resultado da licitação, a PRODAM, respeitadas as ordens de classificação, convocará os interessados para assinatura da **Ata de Registro de Preços** que, após cumpridos os requisitos de publicidade, terá efeito de compromisso de fornecimento nas condições estabelecidas.

13.2 As convocações de que tratam o subitem anterior deverão ser atendidas no prazo máximo de 5 (cinco) dias úteis, prorrogável apenas 1 (uma) única vez e por igual período, desde que a solicitação seja apresentada ainda durante o transcurso do interstício inicial, desde que ocorra motivo justificado e aceito pela PRODAM, sob pena de decair o direito à contratação, sem prejuízo das sanções cabíveis.

13.3 A Ata firmada com os licitantes fornecedores observará o modelo do Anexo 3 – Minuta da Ata de Registro de Preços

13.4 Sempre que o licitante vencedor não atender à convocação, nos termos definidos no subitem 13.2, é facultado à Administração, dentro do prazo e condições estabelecidos, convocar remanescentes, na ordem de classificação, para fazê-lo em igual prazo e nas mesmas condições, ou revogar o item específico, respectivo ou a licitação.

13.5 Ao assinar a Ata de Registro de Preços, a adjudicatária obriga-se a fornecer o objeto a ela adjudicado, quando solicitado, conforme especificações e condições contidas neste Instrumento convocatório, em seus anexos e também na proposta apresentada, prevalecendo, no caso de divergência, as especificações e condições deste Instrumento convocatório.

13.6 A empresa fornecedora ficará obrigada a atender a todas as demandas solicitadas pela PRODAM, durante a vigência da Ata de Registro de Preços, mesmo se a entrega deles decorrente for prevista para data posterior ao seu vencimento.

13.7 Para cada demanda de serviços deverá ser celebrado instrumento de contrato, conforme Anexo 7 – Minuta de Contrato.

13.8 Caso o objeto não corresponda no todo ou em parte ao especificado no instrumento convocatório e seus respectivos anexos, o fornecedor deverá corrigir ou entregar, sem ônus para a PRODAM, o objeto do contrato, sob pena de aplicação de sanções a critério da Administração

13.9 A Ata de Registro de Preços terá validade de 12 (doze) meses contada a partir da data de sua assinatura

14. GARANTIA

14.1 O fornecedor deverá proceder conforme solicitado no termo de referência.

15. OBRIGAÇÕES DO FORNECEDOR

15.1 Assinar a Ata de Registro de Preços.
15.2 Entregar o objeto conforme solicitação documentada no **Pedido de Compra/ Autorização de Execução de Serviços,** obedecendo aos prazos, bem como as especificações, objeto deste Instrumento convocatório.
15.3 Prestar os esclarecimentos que forem solicitados pela PRODAM e atender prontamente a eventuais solicitações/reclamações.
15.4 Dispor-se a toda e qualquer fiscalização da PRODAM, no tocante ao produto, assim como ao cumprimento das obrigações previstas neste Instrumento convocatório
15.5 Prover todos os meios necessários à garantia da plena operacionalidade do objeto contratado, inclusive considerados os casos de greve ou paralisação de qualquer natureza
15.6 Manter durante toda a execução da Ata de Registro de Preços, em compatibilidade com as obrigações por ela assumidas, todas as condições de habilitação e qualificação exigidas na licitação.

16. OBRIGAÇÕES DA PRODAM

16.1 Efetuar o registro do fornecedor e firmar a correspondente Ata de Registro de Preços;
16.2 Conduzir os procedimentos relativos a eventuais renegociações dos preços registrados;
16.3 Aplicar as sanções por descumprimento do pactuado na Ata de Registro de Preços;
16.4 Efetuar os pagamentos devidos ao Fornecedor, nas condições estabelecidas neste Instrumento convocatório;
16.5 Promover, por intermédio de colaborador indicado, a fiscalização e o acompanhamento da execução do objeto contratado, para que, durante a vigência da Ata de Registro de Preços, sejam mantidas as condições de habilitação e qualificação exigidas nesta licitação.

17. DO FORNECIMENTO E DO RECEBIMENTO DO OBJETO

17.1 Quando tiver necessidade e disponibilidade financeira, a PRODAM demandará a execução do objeto contratado, nas especificações e quantidades a serem adquiridas, encaminhando ao fornecedor e-mail:
17.2 Observado o prazo de entrega previsto no Anexo 1 – Termo de Referência deste instrumento convocatório, a PRODAM emitirá ao fornecedor, documento de termo de recebimento definitivo com o respectivo atesto dos serviços homologados, quanto à qualidade e quantidade
17.3 A aprovação do objeto pela PRODAM não exclui a responsabilidade civil do fornecedor por vícios de quantidade ou qualidade do mesmo ou disparidades com as especificações estabelecidas no Anexo 1 – Termo de Referência deste instrumento convocatório

18. DO PAGAMENTO

18.1 O prazo de pagamento será conforme estabelecido no Termo de Referência – Anexo 1 deste instrumento, realizado após os atestos e autorizações das áreas competentes da PRODAM.

18.2 Os pagamentos devidos pela PRODAM serão liquidados através de cheque nominal ou, através de depósito em conta corrente indicada pelo fornecedor.

18.3 No ato do pagamento, se houver qualquer multa a descontar, será o valor correspondente deduzido da quantia devida.

18.4 Será exigido do fornecedor quando da apresentação da Nota Fiscal correspondente cópia da seguinte documentação: prova de inscrição regular junto ao Cadastro Nacional de Pessoas Jurídicas (CNPJ), prova de regularidade fiscal e previdenciária, apresentando Certidão Negativa de Débitos relativos a Créditos Tributários Federais e à Dívida Ativa da União (C.N.D.) (portaria conjunta PGFN/RFB nº 1751/2014), prova de regularidade para com o Fundo de Garantia por Tempo de Serviço, Certidão de Regularidade de Situação junto ao F.G.T.S., Prova de regularidade para com a Fazenda Estadual e Municipal do domicílio do fornecedor ou outra equivalente, em validade; Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943 (NR)

18.4.1 Conforme disposto na Cláusula 2ª, inciso I, do protocolo ICMS 42, publicado no Diário Oficial da União (DOU) de 15/07/2009 e do Decreto nº 30.775 de 1/12/2010, os fornecedores deverão emitir Nota Fiscal Eletrônica nas compras governamentais, logo o licitante vencedor deverá emitir nota fiscal eletrônica

19. SANÇÕES ADMINISTRATIVAS.

19.1 Aos proponentes que ensejarem o retardamento da execução do certame; não mantiverem a proposta; falharem ou fraudarem a execução da presente aquisição; comportarem-se de modo inidôneo; fizerem declaração falsa ou cometerem fraude fiscal; poderão ser aplicadas, conforme o caso, as seguintes sanções, sem prejuízo da reparação dos danos causados à PRODAM pelo infrator:

19.1.1 Advertência e anotação restritiva no Cadastro de Fornecedores da PRODAM;

19.1.2 Multa;

19.1.3 Suspensão temporária de participação em licitação e impedimento de contratar com a Prodam, não superior a 2 (dois) anos;

19.2 Não será aplicada multa se, comprovadamente, o atraso da entrega do objeto advir de caso fortuito ou motivo de força maior, ambos aceitos pela PRODAM.

19.2 A aplicação das penalidades ocorrerá após defesa prévia do interessado, no prazo de 10 (dez) dias úteis a contar da intimação do ato.

20. DISPOSIÇÕES FINAIS

20.1 A presente licitação não importa necessariamente em contratação, podendo a Administração da PRODAM revogá-la no todo ou em parte, por razões de interesse público, derivadas de fato superveniente comprovado ou anulá-la por ilegalidade, de ofício ou por provocação mediante ato escrito e fundamentado disponibilizado no sistema para o conhecimento dos participantes da licitação – não gerando a obrigação de indenizar.

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

20.3 O proponente 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 implicará imediata desclassificação do proponente que o tiver apresentado, ou, caso tenha sido o vencedor, a rescisão do contrato, sem prejuízo das demais sanções cabíveis.

20.4 Após apresentação da proposta, não caberá desistência, salvo por motivo justo decorrente de fato superveniente e aceito pelo Pregoeiro.

20.5 Na contagem dos prazos estabelecidos neste Instrumento convocatório, excluir-se-á o dia do início e incluir-se-á o do vencimento. Só se iniciam e vencem os prazos em dias de expedientes na PRODAM.

20.6 É facultado ao Pregoeiro, ou à Autoridade Superior, em qualquer fase da licitação, promover diligências com vistas a esclarecer ou a complementar a instrução do processo, vedada a inclusão posterior de documento ou informação que deveria constar no ato da sessão pública.

20.7 Os proponentes intimados para prestar quaisquer esclarecimentos adicionais deverão fazê-lo no prazo determinado pelo Pregoeiro, sob pena de desclassificação/inabilitação.

20.8 O desatendimento de exigências formais não essenciais não importará no afastamento do proponente, desde que seja possível a aferição da sua qualificação e a exata compreensão da sua proposta.

20.9 As normas que disciplinam este Pregão serão sempre interpretadas em favor da ampliação da disputa entre os proponentes, desde que não comprometam o interesse da Administração, a finalidade e a segurança da contratação.

20.10 As decisões referentes a este processo licitatório poderão ser comunicadas aos proponentes por qualquer meio de comunicação que comprove o recebimento; ou através por meio do sistema eletrônico através do site http://www.comprasgovernamentais.gov.br; ou através da publicação no portal de transparência da PRODAM; ou, ainda, mediante publicação no Diário Oficial do Estado do Amazonas

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

20.12 O Instrumento convocatório encontra-se disponível no site

http://www.comprasgovernamentais.gov.br/, bem como na página da PRODAM na internet, no endereço www.prodam.am.gov.br.

20.13 O foro designado para julgamento de quaisquer questões judiciais resultantes deste instrumento convocatório será o local da realização do certame, considerado aquele a que está vinculado ao Pregoeiro.

20.14 São partes integrantes deste instrumento convocatório:

20.14.1 **Anexo 1** – Termo de Referência;

20.14.1.1 – **Anexo 01-A** – Modelo de Proposta de Preços:

20.14.2 **Anexo 2** – Documentos para Habilitação;

20.14.3 **Anexo 3** – Minuta da Ata de Registro de Preços;

20.14.3.1 **Anexo 3-A** – Anexo da Minuta da Ata de Registro de Preços;

20.14.4 **Anexo 4** – Modelo de Declaração de Fato Superveniente Impeditivo de Habilitação;

20.14.5 **Anexo 5** – Modelo de Declaração Quanto ao Cumprimento às Normas Relativas ao Trabalho do Menor;

20.14.6 **Anexo 6** – Tabela de Preço Máximo;

20.14.7 **Anexo 7** – Minuta de Contrato

20.14.7 **Anexo 7-A** – Anexo da Minuta de Contrato – Termo de Responsabilidade e Confidencialidade para Fornecedores e Parceiros

Manaus (AM), 01 de novembro de 2022

GILSON DE SENA DA SILVA

Assinado de forma digital por GILSON DE SENA DA SILVA
Dados: 2022.11.07 12:29:40 -04'00'

Gilson de Sena da Silva
Pregoeiro

Equipe de Apoio:
Cleane Vidal Teixeira (Presidente COMLI)
Endel Batista Passos (Secretário)

Aprovação Assessoria Jurídica:

PREGÃO ELETRÔNICO SRP 11/2022

ANEXO 1 – TERMO DE REFERÊNCIA

1. DA IDENTIFICAÇÃO DA PRODAM

1.1. Razão Social: PRODAM – Processamento de Dados Amazonas S/A;

1.2. **CNPJ:** 04.407.920/0001-80;

1.3. Endereço sede: Rua Jonathas Pedrosa, n°1937. Praça 14 de Janeiro. Manaus -AM. CEP 69020-110;

1.4. Endereço eletrônico: www.prodam.am.gov.br / sacp@prodam.am.gov.br;

1.5. Contato: 2121-6500 / 2121-6490 / 0800-0922626;

1.6. Diretor Presidente: Lincoln Nunes da Silva.

2. DO OBJETO

2.1. Contratação de empresa especializada para o fornecimento de Solução de Segurança Avançada para Endpoints e Servidores, com proteção integrada contra ataques complexos, direcionados e descoberta avançada de ameaças em nível de rede, com capacidade de respostas automatizadas a incidentes, bem como serviços de instalação, configuração, treinamento, serviços de consultoria e suporte técnico em sistemas de segurança na solução fornecida para prevenção de vírus de computador, spywares, APT e outras ameaças por um período de 36 meses.

3. ÁREA DEMANDANTE

3.1. Este processo tem como setor demandante a área comercial da PRODAM através do SIGED MEMO Nº 002/2022-GENEG/PRODAM.

4. DA JUSTIFICATIVA

4.1. A PRODAM tem como objetivo organizacional a prestação de serviços especializados em Tecnologia da Informação e Comunicação aos órgãos integrantes da Administração Pública Estadual, prioritariamente. No Art. 5º do seu estatuto, em parágrafo único, estabelece: “Os recursos financeiros obtidos pela PRODAM serão prioritariamente orientados para atualização do parque tecnológico e a capacitação técnica, objetivando a segurança dos dados ...”. A PRODAM

disponibiliza serviços públicos para o cidadão, presta serviço de tecnologia da informação e comunicação e segurança da informação para grande parte dos órgãos do poder executivo estadual, e necessita dispor de ferramentas para proteção da informação para evitar a exploração de vulnerabilidades no ambiente tecnológico como contaminação por malwares, vazamento de informações e roubo de dados, dentre outros que, se concretizados, podem acarretar prejuízos financeiros e danos à imagem institucional.

4.2. As soluções de antivírus/antimalwares são a camada de proteção de dados mais básica em uma organização. São necessárias para evitar ameaças advindas por dispositivos de rede como estações de trabalho, notebooks, servidores e dispositivos móveis e quando bem configuradas reduzem consideravelmente os riscos de contaminação por malwares, vazamento de informações, phishing, ransomware, roubo de dados, dentre outros. Estima-se que 70% dos ataques de segurança da informação iniciam-se através dos endpoints. Face ao término do período de vigência da licença de atualização e suporte do software do tipo antivírus para proteção das estações de trabalho, servidores e dispositivos móveis, adquirida em 2019 pela PRODAM e diante do aumento na quantidade e sofisticação das ameaças cibernéticas nos últimos anos, além da popularização do trabalho remoto a partir da pandemia do Covid-19, torna-se este recurso uma camada de segurança imprescindível e que precisa ter suas facilidades estendidas para proteção de vulnerabilidades e identificação e resposta a incidentes, sendo desejável que se integre a outras camadas de segurança de rede. Portanto, devido as responsabilidades inerentes e legais da PRODAM, busca-se manter altos níveis de proteção para o ambiente de redes de computadores da PRODAM, seu datacenter bem como oferecer aos seus clientes serviços de proteção de “endpoints”.

4.3. Seguindo as tendências mundiais do mercado, as soluções de next generation antimalware são uma evolução da tradicional proteção de antivírus para endpoints, que não são mais suficientes para reduzir a superfície dos ataques cibernéticos a partir destes dispositivos. As soluções de Next Generation antimalware utilizam técnicas de segurança para analisar o comportamento de malware's, novos e desconhecidos, para descobrir as táticas de invasão através de técnicas de

segurança que incluem inteligência artificial (IA) e aprendizagem de máquina (ML). Estas soluções estão evoluindo para além do EPP (Endpoint Protection Plataform), que possuem recursos de segurança como por exemplo malware, anti-ransomware, anti-exploit prevention, proteção preventiva com Deep Learning ATP - Advanced Threat Protection (detecta ameaças conhecidas e desconhecidas), para bloquear acesso a vulnerabilidades, realizar detecção e resposta a incidentes de segurança da informação de forma proativa, com EDR (Endpoint Detection and Response) gerenciado por ferramentas de XDR, que pode integrar-se a uma solução de NDR (Network detection and response) para detecção e resposta a incidentes na rede corporativa.

4.4. SIGLAS

AI	Artificial intelligence (especialmente quando utilizado para identificar e alertar ameaças desconhecidas)
EDR	Endpoint detection and response (para estágios de pós infecção de um ataque ou exploit)
EPP	Endpoint protection platform (ofecece prevenção para malwares ou exploits)
ML	Machine learning (ex., quando agentes utilizam algoritmos matemáticos para determinar as ameaças)
XDR	Extended detection and response (um sistema unificado que combina as fontes de telemetria e integra múltiplas ferramentas, em console única, geralmente com análise por inteligência artificial e automatizada, para detecção e resposta a incidentes de segurança da informação mais rápida e precisa)
NDR	Network Detection and Response (ou Detecção e Resposta de Rede, em português) é a ferramenta capaz de coletar e analisar o tráfego de redes corporativas para identificar e responder a ataques cibernéticos, permitindo que os mesmos sejam neutralizados.
CASB	Cloud Acess Security Brocker (um software local ou baseado em nuvem que fica entre os usuários do serviço em nuvem e os aplicativos em nuvem e monitora todas as atividades e aplica as políticas de segurança.)

5. DOS RESULTADOS ESPERADOS

5.1. Proteger Endpoints e Servidores de camada de proteção contra vírus, malwares e ameaças cibernéticos;

5.2. Garantir a integridade das informações sob custodia da empresa;

5.3. Proporcionar facilidade na gestão da solução de segurança dos endpoints e servidores;

5.4. Disponibilizar ambiente em nuvem para gestão e atualização da solução;

5.5. Disponibilizar informações úteis sobre as estações de trabalho e dispositivos móveis;

5.6. Proteger o e-mail no Office 365;

5.7. Gerar dados e informações para maior eficiência das equipes de tratamento e resposta a incidentes com a oferta dos serviços de EDR;

5.8. Dar maior agilidade da detecção e eliminação de acesso a arquivos e links infectados;

5.9. Dar maior aderência com a legislação e orientações relacionadas à proteção de dados pessoais e a segurança das informações;

5.10. Atender a demanda de soluções de endpoint e servidores para os clientes.

5.11. Criar uma “prateleira” de produtos de segurança passível de ser ofertada como serviço aos clientes da PRODAM;

5.12. Possibilitar a renovação de licenças de antivírus para DATACENTERS.

6. DA COMPOSIÇÃO DOS LOTES

6.1. **LOTE ÚNICO** – Solução de Proteção para uso Geral

ITEM	DESCRIÇÃO	Unidade	Quantidade
1	Aquisição de Licenças da Solução de Proteção Avançada para *Endpoints* e Servidores Físicos com validade de 36 meses	Licença	20.000
2	Aquisição de Licenças da Solução de Proteção Avançada para Ambientes Virtuais com validade de 36 meses	Licença	1.000
3	Aquisição de Licenças da Solução de Proteção para Mobile com validade de 36 meses	Licença	1.000
4	Aquisição de Licença da Solução de descoberta avançada de ameaças em nível de rede, com capacidade de análise de até 1 Gbit/s de Throughput, com validade de 36 meses	Licença	1
5	Aquisição de Licença de Plataforma automatizada de conscientização em Segurança da Informação com validade de 36 meses	Usuário	2.500
6	Treinamentos		
6.1	Serviço de treinamento da Solução de Proteção	Turma	4
6.2	Serviço de treinamento para resposta à incidentes	Turma	1
7	Serviço de Consultoria e Suporte Técnico na Solução de Proteção Avançada	Hora	2.100

6.2. **Sobre o não parcelamento da solução**

6.2.1. O agrupamento dos itens em um lote único, levou em consideração questões técnicas, bem como o ganho de economia em escala, sem prejuízo a ampla competitividade, uma vez que existem no mercado vários fabricantes com capacidade de fornecer a solução na forma em que está agrupada nesta contratação. O agrupamento encontra ainda justificativa em decisões já deliberadas pelo TCU sobre a matéria, tais como, o informativo 106 do TCU que traz decisão que "A aquisição de itens diversos em lotes deve estar respaldada em critérios justificantes", adotando o entendimento do acórdão 5260/2011 – TCU – 1a câmara, de 06/07/2011, que decidiu que "Inexiste ilegalidade na realização de pregão com previsão de adjudicação por lotes, e não por itens, desde que os lotes sejam integrados por itens de uma mesma natureza e que guardem correlação entre si "

7. DAS ESPECIFICAÇÕES TÉCNICAS

7.1. **Solução de Proteção Avançada para Endpoints e Servidores Físicos com validade de 36 meses – ITEM 1,** o qual deverá atender aos requisitos técnicos enumerados a seguir:

7.1.1. **Servidor de Administração e Console Administrativa**

7.1.2. **Compatibilidade:**

7.1.2.1. Microsoft Windows Server 2008 (Todas edições);

7.1.2.2. Microsoft Windows Server 2008 x64 SP1 (Todas edições);

7.1.2.3. Microsoft Windows Server 2008 R2 (Todas edições);

7.1.2.4. Microsoft Windows Server 2012 (Todas edições x64);

7.1.2.5. Microsoft Windows Server 2012 R2 (Todas edições x64);

7.1.2.6. Microsoft Windows Server 2016 x64

7.1.2.7. Microsoft Windows Small Business Server 2008 (Todas edições);

7.1.2.8. Microsoft Windows Small Business Server 2011 (Todas edições);

7.1.2.9. Microsoft Windows 7 SP1 Professional / Enterprise / Ultimate x32/x64;

7.1.2.10. Microsoft Windows 7 SP1 Professional / Enterprise / Ultimate x32/x64;

7.1.2.11. Microsoft Windows 8 SP1 Professional / Enterprise x32/x64;

7.1.2.12. Microsoft Windows 8 Professional / Enterprise x64;

7.1.2.13. Microsoft Windows 8.1 Professional / Enterprise x32;

7.1.2.14. Microsoft Windows 8.1 Professional / Enterprise x64;

7.1.2.15. Microsoft Windows 10 (Todas edições x32);

7.1.2.16. Microsoft Windows 10 (Todas edições x64);

7.1.3. **Suporta as seguintes plataformas virtuais:**

7.1.3.1. Vmware: Workstation 12.x Pro, vSphere 5.5, vSphere 6;

7.1.3.2. Microsoft Hyper-V: 2008, 2008 R2, 2008 R2 SP1, 2012, 2012 R2;

7.1.3.3. 1.2.4. Microsoft Virtual PC 6.0.156.0;

7.1.3.4. 1.2.5. Parallels Desktop 7 e 11;

7.1.3.5. 1.2.6. Oracle VM VirtualBox 4.0.4-70112;

7.1.3.6. 1.2.7. Citrix XenServer 6.2 e 6.5;

7.1.4. **Características:**

7.1.4.1. A console deve ser acessada via WEB (HTTPS) ou MMC;

7.1.4.2. Console deve ser baseada no modelo cliente/servidor;

7.1.4.3. Compatibilidade com Windows Failover Clustering ou outra solução de alta disponibilidade;

7.1.4.4. Deve permitir a atribuição de perfis para os administradores da Solução de Antivírus;

7.1.4.5. Deve permitir incluir usuários do AD para logarem na console de administração

7.1.4.6. Console deve ser totalmente integrada com suas funções e módulos caso haja a necessidade no futuro de adicionar novas tecnologias tais como, criptografia, Patch management e MDM;

7.1.4.7. As licenças deverão ser perpétuas, ou seja, expirado a validade da mesma o produto deverá permanecer funcional para a proteção contra códigos maliciosos utilizando as definições até o momento da expiração da licença;

7.1.4.8. Capacidade de remover remotamente e automaticamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores;

7.1.4.9. Capacidade de instalar remotamente a solução de antivírus nas estações e servidores Windows, através de compartilhamento administrativo, login script e/ou GPO de Active Directory;

7.1.4.10. Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria;

7.1.4.11. Deve armazenar histórico das alterações feitas em políticas;

7.1.4.12. Deve permitir voltar para uma configuração antiga da política de acordo com o histórico de alterações efetuadas pelo administrador apenas selecionando a data em que a política foi alterada;

7.1.4.13. Deve ter a capacidade de comparar a política atual com a anterior, informando quais configurações foram alteradas;

7.1.4.14. A solução de gerência deve permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas;

7.1.4.15. Através da solução de gerência, deve ser possível verificar qual licença está aplicada para determinado computador;

7.1.4.16. Capacidade de instalar remotamente a solução de segurança em smartphones e tablets de sistema iOS e Android;

7.1.4.17. Capacidade de instalar remotamente qualquer “app” em smartphones e tablets de sistema iOS;

7.1.4.18. A solução de gerência centralizada deve permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle;

7.1.4.19. 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;

7.1.4.20. Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux e Mac) protegidos pela solução antivírus;

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

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

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

7.1.4.24. Capacidade de atualizar os pacotes de instalação com as últimas

vacinas;

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

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

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

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

- Nome do computador;
- Nome do domínio;
- Range de IP;
- Sistema Operacional;
- Máquina virtual.

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

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

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

7.1.4.32. 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;

7.1.4.33. 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 antivírus instalado. Caso não possuir, deve instalar o antivírus

automaticamente;

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

7.1.4.35. 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;

7.1.4.36. Deve fornecer as seguintes informações dos computadores:

7.1.4.37. Se o antivírus está instalado;

7.1.4.38. Se o antivírus está iniciado;

7.1.4.39. Se o antivírus está atualizado;

7.1.4.40. Minutos/horas desde a última conexão da máquina com o servidor administrativo;

7.1.4.41. Minutos/horas desde a última atualização de vacinas;

7.1.4.42. Data e horário da última verificação executada na máquina;

7.1.4.43. Versão do antivírus instalado na máquina;

7.1.4.44. Se é necessário reiniciar o computador para aplicar mudanças;

7.1.4.45. Data e horário de quando a máquina foi ligada;

7.1.4.46. Quantidade de vírus encontrados (contador) na máquina;

7.1.4.47. Nome do computador;

7.1.4.48. Domínio ou grupo de trabalho do computador;

7.1.4.49. Data e horário da última atualização de vacinas;

7.1.4.50. Sistema operacional com Service Pack;

7.1.4.51. Quantidade de processadores;

7.1.4.52. Quantidade de memória RAM;

7.1.4.53. Usuário(s) logado(s) naquele momento, com informações de contato (caso disponíveis no Active Directory);

7.1.4.54. Endereço IP;

7.1.4.55. Aplicativos instalados, inclusive aplicativos de terceiros, com histórico de instalação, contendo data e hora que o software foi instalado ou

removido;

7.1.4.56. Atualizações do Windows Updates instaladas;

7.1.4.57. Informação completa de hardware contendo: processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de áudio, adaptadores de rede, monitores, drives de CD/DVD;

7.1.4.58. Vulnerabilidades de aplicativos instalados na máquina;

7.1.4.59. Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterá-las;

7.1.4.60. Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como:

7.1.4.60.1. Alteração de Gateway Padrão;

7.1.4.60.2. Alteração de subrede;

7.1.4.60.3. Alteração de domínio;

7.1.4.60.4. Alteração de servidor DHCP;

7.1.4.60.5. Alteração de servidor DNS;

7.1.4.60.6. Alteração de servidor WINS;

7.1.4.60.7. Alteração de subrede;

7.1.4.60.8. Resolução de Nome;

7.1.4.60.9. Disponibilidade de endereço de conexão SSL;

7.1.4.61. Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet;

7.1.4.62. Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes;

7.1.4.63. Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus;

7.1.4.64. Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos;

7.1.4.65. 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;

7.1.4.66. 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;

7.1.4.67. Capacidade de exportar relatórios para os seguintes tipos de arquivos: PDF, HTML e XML;

7.1.4.68. Capacidade de gerar traps SNMP para monitoramento de eventos;

7.1.4.69. Capacidade de enviar e-mails para contas específicas em caso de algum evento;

7.1.4.70. Listar em um único local, todos os computadores não gerenciados na rede;

7.1.4.71. Deve encontrar computadores na rede através de no mínimo três formas: Domínio, Active Directory e subredes;

7.1.4.72. Deve possuir compatibilidade com Microsoft NAP, quando instalado em um Windows 2008 Server;

7.1.4.73. Capacidade de baixar novas versões do antivírus direto pela console de gerenciamento, sem a necessidade de importá-los manualmente

7.1.4.74. 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;

7.1.4.75. Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado intervalo de tempo);

7.1.4.76. Deve através de opções de optimizações fazer com que o computador gerenciado conceda recursos à outras aplicações, mantendo o antivírus ativo porém sem comprometer o desempenho do computador;

7.1.4.77. Deve permitir a configuração de senha no endpoint e configurar quando que será necessário a utilizá-la, (ex: Solicitar senha quando alguma tarefa de scan for criada localmente no endpoint);

7.1.4.78. 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;

7.1.4.79. Deve ser capaz de configurar quais eventos serão armazenados localmente, nos eventos do windows ou ainda se serão mostrados na tela para o colaborador, sejam estes eventos informativos, de alertas ou de erros;

7.1.4.80. Capacidade de realizar atualização incremental de vacinas nos computadores clientes;

7.1.4.81. Deve armazenar localmente e enviar ao servidor de gerência a ocorrência de vírus com os seguintes dados, no mínimo:

- Nome do vírus;
- Nome do arquivo infectado;
- Data e hora da detecção;
- Nome da máquina ou endereço IP;
- Ação realizada.

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

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

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

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

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

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

7.1.4.88. Capacidade de diferenciar máquinas virtuais de máquinas físicas.

7.1.5. **Estações Windows**

7.1.5.1. **Compatibilidade:**

7.1.5.1.1. Microsoft Windows XP Professional x86;

7.1.5.1.2. Microsoft Windows Vista x86 / x64 SP2;

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

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

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

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

7.1.5.1.7. Microsoft Windows Server 2012 R2 Standard x64;

7.1.5.1.8. Microsoft Windows Server 2012 Foundation x64;

7.1.5.1.9. Microsoft Windows Server 2012 Standard x64;

7.1.5.1.10. Microsoft Small Business Server 2011 Standard x64;

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

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

7.1.5.1.13. Microsoft Windows Server 2016 x64

7.1.5.2. **Características:**

7.1.5.2.1. Deve prover as seguintes proteções:

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

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

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

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

7.1.5.2.1.5. Firewall com IDS;

7.1.5.2.1.6. Autoproteção (contra-ataques aos serviços/processos

do antivírus);

7.1.5.2.1.7. Controle de dispositivos externos;

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

7.1.5.2.1.9. Controle de acesso a sites por horário;

7.1.5.2.1.10. Controle de acesso a sites por usuários;

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

7.1.5.2.1.12. Controle de execução de aplicativos;

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

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

7.1.5.2.3. 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);

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

7.1.5.2.5. 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 antivírus, (ex: “Win32.Trojan.banker”) para que qualquer objeto detectado com o veredicto escolhido seja ignorado;

7.1.5.2.6. 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;

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

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

7.1.5.2.9. 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;

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

7.1.5.2.11. Capacidade de verificar somente arquivos novos e alterados;

7.1.5.2.12. Capacidade de verificar objetos usando heurística;

7.1.5.2.13. Capacidade de agendar uma pausa na verificação;

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

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

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

7.1.5.2.16.1. Perguntar o que fazer, ou;

7.1.5.2.16.2. Bloquear acesso ao objeto;

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

7.1.5.2.16.4. Caso positivo de desinfecção:

7.1.5.2.16.5. Restaurar o objeto para uso;

7.1.5.2.16.6. Caso negativo de desinfecção:

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

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

7.1.5.2.18. Capacidade de verificar e-mails recebidos e enviados nos protocolos POP3, POP3S, IMAP, NNTP, SMTP e MAPI;

7.1.5.2.19. Capacidade de verificar links inseridos em e-mails contra phishings;

7.1.5.2.20. Capacidade de verificar tráfego nos browsers: Internet Explorer, Firefox, Google Chrome e Opera;

7.1.5.2.21. Capacidade de verificação de corpo e anexos de e-mails usando heurística;

7.1.5.2.22. O antivírus de e-mail, ao encontrar um objeto potencialmente perigoso, deve:

7.1.5.2.22.1. Perguntar o que fazer, ou;

7.1.5.2.22.2. Bloquear o e-mail;

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

7.1.5.2.22.4. Caso positivo de desinfecção:

7.1.5.2.22.4.1. Restaurar o e-mail para o usuário;

7.1.5.2.22.5. Caso negativo de desinfecção:

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

7.1.5.2.23. Caso o e-mail conter código que parece ser, mas não é definitivamente malicioso, o mesmo deve ser mantido em quarentena;

7.1.5.2.24. Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados;

7.1.5.2.25. Capacidade de filtrar anexos de e-mail, apagando-os ou renomeando-os de acordo com a configuração feita pelo administrador;

7.1.5.2.26. Capacidade de verificação de tráfego HTTP/HTTPS e qualquer script do Windows Script Host (JavaScript, Visual Basic Script, etc), usando heurísticas;

7.1.5.2.27. Deve ter suporte total ao protocolo Ipv6;

7.1.5.2.28. Capacidade de alterar as portas monitoradas pelos módulos de Web e E-mail;

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

7.1.5.2.29.1. Perguntar o que fazer, ou;

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

7.1.5.2.29.3. Permitir acesso ao objeto;

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

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

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

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

7.1.5.2.31. 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;

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

7.1.5.2.33. 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;

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

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

7.1.5.2.36. 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;

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

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

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

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

7.1.5.2.38.1. Discos de armazenamento locais;

7.1.5.2.38.2. Armazenamento removível;

7.1.5.2.38.3. Impressoras;

7.1.5.2.38.4. CD/DVD;

7.1.5.2.38.5. Drives de disquete;

7.1.5.2.38.6. Modems;

7.1.5.2.38.7. Dispositivos de fita;

7.1.5.2.38.8. Dispositivos multifuncionais;

7.1.5.2.38.9. Leitores de smart card;

7.1.5.2.38.10. Dispositivos de sincronização via ActiveSync (Windows CE, Windows Mobile, etc);

7.1.5.2.38.11. Wi-Fi;

7.1.5.2.38.12. Adaptadores de rede externos;

7.1.5.2.38.13. Dispositivos MP3 ou smartphones;

7.1.5.2.38.14. Dispositivos Bluetooth;

7.1.5.2.38.15. Câmeras e Scanners.

7.1.5.2.39. 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;

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

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

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

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

7.1.5.2.44. 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);

7.1.5.2.45. O controle de aplicações deve ter a capacidade de criar regras seguindo os seguintes modos de operação:

7.1.5.2.45.1. Black list: Permite a execução de qualquer aplicação, exceto pelas especificadas por regras.

7.1.5.2.45.2. White list: Impede a execução de qualquer aplicação, esxeto pelas especificadas por regras.

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

7.1.5.2.47. 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;

7.1.5.2.48. 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;

7.1.5.2.49. 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.

7.1.5.2.50. Capacidade de voltar ao estado anterior do sistema operacional após um ataque de malware.

7.1.5.2.51. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros.

7.1.5.2.52. Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning).

7.1.5.2.53. Capacidade de integração com o Windows Defender Security Center.

7.1.5.2.54. Capacidade de integração com a Antimalware Scan Interface (AMSI).

7.1.5.2.55. Capacidade de detecção de arquivos maliciosos executados em Subsistema Windows para Linux (WSL).

7.1.5.2.56. Deve possuir módulo que monitora e bloqueia atividades potencialmente maliciosas, baseado no comportamento do usuário e Machine Learning.

7.1.5.2.56.1. O módulo deve ser capaz de agir nos seguintes estados:

7.1.5.2.56.2. Aprendizado: coleta informações sobre as atividades executadas pelo usuário.

7.1.5.2.56.3. Bloqueio: bloqueia as atividades potencialmente maliciosas que não sejam compatíveis com a rotina do usuário.

7.1.5.2.56.4. Notificação: notifica sobre as atividades potencialmente maliciosas que não sejam compatíveis com a rotina do usuário.

7.1.6. **Estações Mac OS X**

7.1.6.1. **Compatibilidade:**

7.1.6.1.1. masOS High Sierra 10.13

7.1.6.1.2. macOS Sierra 10.12

7.1.6.1.3. Mac OS X 10.11 (El Capitan);

7.1.6.1.4. Mac OS X 10.10 (Yosemite);

7.1.6.1.5. Mac OS X 10.9 (Mavericks);

7.1.6.2. **Características:**

7.1.6.2.1. Deve prover proteção residente para arquivos (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;

7.1.6.2.2. Possuir módulo de web-antivírus para proteger contra ameaças durante navegação na internet com possíbilidade de analisar endereços https;

7.1.6.2.3. Possuir módulo de bloqueio á ataques na rede;

7.1.6.2.4. Possibilidade de bloquear a comunicação entre a máquina atacante e os demais computadores por tempo definido pelo administrador;

7.1.6.2.5. Capacidade de criar exclusões para computadores que não devem ser monitorados pelo módulo de bloqueio à ataques na rede;

7.1.6.2.6. Possibilidade de importar uma chave no pacote de instalação;

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

7.1.6.2.8. Deve possuir suportes a notificações utilizando o Growl;

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

7.1.6.2.10. Capacidade de voltar para a base de dados de vacina anterior;

7.1.6.2.11. Capacidade de varrer a quarentena automaticamente após cada atualização de vacinas;

7.1.6.2.12. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do

antivírus, (ex: “Win32.Trojan.banker”) para que qualquer objeto detectado com o veredicto escolhido seja ignorado;

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

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

7.1.6.2.15. Capacidade de verificar somente arquivos novos e alterados;

7.1.6.2.16. Capacidade de verificar objetos usando heurística;

7.1.6.2.17. Capacidade de agendar uma pausa na verificação;

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

7.1.6.2.18.1. Perguntar o que fazer, ou;

7.1.6.2.18.2. Bloquear acesso ao objeto;

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

7.1.6.2.18.4. Caso positivo de desinfecção:

7.1.6.2.18.4.1. Restaurar o objeto para uso;

7.1.6.2.18.5. Caso negativo de desinfecção:

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

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

7.1.6.2.20. Capacidade de verificar arquivos de formato de email;

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

7.1.6.2.22. Capacidade de ser instalado, removido e administrado pela

mesma console central de gerenciamento.

7.1.7. **Estações de trabalho Linux**

7.1.7.1. **Compatibilidade:**

7.1.7.1.1. **Plataforma 32-bits:**

7.1.7.1.1.1. Ubuntu 14.04.5 LTS

7.1.7.1.1.2. Ubuntu 16.04.4 LTS

7.1.7.1.1.3. Ubuntu 17.10.1

7.1.7.1.1.4. Red Hat® Enterprise Linux® 6.9

7.1.7.1.1.5. CentOS-6.9

7.1.7.1.1.6. Debian GNU/Linux 8.10

7.1.7.1.1.7. Debian GNU/Linux 9.4

7.1.7.1.1.8. AltLinux 8.0.0

7.1.7.1.1.9. AltLinux 8.2*

7.1.7.1.1.10. GosLinux 6.6

7.1.7.1.2. **Plataforma 64-bits:**

7.1.7.1.2.1. Ubuntu 14.04.5 LTS

7.1.7.1.2.2. Ubuntu 16.04.4 LTS

7.1.7.1.2.3. Ubuntu 17.10.1

7.1.7.1.2.4. Ubuntu 18.04

7.1.7.1.2.5. Red Hat® Enterprise Linux® 6.9

7.1.7.1.2.6. Red Hat® Enterprise Linux® 7.4

7.1.7.1.2.7. CentOS-6.9

7.1.7.1.2.8. CentOS-7.4

7.1.7.1.2.9. Debian GNU/Linux 8.10

7.1.7.1.2.10. Debian GNU/Linux 9.4

7.1.7.1.2.11. OracleLinux 7.4

7.1.7.1.2.12. SUSE® Linux Enterprise Server 12 SP3

7.1.7.1.2.13. openSUSE® 42.3

7.1.7.1.2.14. AltLinux 8.0.0

7.1.7.1.2.15. AltLinux 8.2*

7.1.7.1.2.16. GosLinux 6.6

7.1.7.1.2.17. EMIAS 1.0

7.1.7.2. **Características:**

7.1.7.2.1. Deve prover as seguintes proteções:

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

7.1.7.2.3. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;

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

7.1.7.2.5. Capacidade de criar exclusões por local, máscara e nome da ameaça;

7.1.7.2.6. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);

7.1.7.2.7. 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;

7.1.7.2.8. Detectar aplicações que possam ser utilizadas como vetor de ataque por hackers;

7.1.7.2.9. Fazer detecções através de heurística utilizando no mínimo as seguintes opções de nível:

7.1.7.2.9.1. Alta;

7.1.7.2.9.2. Média;

7.1.7.2.9.3. Baixa;

7.1.7.2.9.4. Recomendado;

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

7.1.7.2.11. Verificação por agendamento: procura de arquivos infectados e

suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados.

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

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

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

7.1.7.2.15. Capacidade de verificar objetos usando heurística;

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

7.1.7.2.17. Possibilidade de

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

7.1.7.3. **Servidores Windows**

7.1.7.3.1. **Compatibilidade:**

7.1.7.3.1.1. **Plataforma 32-bits:**

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

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

7.1.7.3.1.1.3. Windows Server 2003 Standard / Enterprise / Datacenter SP2 e posterior;

7.1.7.3.1.1.4. Windows Server 2003 R2 Standard / Enterprise / Datacenter SP2 e posterior;

7.1.7.3.1.2. **Plataforma 64-bits**

7.1.7.3.1.2.1. Microsoft Windows Server 2003 Standard / Enterprise / Datacenter SP2 ou posterior;

7.1.7.3.1.2.2. Microsoft Windows Server 2003 R2 Standard / Enterprise / Datacenter SP2 ou posterior;

7.1.7.3.1.2.3.

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

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

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

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

7.1.7.3.1.2.8. Microsoft Windows Storage Server 2008 R2;

7.1.7.3.1.2.9. Microsoft Windows Storage Server 2008 SP2 Standard Edition;

7.1.7.3.1.2.10. Microsoft Windows Storage Server SP2 Workgroup Edition;

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

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

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

7.1.7.3.1.2.14. Microsoft Windows Server 2012 Core Essentials / Standard / Foundation / Datacenter;

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

7.1.7.3.1.2.16. Microsoft Windows Storage Server 2012 (Todas edições);

7.1.7.3.1.2.17. Microsoft Windows Storage Server 2012 R2

(Todas edições);

7.1.7.3.1.2.18. Microsoft Windows Hyper-V Server 2012;

7.1.7.3.1.2.19. Microsoft Windows Hyper-V Server 2012 R2;

7.1.7.3.1.2.20. Windows Server 2016 Essentials/Standard/Datacenter/MultiPoint Premium Server;

7.1.7.3.1.2.21. Windows Server 2016 Core Standard / Datacenter;

7.1.7.3.1.2.22. Windows Storage Server 2016;

7.1.7.3.1.2.23. Windows Hyper-V Server 2016.

7.1.7.3.2. **Características:**

7.1.7.3.2.1. Deve prover as seguintes proteções:

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

7.1.7.3.2.1.2. Auto-proteção contra-ataques aos serviços/processos do antivírus;

7.1.7.3.2.1.3. Firewall com IDS;

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

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

7.1.7.3.2.3. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;

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

7.1.7.3.2.4.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);

7.1.7.3.2.4.2. Gerenciamento de tarefa (criar ou excluir tarefas de

verificação);

7.1.7.3.2.4.3. Leitura de configurações;

7.1.7.3.2.4.4. Modificação de configurações;

7.1.7.3.2.4.5. Gerenciamento de Backup e Quarentena;

7.1.7.3.2.4.6. Visualização de relatórios;

7.1.7.3.2.4.7. Gerenciamento de relatórios;

7.1.7.3.2.4.8. Gerenciamento de chaves de licença;

7.1.7.3.2.4.9. Gerenciamento de permissões (adicionar/excluir permissões acima);

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

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

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

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

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

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

7.1.7.3.2.9. Capacidade de automaticamente pausar e não iniciar tarefas agendadas caso o servidor esteja rodando com fonte

ininterrupta de energia (uninterruptible Power supply – UPS);

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

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

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

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

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

7.1.7.3.2.15. 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;

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

7.1.7.3.2.17. 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;

7.1.7.3.2.18. Capacidade de verificar somente arquivos novos e alterados;

7.1.7.3.2.19. Capacidade de escolher qual tipo de objeto composto

será verificado (ex: arquivos comprimidos, arquivos auto descompressores, .PST, arquivos compactados por compactadores binários, etc.);

7.1.7.3.2.20. Capacidade de verificar objetos usando heurística;

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

7.1.7.3.2.22. Capacidade de agendar uma pausa na verificação;

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

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

7.1.7.3.2.24.1. Perguntar o que fazer, ou;

7.1.7.3.2.24.2. Bloquear acesso ao objeto;

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

7.1.7.3.2.24.4. Caso positivo de desinfecção:

7.1.7.3.2.24.5. Restaurar o objeto para uso;

7.1.7.3.2.24.6. Caso negativo de desinfecção:

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

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

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

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

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

7.1.7.3.2.29. Bloquear atividade de malware explorando

vulnerabilidades em softwares de terceiros

7.1.7.3.2.30. Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning).

7.1.7.3.2.31. Capacidade de bloquear a criptografia de arquivos em pastas compartilhadas, após a execução de um malware em um dispositivo que possua o mapeamento da pasta.

7.1.7.4. **Servidores Linux**

7.1.7.4.1. **Compatibilidade:**

7.1.7.4.1.1. **Plataforma 32-bits:**

7.1.7.4.1.1.1. Red Hat® Enterprise Linux® 6.9 Server

7.1.7.4.1.1.2. CentOS-6.9

7.1.7.4.1.1.3. Ubuntu 14.04.5 LTS

7.1.7.4.1.1.4. Ubuntu 16.04.2 LTS

7.1.7.4.1.1.5. Ubuntu 17.10.1

7.1.7.4.1.1.6. Debian GNU / Linux 8.10

7.1.7.4.1.1.7. Debian GNU / Linux 9.4

7.1.7.4.1.1.8. AltLinux 8.0.0

7.1.7.4.1.1.9. AltLinux 8.2

7.1.7.4.1.2. **Plataforma 64-bits:**

7.1.7.4.1.2.1. Red Hat® Enterprise Linux® 6.9 Server

7.1.7.4.1.2.2. Red Hat® Enterprise Linux® 7.4 Server

7.1.7.4.1.2.3. Red Hat® Enterprise Linux® 7.5 Server

7.1.7.4.1.2.4. CentOS-6.9

7.1.7.4.1.2.5. CentOS-7.4

7.1.7.4.1.2.6. CentOS-7.5

7.1.7.4.1.2.7. Ubuntu 14.04.5 LTS

7.1.7.4.1.2.8. Ubuntu 16.04.4 LTS

7.1.7.4.1.2.9. Ubuntu 17.10.1

7.1.7.4.1.2.10. Ubuntu 18.04

7.1.7.4.1.2.11. Debian GNU / Linux 8.10

7.1.7.4.1.2.12. Debian GNU / Linux 9.4

7.1.7.4.1.2.13. SUSE® Linux Enterprise Server 12 SP3

7.1.7.4.1.2.14. Oracle Linux 7.4

7.1.7.4.1.2.15. SUSE® Linux Enterprise Server 12 SP2

7.1.7.4.1.2.16. OpenSUSE® 42.3

7.1.7.4.1.2.17. AltLinux 8.0.0

7.1.7.4.1.2.18. AltLinux 8.2

7.1.7.4.1.2.19. EMIAS 1.0

7.1.7.4.1.2.20. Amazon Linux AMI

7.1.7.4.2. **Características:**

7.1.7.4.3. Deve prover as seguintes proteções:

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

7.1.7.4.3.2. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;

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

7.1.7.4.4.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);

7.1.7.4.4.2. 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;

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

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

objetos infectados;

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

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

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

7.1.7.4.8. Capacidade de verificar objetos usando heurística;

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

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

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

7.1.7.5. **Criptografia**

7.1.7.5.1. **Compatibilidade**

7.1.7.5.1.1. Microsoft Windows 7 Ultimate SP1 ou superior x86/x64;

7.1.7.5.1.2. Microsoft Windows 7 Enterprise SP1 ou superior x86/x64;

7.1.7.5.1.3. Microsoft Windows 7 Professional SP1 ou superior x86/x64;

7.1.7.5.1.4. Microsoft Windows 8 Enterprise x86/x64;

7.1.7.5.1.5. Microsoft Windows 8 Pro x86/x64;

7.1.7.5.1.6. Microsoft Windows 8.1 Pro x86/x64;

7.1.7.5.1.7. Microsoft Windows 8.1 Enterprise x86/x64;

7.1.7.5.1.8. Microsoft Windows 10 Enterprise x86/x64;

7.1.7.5.1.9. Microsoft Windows 10 Pro x86/x64;

7.1.7.5.1.10. Microsoft Windows Vista x86/x64 SP2 ou superior;

7.1.7.5.1.11. Microsoft Windows XP Professional x86 SP3 ou superior

7.1.7.5.2. **Características**

7.1.7.5.2.1. O acesso ao recurso criptografado (arquivo, pasta ou disco) deve ser garantido mesmo em caso o usuário tenha esquecido a senha, através de procedimentos de recuperação;

7.1.7.5.2.2. Utilizar, no mínimo, algoritmo AES com chave de 256 bits;

7.1.7.5.2.3. Capacidade de criptografar completamente o disco rígido da máquina, adicionando um ambiente de pré-boot para autenticação do usuário;

7.1.7.5.2.4. Capacidade de utilizar Single Sign-On para a autenticação de pré-boot;

7.1.7.5.2.5. Permitir criar vários usuários de autenticação pré-boot;

7.1.7.5.2.6. Capacidade de criar um usuário de autenticação pré-boot comum com uma senha igual para todas as máquinas a partir da console de gerenciamento;

7.1.7.5.2.7. Capacidade de criptografar drives removíveis de acordo com regra criada pelo administrador, com as opções:

7.1.7.5.2.7.1. Criptografar somente os arquivos novos que forem copiados para o disco removível, sem modificar os arquivos já existentes;

7.1.7.5.2.7.2. Criptografar todos os arquivos individualmente;

7.1.7.5.2.7.3. Criptografar o dispositivo inteiro, de maneira que não seja possível listar os arquivos e pastas armazenadas;

7.1.7.5.2.7.4. Criptografar o dispositivo em modo portátil, permitindo acessar os arquivos em máquinas de terceiros através de uma senha;

7.1.7.5.2.8. Capacidade de selecionar pastas e arquivos (por tipo, ou extensão) para serem criptografados automaticamente. Nesta modalidade, os arquivos devem estar acessíveis para todas as máquinas gerenciadas pela mesma console de

maneira transparente para os usuários;

7.1.7.5.2.9. Capacidade de criar regras de exclusões para que certos arquivos ou pastas nunca sejam criptografados;

7.1.7.5.2.10. Capacidade de selecionar aplicações que podem ou não ter acesso aos arquivos criptografados;

7.1.7.5.2.11. Verifica compatibilidade de hardware antes de aplicar a criptografia;

7.1.7.5.2.12. Possibilita estabelecer parâmetros para a senha de criptografia;

7.1.7.5.2.13. Bloqueia o reuso de senhas;

7.1.7.5.2.14. Bloqueia a senha após um número de tentativas pré-estabelecidas;

7.1.7.5.2.15. Capacidade de permitir o usuário solicitar permissão a determinado arquivo criptografado para o administrador mediante templates customizados;

7.1.7.5.2.16. Permite criar exclusões para não criptografar determinados “discos rígidos” através de uma busca por nome do computador ou nome do dispositivo

7.1.7.5.2.17. Permite criptografar as seguintes pastas pré-definidas: “meus documentos”, “Favoritos”, “Desktop”, “Arquivos temporários” e “Arquivos do outlook”;

7.1.7.5.2.18. Permite utilizar variáveis de ambiente para criptografar pastas customizadas;

7.1.7.5.2.19. Capacidade de criptografar arquivos por grupos de extensão, tais como: Documentos do office, Document, arquivos de audio, etc;

7.1.7.5.2.20. Permite criar um grupo de extensões de arquivos a serem criptografados;

7.1.7.5.2.21. Capacidade de criar regra de criptografia para arquivos gerados por aplicações;

7.1.7.5.2.22. Permite criptografia de dispositivos móveis mesmo

quando o endpoint não possuir comunicação com a console de gerenciamento.

7.1.7.5.2.23. Capacidade de deletar arquivos de forma segura após a criptografia;

7.1.7.5.2.24. Capacidade de criptografar somente o espaço em disco utilizado;

7.1.7.5.2.25. Deve ter a opção de criptografar arquivos criados a partir de aplicações selecionadas pelo administrador;

7.1.7.5.2.26. Capacidade de bloquear aplicações selecionadas pelo administrador de acessarem arquivos criptografados;

7.1.7.5.2.27. Deve permitir criptografar somente o espaço utilizado em dispositivos removíveis tais como pendrives, HD externo, etc;

7.1.7.5.2.28. Capacidade de criptografar discos utilizando a criptografia BitLocker da Microsoft;

7.1.7.5.2.29. Deve ter a opção de utilização de TPM para criptografia através do BitLocker;

7.1.7.5.2.30. Capacidade de fazer “Hardware encryption”;

7.1.7.6. **Gerenciamento de Sistemas**

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

7.1.7.6.2. Deve possibilitar a utilização de servidores PXE na rede para deploy de imagens;

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

7.1.7.6.4. 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;

7.1.7.6.5. Capacidade de gerenciar licenças de softwares de terceiros;

7.1.7.6.6. Capacidade de registrar mudanças de hardware nas máquinas gerenciadas;

7.1.7.6.7. 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;

7.1.7.6.8. Possibilita fazer distribuição de software de forma manual e agendada;

7.1.7.6.9. Suporta modo de instalação silenciosa;

7.1.7.6.10. Suporte a pacotes MSI, exe, bat, cmd e outros padrões de arquivos executáveis;

7.1.7.6.11. Possibilita fazer a distribuição através de agentes de atualização;

7.1.7.6.12. Utiliza tecnologia multicast para evitar tráfego na rede;

7.1.7.6.13. Possibilita criar um inventário centralizado de imagens;

7.1.7.6.14. Capacidade de atualizar o sistema operacional direto da imagem mantendo os dados do usuário;

7.1.7.6.15. Suporte a WakeOnLan para deploy de imagens;

7.1.7.6.16. Capacidade de atuar como servidor de atualização do Windows podendo fazer deploy de patches;

7.1.7.6.17. Suporta modo de teste, podendo atribuir alguns computadores para receberem as atualizações de forma automática para avaliação de alterações no comportamento;

7.1.7.6.18. Capacidade de gerar relatórios de vulnerabilidades e patches;

7.1.7.6.19. Possibilita criar exclusões para aplicação de patch por tipo de sistema operacional, Estação de trabalho e Servidor ou por grupo de administração;

7.1.7.6.20. Permite iniciar instalação de patch e correções de vulnerabilidades ao reiniciar ou desligar o computador;

7.1.7.6.21. Permite baixar atualizações para o computador sem efetuar a instalação

7.1.7.6.22. Permite o administrador instalar somente atualizações aprovadas, instalar todas as atualizações (exceto as bloqueadas) ou instalar todas as atualizações incluindo as bloqueadas;

7.1.7.6.23. Capacidade de instalar correções de vulnerabilidades de acordo com a severidade;

7.1.7.6.24. Permite selecionar produtos a serem atualizados pela console de gerenciamento;

7.1.7.6.25. Permite selecionar categorias de atualizações para serem baixadas e instaladas, tais como: atualizações de segurança, ferramentas, drivers, etc;

7.1.7.6.26. Capacidade de adicionar caminhos específicos para procura de vulnerabilidades e updates em arquivos;

7.1.7.6.27. Capacidade de instalar atualizações ou correções somente em computadores definidos, em grupos definidos ou em uma porcentagem de computadores conforme selecionado pelo administrador;

7.1.7.6.28. Capacidade de configurar o reinício do computador após a aplicação das atualizações e correções de vulnerabilidades;

7.1.7.6.29. Deve permitir selecionar o idioma das aplicações que serão atualizadas;

7.1.7.6.30. Permitir agendar o sincronismo entre a console de gerenciamento e os sites da Microsoft para baixar atualizações recentes;

7.1.7.7. **Detecção e Resposta**

7.1.7.7.1. **Compatibilidade**

7.1.7.7.1.1. Windows 7 SP1 Home / Professional / Enterprise 32-bit / 64-bit

7.1.7.7.1.2. Windows 8.1.1 Professional / Enterprise 32-bit / 64-bit

7.1.7.7.1.3. Windows 10 RS3 (version 1703) Home / Professional / Education / Enterprise 32-bit / 64-bit

7.1.7.7.1.4. Windows 10 RS4 (version 1803) Home / Professional /

Education / Enterprise 32-bit / 64-bit

7.1.7.7.1.5. Windows 10 RS5 (version 1809) Home / Professional / Education / Enterprise 32-bit / 64-bit

7.1.7.7.1.6. Windows 10 RS6 (version 1903) Home / Professional / Education / Enterprise 32-bit / 64-bit

7.1.7.7.1.7. Windows 10 19H2 (version 1909) Home / Professional / Education / Enterprise 32-bit / 64-bit

7.1.7.7.1.8. Windows 10 20H1 (version 2004) Home / Professional / Education / Enterprise 32-bit / 64-bit

7.1.7.7.1.9. Windows Server 2008 R2 Foundation / Standard / Enterprise 64-bit

7.1.7.7.1.10. Windows Server 2012 Foundation / Standard / Enterprise 64-bit

7.1.7.7.1.11. Windows Server 2012 R2 Foundation / Standard / Enterprise 64-bit

7.1.7.7.1.12. Windows Server 2016 Essentials / Standard / Datacenter 64-bit

7.1.7.7.1.13. Windows Server 2019 Essentials / Standard / Datacenter 64-bit

7.1.7.7.2. **Características**

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

7.1.7.7.2.2. A solução deve oferecer módulo focado em capacidades de EDR “Endpoint Detection and Response”, incluindo no mínimo as seguintes capacidades:

7.1.7.7.2.3. O agente deve ter capacidade de coletar e processar dados relacionadas ao veredito e ao contexto da ameaça;

7.1.7.7.2.4. Deve fornecer graficamente a visualização da cadeia do ataque;

7.1.7.7.2.5. 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).

7.1.7.7.2.6. 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:

7.1.7.7.2.6.1. Isolar o host;

7.1.7.7.2.6.2. Iniciar uma varredura nas áreas críticas;

7.1.7.7.2.6.3. Quarentenar o objeto;

7.1.7.7.2.7. Capacidade de integração com a solução de sandbox;

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

7.1.7.7.2.8.1. Detecções provenientes da solução de endpoint;

7.1.7.7.2.8.2. Detecções provenientes da solução de sandbox;

7.1.7.7.2.8.3. Processos;

7.1.7.7.2.8.4. Alterações de registro;

7.1.7.7.2.8.5. DLL’s

7.1.7.7.2.8.6. Conexões remotas;

7.1.7.7.2.8.7. Criação de arquivos;

7.1.7.7.2.9. Varredura por todos os dispositivos executada a partir de indicador de comprometimento (IoC) gerado através da solução e importado pelo administrador.

7.1.7.7.2.10. Possibilidade de exportar os indicadores de comprometimento (IoC) gerados a partir da solução.

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

7.1.7.7.2.11.1. Prevenir a execução de um arquivo;

7.1.7.7.2.11.2. Quarentenar um arquivo;

7.1.7.7.2.11.3. Iniciar uma varredura por IoC;

7.1.7.7.2.11.4. Parar um processo;

7.1.7.7.2.11.5. Executar um processo;

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

7.1.7.7.2.12.1. A opção de isolamento deve estar disponível junto a visualização do incidente;

7.1.7.7.2.12.2. Na configuração padrão, o isolamento deve ser feito de forma granular, permitindo o controle do dispositivo pela console administrativa mesmo após ativação da regra;

7.1.7.7.2.13. A visualização da cadeia de ataque deve conter informações setorizadas por módulos do incidente.

7.1.7.7.2.14. Deve possuir as seguintes opções de gerenciamento:

7.1.7.7.2.14.1. Via console administrativa;

7.1.7.7.2.14.2. Via interface web;

7.1.7.7.2.14.3. Gerenciamento baseado em nuvem;

7.1.7.7.2.14.4. Gerenciamento via linha de comando.

7.1.7.7.2.15. Deve fornecer a opção de proteger a aplicação por senha.

7.1.7.7.2.16. A opção de proteção por senha deve permitir especificar uma força mínima para a senha da aplicação.

7.2. **Solução de Proteção Avançada para Ambientes Virtuais com validade de 36 meses – ITEM 2,** a qual deverá atender aos requisitos técnicos enumerados a seguir:

7.2.1. **Requerimentos Gerais**

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

7.2.1.1.1. Software antivírus sem agente para ambientes virtuais;

7.2.1.1.2. Software antivírus baseado em agente para ambientes virtuais;

7.2.1.1.3. Gerenciamento, monitoramento e atualização de software e vacinas centralizados;

7.2.1.1.4. Capacidade de atualizar definições de vírus e padrões de ataques;

7.2.1.1.5. Documentação do administrador;

7.2.1.1.6. Compatibilidade com a rede a ser protegida.

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

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

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

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

7.2.2.1. Para ser instalado em uma infraestrutura virtualizada, um dos seguintes hypervisors devem ser instalados:

7.2.2.1.1. Microsoft Windows Server 2019 Hyper-V

7.2.2.1.2. Microsoft Windows Server 2016 Hyper-V.

7.2.2.1.3. Microsoft Windows Server 2012 R2 Hyper-V

7.2.2.1.4. Citrix XenServer 7.1 LTSR.

7.2.2.1.5. VMware ESXi 7.0.

7.2.2.1.6. VMware ESXi 6.7.

7.2.2.1.7. VMware ESXi 6.5.

7.2.2.1.8. VMware ESXi 6.0.

7.2.2.1.9. KVM (Kernel-based Virtual Machine) com um dos seguintes sistemas operacionais:

7.2.2.1.9.1. Ubuntu Server 16.04 LTS.

7.2.2.1.9.2. Ubuntu Server 18.04 LTS.

7.2.2.1.9.3. Ubuntu Server 20.04 LTS

7.2.2.1.9.4. Red Hat Enterprise Linux Server 7.6.

7.2.2.1.9.5. CentOS 7.6.

7.2.2.1.10. Proxmox 5.4.

7.2.2.1.11. Proxmox 6.1.

7.2.2.1.12. Proxmox 6.2.

7.2.2.1.13. Skala-R Virtualization 7.0.8 hypervisor.

7.2.2.1.14. HUAWEI FusionCompute CNA 6.3.1 hypervisor.

7.2.2.1.15. Nutanix AHV 5.10 hypervisor.

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

7.2.2.2.1. Windows 7 Professional / Enterprise Service Pack 1 (32 / 64-bit)

7.2.2.2.2. Windows 8.1 Update 1 Professional / Enterprise (32 / 64-bit)

7.2.2.2.3. Windows 10 Desktop Pro / Enterprise / 2016 LTSC / RS4 / 2019 LTSC / 19H1 / 19H2 / 20H1 / 20H2 (32 / 64-bit);

7.2.2.2.4. Windows Server 2008 R2 Service Pack 1 Standard / Enterprise / Datacenter (Desktop experience / Core);

7.2.2.2.5. Windows Server 2012 Standard / Datacenter / Essentials;

7.2.2.2.6. Windows Server 2012 R2 (64-bit);

7.2.2.2.7. Windows Server 2016 (64-bit);

7.2.2.2.8. Windows Server 2019 (64-bit);

7.2.2.2.9. Debian GNU / Linux 8.11 (32 / 64-bit);

7.2.2.2.10. Debian GNU / Linux 9.8 (64-bit);

7.2.2.2.11. Ubuntu Server 16.04 LTS (64-bit);

7.2.2.2.12. Ubuntu Server 18.04 LTS (64-bit);

7.2.2.2.13. CentOS 6.10 (64-bit);

7.2.2.2.14. CentOS 7.7 (64-bit);

7.2.2.2.15. CentOS 8.1 (64-bit);

7.2.2.2.16. ALT Linux 8 (64-bit);

7.2.2.2.17. ALT Linux 7.0.6 (64-bit);

7.2.2.2.18. Red Hat Enterprise Linux Server 6.10 (64-bit);

7.2.2.2.19. Red Hat Enterprise Linux Server 7.7 (64-bit);

7.2.2.2.20. Red Hat Enterprise Linux Server 8.1 (64-bit);

7.2.2.2.21. SUSE Linux Enterprise Server 15 (64-bit);

7.2.2.2.22. Oracle Linux 7.6 (64-bit);

7.2.2.3. A Suite VMware tools deve ser instalada para prover integração entre

o Hypervisor, máquinas virtuais e o conector;

7.2.2.4. O antivírus baseado em agente deve prover as seguintes funcionalidades:

7.2.2.5. Antivírus e monitoramento residente;

7.2.2.6. Proteção contra rootkits e auto dialers a sites pagos;

7.2.2.7. Proteção de pastas compartilhadas contra criptografia externa;

7.2.2.8. Ao detectar criptografia externa, deve criar automaticamente um backup do arquivo;

7.2.2.9. Ao detectar criptografia externa, deve permitir o bloqueio automático da atividade de rede do computador de onde a criptografia veio, com possibilidade de predefinir o período de tempo pelo qual a atividade de rede permanecerá bloqueada;

7.2.2.10. Deve permitir substituir automaticamente os arquivos modificados pelos seus backups;

7.2.2.11. Verificação por heurística para detectar e bloquear malwares desconhecidos;

7.2.2.12. Capacidade de pausar varreduras automaticamente em horários predefinidos;

7.2.2.13. Transferir a verificação de malware e as tarefas intensivas para uma única máquina virtual responsável pela proteção;

7.2.2.14. 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 as alterações após a restauração do acesso;

7.2.2.15. 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;

7.2.2.16. Proteção de e-mail contra malwares verificando tráfego de entrada e saída nos protocolos IMAP, SMTP, POP3 e NNTP independente do cliente de e-mail;

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

7.2.2.18. Bloqueia páginas com banners e pop-ups potencialmente maliciosos na web;

7.2.2.19. Capacidade de detectar e bloquear sites de phishing;

7.2.2.20. Proteção contra ameaças não conhecidas baseadas no comportamento;

7.2.2.21. Capacidade de determinar comportamento anômalo de uma aplicação analisando a sequência de execução.

7.2.2.22. Capacidade de reverter operações de malware durante o tratamento do arquivo;

7.2.2.23. 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;

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

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

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

7.2.2.27. 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/ou categorias predefinidas de aplicações providenciadas pelo fabricante;

7.2.2.28. Deve permitir o bloqueio e a permissão da instalação e/ou execução de programas com base em usuários;

7.2.2.29. Deve ser capaz de, ao ser instalado, criar automaticamente regras de permissão para aplicativos das seguintes categorias:

7.2.2.29.1. Fornecedores confiáveis;

7.2.2.29.2. Componentes do sistema operacional;

7.2.2.29.3. Aplicações de virtualização;

7.2.2.30. Não carregar nenhum módulo de segurança na máquina virtual e sim no appliance virtual;

7.2.2.31. Permitir a verificação em máquinas Linux;

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

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

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

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

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

7.2.2.36.1. Utilizando Multicast;

7.2.2.36.2. Selecionando Servidor de integração;

7.2.2.36.3. Utilizando uma lista de appliances virtuais

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

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

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

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

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

7.2.2.41.1. Verificação automática;

7.2.2.41.2. Verificar os arquivos no acesso ou na modificação;

7.2.2.41.3. Somente no acesso;

7.2.2.42. 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;

7.2.2.43. Capacidade de garantir privilégios na utilização de dispositivos externos para usuários específicos;

7.2.2.44. 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 (áudio, vídeo, etc);

7.2.2.45. Capacidade de controlar acesso a recursos na internet por horário e por usuário;

7.2.2.46. Atualizações centralizadas permitindo que parte do banco de dados de definições seja armazenado na máquina de proteção (SVM);

7.2.2.47. Habilidade de executar tarefas de detecção de vulnerabilidades em aplicações instaladas nos computadores incluindo opção de submeter um relatório de qualquer vulnerabilidade encontrada;

7.2.2.48. Integração com o Windows Update para instalar patches de acordo com as vulnerabilidades encontradas;

7.2.2.49. Capacidade de instalar e distribuir remotamente componentes do antivírus em todas as máquinas protegidas sem utilização de ferramentas de terceiros;

7.2.2.50. Armazenar as informações de arquivos verificados para evitar um novo scan sobre o arquivo e aumentar consumo de recursos;

7.2.2.51. Bloquear, neutralizar e remover os malwares com a opção de notificar os administradores;

7.2.2.52. Console de gerenciamento única para todos os componentes de proteção;

7.2.2.53. Console de gerenciamento única tanto para ambientes físicos como virtuais;

7.2.2.54. Console única para administração de máquinas virtuais Linux e Windows

7.2.2.55. Provê informações detalhadas sobre os eventos e execução de tarefas;

7.2.2.56. Capacidade de aplicar configurações de segurança diferentes para cada grupo de máquinas virtuais;

7.2.2.57. Salvar o backup dos arquivos deletados;

7.2.2.58. Suporta as seguintes tecnologias Vmware: vMotion e/ou Distributed resource Scheduler;

7.2.2.59. Suporta as seguintes tecnologias Citrix: Virtual User Drive, Citrix Receiver, Multi-stream ICA, XenMotion Live Migration, Automated VM protection and recovery, Dynamic memory control;

7.2.2.60. Suporta as seguintes tecnologias Hyper-V: Live migration, Cluster shared volumes, Dynamic memory, Live backup;

7.2.2.61. Suportar rollback do banco de dados de definições;

7.2.2.62. Suportar o esquema de licença de acordo com o número de máquinas virtuais protegidas e de acordo com o número de hardware CPU cores

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

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

7.2.3.1.1. Microsoft Windows 7 Todas as edições (32/64 bits);

7.2.3.1.2. Microsoft Windows 8 Pro/Enterprise 32/64 bits;

7.2.3.1.3. Microsoft Windows 8.1 Pro/Enterprise 32/64 bits;

7.2.3.1.4. Microsoft Windows 10 Education RS3;

7.2.3.1.5. Microsoft Windows 10 Education RS4;

7.2.3.1.6. Microsoft Windows 10 Education RS5;

7.2.3.1.7. Microsoft Windows 10 Education 32/64-bit;

7.2.3.1.8. Microsoft Windows 10 Enterprise RS3/RS4/RS5 (32/64-bit);

7.2.3.1.9. Microsoft Windows 10 Professional RS3/RS4/RS5 (32/64-bit);

7.2.3.1.10. Microsoft Windows Small Business Server 2011 Essentials, Premium e Standard;

7.2.3.1.11. Microsoft Windows Server 2008 R2 Todas edições 32/64 bits;

7.2.3.1.12. Microsoft Windows Server 2012 Todas edições 32/64 bits;

7.2.3.1.13. Microsoft Windows Server 2012 R2 Todas edições 32/64 bits;

7.2.3.1.14. Microsoft Windows Server 2016 x64;

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

7.2.3.1.15.1. Microsoft SQL Server 2012 Express 64-bit;

7.2.3.1.15.2. Microsoft SQL Server 2014 Express 64-bit;

7.2.3.1.15.3. Microsoft SQL Server 2016 Express 64-bit;

7.2.3.1.15.4. Microsoft SQL Server 2017 Express 64-bit;

7.2.3.1.15.5. Microsoft SQL Server 2019 Express 64-bit;

7.2.3.1.15.6. Microsoft SQL Server 2014 (todas as edições) 64-bit;

7.2.3.1.15.7. Microsoft SQL Server 2016 (todas as edições) 64-bit;

7.2.3.1.15.8. Microsoft SQL Server 2017 (todas as edições) 64-bit;

7.2.3.1.15.9. Microsoft SQL Server 2019 (todas as edições) 64-bit;

7.2.3.1.15.10. MySQL Standard Edition 5.7 32-bit/64-bit;

7.2.3.1.15.11. MySQL Enterprise 5.7 32-bit/64-bit;

7.2.3.1.15.12. MariaDB Server 10.3 32-bit/64-bit;

7.2.4. **Requerimentos Console de administração instalada em ambientes virtualizados:**

7.2.4.1. Vmware Workstation 16 Pro;

7.2.4.2. Vmware Workstation 15 Pro;

7.2.4.3. Microsoft Hyper-V Server 2012 64-bit;

7.2.4.4. Microsoft Hyper-V Server 2012 R2 64-bit;

7.2.4.5. Microsoft Hyper-V Server 2016 64-bit;

7.2.4.6. Microsoft Hyper-V Server 2019 64-bit;

7.2.4.7. VMware vSphere 6.7;

7.2.4.8. VMware vSphere 7.1;

7.2.4.9. Citrix XenServer 8.x;

7.2.4.10. Citrix XenServer 7.1 LTSR;

7.2.4.11. Parallels Desktop 16;

7.2.4.12. Oracle VM VirtualBox 6.x;

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

7.2.5.1. Deve ser compatível com Microsoft SCVMM;

7.2.5.2. Capacidade de desativar a interface local do agente (conector) para diminuir uso de memória;

7.2.5.3. Instalação do antivírus a partir de uma única distribuição;

7.2.5.4. Seleção de instalação dependendo do número de pontos protegidos;

7.2.5.5. Capacidade de ler informações do AD para obter dados some as contas dos computadores na organização;

7.2.5.6. Capacidade de fazer a instalação automática através dos grupos gerenciados;

7.2.5.7. Capacidade de realocar computadores de acordo com endereço IP, tipo do sistema operacional e localização no AD;

7.2.5.8. Instalação centralizada;

7.2.5.9. Remoção centralizada (manual ou automática) de aplicações incompatíveis através do servidor de administração;

7.2.5.10. Capacidade de instalar o antivírus de diferentes formas: GPO, agente de administração;

7.2.5.11. Capacidade de atualizar pacotes de instalação com as últimas atualizações;

7.2.5.12. Atualizar de forma automática a versão do antivírus e as definições;

7.2.5.13. Procurar automaticamente por vulnerabilidades nas aplicações e sistemas operacionais presentes da rede;

7.2.5.14. Capacidade de proibir instalação/execução de aplicações;

7.2.5.15. Capacidade de gerenciar I/O de dispositivos externos;

7.2.5.16. Gerenciar a atividade do usuário na internet;

7.2.5.17. Capacidade de testar as atualizações antes de aplicar para o ambiente;

7.2.5.18. Capacidade de executar instalações automáticas baseado no sistema de proteção dedicado, tais como: Vmware ESXi, Microsoft Hyper-V, Citrix XenServer virtualization ou hypervisor;

7.2.5.19. Criar os usuários baseados em RBAC;

7.2.5.20. Criar a hierarquia dos servidores de administração e tem capacidade de gerenciar cada um deles através de uma única console de

gerenciamento;

7.2.5.21. Capacidade de criar servidores de administração lógicos, sem a necessidade de ter um servidor adicional para gerenciamento;

7.2.5.22. Distribuir automaticamente licenças nos computadores gerenciados;

7.2.5.23. Criar o inventário de software e hardware dos computadores gerenciados na rede;

7.2.5.24. Instalação centralizada de aplicações de terceiros;

7.2.5.25. Capacidade de eleger um computador na rede para ser responsável por atualizar outros computadores dentro da rede;

7.2.5.26. Capacidade de gerar relatórios gráficos;

7.2.5.27. Capacidade de exportar relatórios para PDF, XML e CSV;

7.2.5.28. Capacidade de criar contas internas para autenticar no console de administração;

7.2.5.29. Capacidade de criar backup de forma automática ou manual;

7.2.5.30. Suporta Windows Failover Clustering;

7.2.5.31. Console WEB para gerenciar a aplicação;

7.2.5.32. Sistema para controle de virus outbreak.

7.2.5.33. Capacidade de gerenciar permissões de administradores;

7.2.5.34. Capacidade de deletar atualizações já baixadas;

7.2.5.35. Capacidade de distribuir correções de vulnerabilidades em computadores clientes sem instalar atualizações;

7.2.5.36. Capacidade de eleger automaticamente um agente de atualização de acordo com uma análise de rede.

7.2.5.37. Capacidade de manter um histórico das alterações feitas nas ;

7.2.5.38. Permite comparar alterações feitas no console de administração;

7.2.5.39. Deve permitir o rollback de alterações feitas nas políticas através de uma única seleção, sem ter a necessidade de restaurar item por item alterado;

7.2.6. **Requerimentos Console de administração instalada em ambientes virtualizados:**

7.2.6.1. VMware Workstation 16 Pro

7.2.6.2. VMware Workstation 15 Pro

7.2.6.3. Microsoft Hyper-V Server 2012 64 bits

7.2.6.4. Microsoft Hyper-V Server 2012 R2 64 bits

7.2.6.5. Microsoft Hyper-V Server 2016 64 bits

7.2.6.6. Microsoft Hyper-V Server 2019 64 bits

7.2.6.7. Citrix XenServer 7.1 LTSR

7.2.6.8. Citrix XenServer 8.x

7.2.6.9. VMware vSphere 7.1

7.2.6.10. VMware vSphere 6.7

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

7.2.7.1. Deve ser compatível com Microsoft SCVMM;

7.2.7.2. Capacidade de desativar a interface local do agente (conector) para diminuir uso de memória;

7.2.7.3. Instalação do antivírus a partir de uma única distribuição;

7.2.7.4. Seleção de instalação dependendo do número de pontos protegidos;

7.2.7.5. Capacidade de ler informações do AD para obter dados some as contas dos computadores na organização;

7.2.7.6. Capacidade de fazer a instalação automática através dos grupos gerenciados;

7.2.7.7. Capacidade de realocar computadores de acordo com endereço IP, tipo do sistema operacional e localização no AD;

7.2.7.8. Instalação centralizada;

7.2.7.9. Remoção centralizada (manual ou automática) de aplicações incompatíveis através do servidor de administração;

7.2.7.10. Capacidade de instalar o antivírus através de GPO ou agente de administração;

7.2.7.11. Capacidade de atualizar pacotes de instalação com as últimas atualizações;

7.2.7.12. Atualizar de forma automática a versão do antivírus e as definições;

7.2.7.13. Procurar automaticamente por vulnerabilidades nas aplicações e

sistemas operacionais presentes da rede;

7.2.7.14. Capacidade de proibir instalação/execução de aplicações;

7.2.7.15. Capacidade de gerenciar I/O de dispositivos externos;

7.2.7.16. Gerenciar a atividade do usuário na internet;

7.2.7.17. Capacidade de testar as atualizações antes de aplicar para o ambiente;

7.2.7.18. Capacidade de executar instalações automáticas baseado no sistema de proteção dedicado, tais como: Vmware ESXi, Microsoft Hyper-V, Citrix XenServer virtualization ou hypervisor;

7.2.7.19. Criar os usuários baseados em RBAC;

7.2.7.20. Criar a hierarquia dos servidores de administração e tem capacidade de gerenciar cada um deles através de uma única console de gerenciamento;

7.2.7.21. Capacidade de criar servidores de administração lógicos, sem a necessidade de ter um servidor adicional para gerenciamento;

7.2.7.22. Distribuir automaticamente licenças nos computadores gerenciados;

7.2.7.23. Criar o inventário de software e hardware dos computadores gerenciados na rede;

7.2.7.24. Instalação centralizada de aplicações de terceiros;

7.2.7.25. Capacidade de eleger um computador na rede para ser responsável por atualizar outros computadores dentro da rede;

7.2.7.26. Capacidade de gerar relatórios gráficos;

7.2.7.27. Capacidade de exportar relatórios para PDF, XML e CSV;

7.2.7.28. Capacidade de criar contas internas para autenticar no console de administração;

7.2.7.29. Capacidade de criar backup de forma automática ou manual;

7.2.7.30. Suporta Windows Failover Clustering;

7.2.7.31. Console WEB para gerenciar a aplicação;

7.2.7.32. Sistema para controle de vírus outbreak.

7.2.7.33. Capacidade de gerenciar permissões de administradores;

7.2.7.34. Capacidade de deletar atualizações já baixadas;

7.2.7.35. Capacidade de distribuir correções de vulnerabilidades em computadores clientes sem instalar atualizações;

7.2.7.36. Capacidade de eleger um agente de atualização de acordo com uma análise de rede.

7.2.7.37. Capacidade de manter um histórico das alterações feitas nas políticas tanto de Linux como Windows;

7.2.7.38. Permite comparar alterações feitas no console de administração;

7.2.7.39. Deve permitir o rollback de alterações feitas nas políticas através de uma única seleção, sem ter a necessidade de restaurar item por item alterado;

7.3. **Solução de Proteção para Mobile com validade de 36 meses – ITEM 3,** a qual deverá atender aos requisitos técnicos enumerados a seguir:

7.3.1. **Smartphones e tablets**

7.3.1.1. **Compatibilidade:**

7.3.1.1.1. Dispositivos com os sistemas operacionais:

7.3.1.1.1.1. Android 5.0 – 5.1.1

7.3.1.1.1.2. Android 6.0 – 6.0.1

7.3.1.1.1.3. Android 7.0 – 7.12

7.3.1.1.1.4. Android 8.0 – 8.1

7.3.1.1.1.5. Android 9.0

7.3.1.1.1.6. Android 10.0

7.3.1.2. **Características:**

7.3.1.2.1. Deve prover as seguintes proteções:

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

7.3.1.2.1.2. Proteção contra adware e autodialers;

7.3.1.2.1.3. Todos os objetos transmitidos usando conexões wireless (porta de infravermelho, Bluetooth) e mensagens EMS, durante sincronismo com PC e ao realizar download usando o browser;

7.3.1.2.1.4. Arquivos abertos no smartphone;

7.3.1.2.1.5. Programas instalados usando a interface do smartphone

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

7.3.1.2.1.7. Deverá isolar em área de quarentena os arquivos infectados;

7.3.1.2.1.8. Deverá atualizar as bases de vacinas de modo agendado;

7.3.1.2.1.9. Capacidade de desativar por política:

7.3.1.2.1.9.1. Wi-fi;

7.3.1.2.1.9.2. Câmera;

7.3.1.2.1.9.3. Bluetooth.

7.3.1.2.1.10. Deverá ter função de limpeza de dados pessoais a distância, em caso de roubo, por exemplo;

7.3.1.2.1.11. Capacidade de requerer uma senha para desbloquear o dispositivo e personalizar a quantidade de caracteres para esta senha;

7.3.1.2.1.12. Deverá ter firewall pessoal (Android);

7.3.1.2.1.13. Capacidade de tirar fotos quando a senha for inserida incorretamente;

7.3.1.2.1.14. Capacidade de enviar comandos remotamente de:

7.3.1.2.1.14.1. Localizar;

7.3.1.2.1.14.2. Bloquear.

7.3.1.2.1.15. Capacidade de detectar Root em dispositivos Android;

7.3.1.2.1.16. Capacidade de bloquear o acesso a site por categoria em dispositivos;

7.3.1.2.1.17. Capacidade de bloquear o acesso a sites phishing ou maliciosos;

7.3.1.2.1.18. Capacidade de configurar White e blacklist de aplicativos;

7.3.1.2.1.19. Capacidade de localizar o dispositivo quando

necessário;

7.3.1.2.1.20. Permitir atualização das definições quando estiver em “roaming”;

7.3.1.2.1.21. Capacidade de selecionar endereço do servidor para buscar a definição de vírus;

7.3.1.2.1.22. Capacidade de agendar uma verificação (Android);

7.3.1.2.1.23. Capacidade de enviar URL de instalação por e-mail;

7.3.1.2.1.24. Capacidade de fazer a instalação através de um link QRCode;

7.3.1.2.1.25. Capacidade de executar as seguintes ações caso a desinfecção falhe (Android):

7.3.1.2.1.25.1. Deletar;

7.3.1.2.1.25.2. Ignorar;

7.3.1.2.1.25.3. Quarentenar;

7.3.1.2.1.25.4. Perguntar ao usuário.

7.3.1.3. **Gerenciamento de dispositivos móveis (MDM) - Android**

7.3.1.3.1. **Compatibilidade:**

7.3.1.3.1.1. Dispositivos com os sistemas operacionais:

7.3.1.3.1.1.1. Android 5.0 – 5.1.1

7.3.1.3.1.1.2. Android 6.0 – 6.0.1

7.3.1.3.1.1.3. Android 7.0 – 7.12

7.3.1.3.1.1.4. Android 8.0 – 8.1

7.3.1.3.1.1.5. Android 9.0

7.3.1.3.1.1.6. Android 10.0

7.3.1.3.1.2. Softwares de gerência de dispositivos:

7.3.1.3.1.2.1. VMWare AirWatch 9.3;

7.3.1.3.1.2.2. MobileIron 10.0;

7.3.1.3.1.2.3. IBM Maas360 10.68;

7.3.1.3.1.2.4. Microsoft Intune 1908;

7.3.1.3.1.2.5. SOTI MobiControl 14.1.4 (1693);

7.3.1.3.2. **Características:**

7.3.1.3.2.1. Capacidade de aplicar políticas de ActiveSync através do servidor Microsoft Exchange;

7.3.1.3.2.2. Capacidade de ajustar as configurações de:

7.3.1.3.2.2.1. Sincronização de e-mail;

7.3.1.3.2.2.2. Uso de aplicativos;

7.3.1.3.2.2.3. Senha do usuário;

7.3.1.3.2.2.4. Criptografia de dados;

7.3.1.3.2.2.5. Conexão de mídia removível.

7.3.1.3.2.3. Capacidade de instalar certificados digitais em dispositivos móveis;

7.3.1.3.2.4. Deve permitir configurar horário para sincronização do dispositivo com a console de gerenciamento;

7.3.1.3.2.5. Capacidade de desinstalar remotamente o antivírus do dispositivo;

7.3.1.3.2.6. Deve permitir fazer o upgrade do antivírus de forma remota sem a necessidade de desinstalar a versão atual;

7.3.1.3.2.7. Capacidade de sincronizar com Samsung Knox;

7.3.1.4. **Gerenciamento de dispositivos móveis (MDM) – iOS**

7.3.1.4.1. **Compatibilidade:**

7.3.1.4.1.1. Dispositivos com os sistemas operacionais:

7.3.1.4.1.1.1. iOS 10.0 – 10.3.3

7.3.1.4.1.1.2. iOS 11.0 – 11.3

7.3.1.4.1.1.3. iOS 12.0

7.3.1.4.1.1.4. iOS 13.0

7.3.1.4.2. **Características:**

7.3.1.4.2.1. Capacidade de aplicar políticas de ActiveSync através do servidor Microsoft Exchange;

7.3.1.4.2.2. Capacidade de ajustar as configurações de:

7.3.1.4.2.2.1. Sincronização de e-mail;

7.3.1.4.2.2.2. Senha do usuário;

7.3.1.4.2.2.3. Criptografia de dados;

7.3.1.4.2.3. Capacidade de instalar certificados digitais em dispositivos móveis;

7.3.1.4.2.4. Capacidade de instalar as ferramentas necessárias para o gerenciamento dos dispositivos clientes através de:

7.3.1.4.2.4.1. Link por e-mail;

7.3.1.4.2.4.2. Link por mensagem de texto;

7.3.1.4.2.4.3. QR Code

7.3.1.4.2.5. Capacidade de, remotamente, apagar todos os dados de dispositivos iOS;

7.3.1.4.2.6. Capacidade de, remotamente, bloquear um dispositivo iOS;

7.4. **Solução de descoberta avançada de ameaças em nível de rede com validade de 36 meses – ITEM 4,** o qual deverá atender aos requisitos técnicos enumerados a seguir:

7.4.1. **Servidor de Administração e Console Administrativa**

7.4.1.1. **Das capacidades da console de gerenciamento**

7.4.1.1.1. A Console de gerenciamento deve apresentar uma dashboard customizável;

7.4.1.1.2. Deve apresentar a saúde do sistema, informando quais componentes estão atualizados ou não;

7.4.1.1.3. Deve mostrar em tempo real o tráfego sendo processado pelos sensores;

7.4.1.1.4. Deve apresentar em tempo real gráfico de pacotes descartados caso não suporte o tráfego gerado;

7.4.1.1.5. Deve permitir criar perfis de layout;

7.4.1.1.6. Deve permitir exportar para PDF o layout atual da solução;

7.4.1.1.7. Deve mostrar pelo menos as seguintes informações atualizadas sobre a ferramenta:

7.4.1.1.7.1. Saúde do sistema;

7.4.1.1.7.2. Tráfego em tempo real;

7.4.1.1.7.3. Top 10 domínios mais acessados;

7.4.1.1.7.4. Mostrar alertas por importância;

7.4.1.1.7.5. Top 10 Ips mais acessados;

7.4.1.1.7.6. Alertas por tecnologias de detecção;

7.4.1.1.7.7. Alertas por vetor de ataques;

7.4.1.1.8. Deve permitir criar novos usuários para acesso à console com

pelo menos 3 níveis de acesso;

7.4.1.1.9. Deve permitir integração com a Console de gerenciamento da ferramenta de antivírus caso seja necessário a implementação de EDR;

7.4.1.1.10. Os alertas deverão ser exibidos permitindo visualizar quantos são novos, quantos estão em processo e quantos já foram processados;

7.4.1.1.11. Deve mostrar quantidades de eventos pela criticidade, alto, médio ou baixo;

7.4.1.1.12. Deve permitir exportar os alertas para o formato (.txt);

7.4.1.1.13. Possibilidade de assinalar um evento para determinado usuário para verificação;

7.4.1.1.14. Deve suportar arquivos no formato CEF para integração com SIEM;

7.4.1.1.15. O usuário com conta administrativa deve ter permissão para assinalar um incidente para usuários específicos;

7.4.1.1.16. Possibilidade de marcar evento como processado para informar que o incidente já foi analisado e resolvido;

7.4.1.1.17. Deve se possível gerenciar o status de cada evento;

7.4.1.1.18. As seguintes informações devem ser mostradas nos alertas de eventos:

7.4.1.1.18.1. Host onde ocorreu o incidente;

7.4.1.1.18.2. Origem do ataque;

7.4.1.1.18.3. Destino do ataque;

7.4.1.1.18.4. Dia e horário de quanto ocorreu o ataque;

7.4.1.1.18.5. Nome do objeto considerado malicioso;

7.4.1.1.18.6. Tamanho do objeto;

7.4.1.1.18.7. Hash do objeto em pelo menos MD5 e SHA256;

7.4.1.1.18.8. URL do ataque;

7.4.1.1.18.9. Nome da tecnologia responsável por identificar o ataque;

7.4.1.1.18.10. Informar se o ataque possui caracteristicas baseado no YARA (Ferramenta open source);

7.4.1.1.19. A console de gerenciamento deverá permitir que o administrador procure por eventos similares na rede baseado no tipo de arquivo, no hash do arquivo, tipo de evento e nome do arquivo;

7.4.1.1.20. Deve permitir a instalação do sensor de endpoint de forma remota;

7.4.1.1.21. Possibilidade de mostrar a sequência de atividades executadas pelo malware quando executada no sandbox;

7.4.1.1.22. Deve permitir fazer uma busca no sistema por eventos baseados em regras;

7.4.1.1.23. Deve permitir fazer buscas de IoCs no banco de dados através de informações recebidas pelos agentes;

7.4.1.1.24. Deve permitir buscar no sistema eventos baseados nas seguintes categorias:

7.4.1.1.24.1. Texto completo;

7.4.1.1.24.2. Por host;

7.4.1.1.24.3. Por tipo de vento;

7.4.1.1.24.4. Por arquivos;

7.4.1.1.24.5. Pelo hash MD5 e SHA256;

7.4.1.1.24.6. Pela conexão de rede;

7.4.1.1.24.7. Chave de registro;

7.4.1.1.24.8. Eventos do windows;

7.4.1.1.24.9. Alteração de nome do host;

7.4.1.1.25. Deve permitir importar IOCs (Indices de comprometimento) visando encontrar ataques de acordo com informações contidas no IoC;

7.4.1.1.26. Capacidade de executar as seguintes tarefas remotamente nos endpoints que possuem o EDR (Endpoint Detection Response) instalado:

7.4.1.1.26.1. Finalizar processo;

7.4.1.1.26.2. Executar programa;

7.4.1.1.26.3. Coletar arquivo;

7.4.1.1.26.4. Deletar arquivo;

7.4.1.1.26.5. Quarentenar arquivo;

7.4.1.1.26.6. Restaurar arquivo da quarentena;

7.4.1.1.27. Deve permitir ao coletar um arquivo remotamente enviar automaticamente para o SANDBOX para análise;

7.4.1.1.28. Deve possuir funcionalidade que permita prevenir um arquivo de ser executado em qualquer host com o EDR instalado através do hash MD5/SHA256;

7.4.1.1.29. Deverá possuir capacidade de disponibilizar facilmente as amostras dos arquivos suspeitos detectados e do arquivo PCAP do contexto de captura;

7.4.1.1.30. Deverá permitir o uso de base de conhecimento na Internet do próprio fabricante, com atualização automática de regras e assinaturas, para consultas automáticas em bases de reputação e correlacionamento de informações sobre ameaças conhecidas, identificando assim as respectivas recomendações de ações;

7.4.1.1.31. Deve possuir plataforma de inteligência de ameaças, informando se o ataque faz parte de uma campanha global, quais as regiões e plataformas afetadas pelo ataque, bem como disponibilizar links de referência sobre a ameaça;

7.4.1.1.32. Deve possuir plataforma do próprio fabricante com informações sobre as ameaças, informando título, data descoberta e descrição sobra a ameaça.

7.4.1.1.33. Deve possuir integração com portal de inteligência para avançar na pesquisa a partir dos eventos;

7.4.1.1.34. Deve ser possível realizar consultas de IP, HASH domínios no portal de inteligência do próprio fabricante.

7.4.1.1.35. Para cada malware, exploit ou componente malicioso, a ferramenta deve possuir links para detalhar informações sobre estes;

7.4.1.1.36. Possibilidade de selecionar quais dispositivos serão afetados pela tarefa de prevenção de execução de arquivos;

7.4.1.1.37. Capacidade de baixar arquivos quarentenados diretamente pela console de administração do antiapt;

7.4.1.1.38. Capacidade de visualizar quantos endpoints possuem o EDR instalado através de integração com a Console de gerenciamento do antivírus;

7.4.1.1.39. Deve mostrar quantos Endpoints estão sendo gerenciados informando também quantos não possuem EDR instalado;

7.4.1.1.40. Possuir relatórios customizáveis possibilitando adicionar ou remover colunas de identificação e status de ventos;

7.4.1.1.41. Deve permitir criar relatórios baseados na tecnologia de proteção utilizada;

7.4.1.1.42. Criar relatórios de eventos organizados pelas seguintes severidades: baixa, média e alta;

7.4.1.1.43. Deve permitir adicionar imagens ao relatório;

7.4.1.1.44. Permitir criar listas brancas baseadas nos seguintes filtros:

7.4.1.1.44.1. Por hash MD5;

7.4.1.1.44.2. Por formato;

7.4.1.1.44.3. Por URL;

7.4.1.1.44.4. Por e-mail;

7.4.1.1.44.5. Por subrede;

7.4.1.1.45. Permitir criar regras de notificações para envio por e-mail quando novos eventos são identificados pela ferramenta;

7.4.1.1.46. Deve permitir configurar o status do endpoint de acordo com a quantidade de dias de inatividade;

7.4.1.1.47. Deve permitir integrar a solução com pelo menos as seguintes

ferramentas de SIEM: ArchSight, Splunk e IBM Qradar;

7.4.2. **Características para o Sandbox**

7.4.2.1. As Sandboxes deverão suportar os seguintes sistemas operacionais:

7.4.2.1.1. Windows XP x86 Sp3;

7.4.2.1.2. Windows 7 X64;

7.4.2.1.3. Windows 10 x64;

7.4.2.2. Suportar atualização da base de dados da Rede de Inteligência de forma automática e sem causar nenhum tipo de indisponibilidade da solução

7.4.2.3. A análise inicial deve ser realizada de forma local no ambiente de detecção, o envio de artefatos para verificação na Sandbox deve ocorrer de forma automática, ou seja, caso a inteligência do produto identifique a necessidade de encaminhar o objeto para análise na sandbox este processo deve ocorrer sem a intervenção de qualquer usuário;

7.4.2.4. A solução deve ser capaz de prover dados forense detalhados, via interface gráfica, relacionados à infecção, demonstrando o ciclo de vida completo do ataque. Estes dados forenses devem incluir a cronologia completa do ataque e não apenas uma porção do ataque, assim como:

7.4.2.4.1. URLs/sites web relacionados ao ataque,

7.4.2.4.2. hashes MD5/SHA256,

7.4.2.4.3. binários maliciosos anexados,

7.4.2.5. Detectar e inspecionar, no mínimo, os seguintes tipos de arquivo, considerando as diferentes versões de sistemas operacionais e aplicativos existentes:

7.4.2.5.1. Arquivos executáveis;

7.4.2.5.2. Scripts;

7.4.2.5.3. Arquivos;

7.4.2.5.4. Documentos do office;

7.4.2.5.5. Arquivos de mídia;

7.4.2.5.6. Arquivos de Android (APK)

7.4.2.6. A solução deverá prover um método de disponibilizar updates das Sandboxes sem requerer um completo update do sistema operacional ou upgrade da solução e sem indisponibilidade de sua detecção;

7.4.2.7. Toda análise básica de malwares, incluindo malwares desconhecidos, deve ser realizada de forma automatizada através da detecção do exploit, sem a necessidade de criação de regras específicas ou interação de um operador;

7.4.2.8. Toda a análise do comportamento do malware deve ser registrada em tempo de execução;

7.4.2.9. A solução deve suportar importação de regras YARA personalizadas,

para permitir flexibilidade na criação de regras para análise de ameaças;

7.4.2.10. Suportar mecanismo de whitelist pelos seguintes métodos:

7.4.2.10.1. Hash MD5 do arquivo;

7.4.2.10.2. Formato do arquivo;

7.4.2.10.3. E-mail;

7.4.2.10.4. Subrede.

7.4.2.11. Deve permitir o envio de alertas por e-mail;

7.4.2.12. A solução deverá suportar mais de um Sandbox em cluster, permitindo o escalonamento baseado na necessidade do contratante;

7.4.2.13. Deverá possuir a capacidade de detectar ameaças direcionadas, realizando inspeção de tráfego até a camada 7 de forma a prevenir ataques do dia zero e executar análise profunda de documentos que contenham conteúdo malicioso ou redirecionamentos para outras URL's maliciosas;

7.4.2.14. O sandbox da solução deve possuir mecanismos para prevenção de evasão.

7.4.3. **Sensores de detecção**

7.4.3.1. A solução deverá permitir que o sensor monitore tráfego WEB, Mail e Rede;

7.4.3.2. Deverá permitir integração com solução de proxy utilizando o protocolo ICAP permitindo analisar protocolos seguros (ex: HTTPS);

7.4.3.3. Deverá verificar mensagens de email através do protocolo POP3 e SMTP;

7.4.3.4. Deverá processar tráfego espelhado e extrair objetos e metadados do DNS

7.4.3.5. A solução deve suportar um throughput de análise de no máximo 4000 Mbps;

7.4.3.6. A solução deverá ser gerenciada por console Web suportando no mínimo os browsers Internet Explorer e Firefox;

7.4.3.7. Deve permitir configurar mais de um sensor de rede caso o ambiente corporativo tenha mais de um ponto para análise;

7.4.3.8. Deverá possuir a capacidade de atualizar as vacinas do sensor pela internet ou através da console de gerenciamento;

7.4.3.9. O Sensor de rede deverá suportar SPAN Port ou TAP para análise do tráfego;

7.4.3.10. Deverá ser capaz de identificar ameaças evasivas em tempo real com o provimento de análise profunda e inteligência para identificar e prevenir ataques;

7.4.3.11. O sensor deverá encaminhar automaticamente para a sandbox um artefato potencialmente perigoso identificado no tráfego de rede;

7.4.3.12. O sensor deverá alertar qualquer artefato malicioso identificado já conhecido sem a necessidade de intervenção manual;

7.4.3.13. Deverá detectar incidentes de segurança motivados por conexões da rede interna com sites maliciosos ou servidores de central de comando (C&C) externos além da detecção de malwares conhecidos e desconhecidos, ransonware, Exploits, Botnets, Cross Site Script, SQL Injection, comunicações p2p, instant messengers; streaming, tentativas de scan de rede, tentativas de brute-force, situações de evasão e roubo de informação etc;

7.4.3.14. Deverá ter capacidade de verificar em tempo real a reputação de endereços web (URL's) e servidores de correio SMTP;

7.4.3.15. Deverá analisar arquivos maliciosos na rede utilizando vacinas e técnicas de heurística.

7.4.3.16. Deverá atuar de forma passiva na captura de tráfego sem oferecer impacto no desempenho da rede;

7.4.3.17. Deve permitir utilizar um sensor de rede como proxy, ou seja, deve permitir que o sensor receba informações do Endpoint para enviar à console de gerenciamento;

7.4.3.18. O Sensor deverá detectar sites maliciosos através de reputação;

7.4.3.19. O sensor deverá ter acesso a rede global de inteligência da fabricante;

7.4.3.20. Deverá integrar com a infraestrutura extraindo objetos do tráfego de rede e efetuando uma análise inicial;

7.4.3.21. Deverá receber objetos para serem verificados dos switches, servidores de proxy e servidores de e-mail;

7.4.3.22. Deverá atuar como IDS na rede detectando anomalias no tráfego de rede e alertando a console de gerenciamento sobre os eventuais incidentes;

7.4.3.23. Caso necessário, deve suportar uma arquitetura única atuando como sensor de rede e console de gerenciamento em uma mesma máquina virtual;

7.4.3.24. Através de consulta na base global da fabricante, deverá detectar os seguintes itens:

7.4.3.24.1. Endereços envolvidos em campanhas de ataques persistentes;

7.4.3.24.2. Servidores de "Command & Control";

7.4.3.24.3. Sites maliciosos;

7.4.3.24.4. Sites de phishing;

7.4.3.25. Deverá possuir tecnologia de cache para evitar envio de solicitações duplicadas;

7.4.3.26. Deve possuir capacidade de verificar links ativos em documentos do office;

7.4.3.27. O sensor de endpoint deve ser compatível com fabricantes terceiras, permitindo que colete e envie informações a console de gerenciamento sem causar conflito com a atual solução de antivírus.

7.5. **Plataforma automatizada de conscientização em Segurança da Informação com validade de 36 meses – ITEM 5,** o qual deverá atender aos requisitos técnicos enumerados a seguir:

7.5.1. **Compatibilidade com sistemas operacionais de desktop:**
- 7.5.1.1. Windows 10;
- 7.5.1.2. Windows 7;
- 7.5.1.3. MacOS 10.12 e superior.

7.5.2. **Compatibilidade com sistemas operacionais de dispositivos mobiles:**
- 7.5.2.1. iOS 11 e superiores;
- 7.5.2.2. Android 5.x e superiores;

7.5.3. **Suporte aos browsers:**
- 7.5.3.1. Microsoft Edge;
- 7.5.3.2. Internet Explorer 11;
- 7.5.3.3. Firefox;
- 7.5.3.4. Google Chrome;
- 7.5.3.5. Safari for MacOS;
- 7.5.3.6. Safari(iOS);
- 7.5.3.7. Google Chrome(Android).

7.5.4. **Suporte aos leitores de email do usuário final:**
- 7.5.4.1. Apple Mail 10+;
- 7.5.4.2. MS Outlook 2010+ (Windows, macOS);
- 7.5.4.3. Mail.App (iPhone SE ou superior);
- 7.5.4.4. Outlook (Google Pixel, iPhone 7 ou superior);
- 7.5.4.5. GMail;
- 7.5.4.6. Google Apps;
- 7.5.4.7. Office 365;
- 7.5.4.8. Outlook.com;
- 7.5.4.9. Yahoo!

7.5.5. **Características:**
- 7.5.5.1. A plataforma de treinamento deverá conter base de conhecimento com as principais dúvidas, dicas e guias de recomendações para o administrador da plataforma;
- 7.5.5.2. Durante a validade da licença, as atualizações da plataforma devem ser entregues sem ônus adicional;
- 7.5.5.3. Atualizações devem ser disponibilizadas para:
  - 7.5.5.3.1. Atualização de conteúdo dos treinamentos;

7.5.5.3.2. Adição de novos conteúdos;
7.5.5.3.3. Novas funcionalidades para facilitar administração;
7.5.5.3.4. Novas funcionalidades para facilitar interação dos usuários;
7.5.5.3.5. Melhorias gerais do sistema e correção de bugs;
7.5.5.4. As atualizações na plataforma devem ser realizadas sem causar indisponibilidade ou afetar as funcionalidades;
7.5.5.5. O plano de atualização da plataforma deve:
7.5.5.5.1. Ser apresentado ao administrador da plataforma dias antes da sua execução;
7.5.5.5.2. Possibilitar ao administrador sugerir melhorias e votar estas melhorias durante a fase de discussão destas;
7.5.5.6. A interface da plataforma de treinamento, as notificações por e-mail e todo material de treinamento deverá ser disponibilizado minimamente nos idiomas Português, Inglês, Espanhol, Alemão e Francês;
7.5.5.7. A plataforma deverá gerar automaticamente os seguintes relatórios de acompanhamento ao Administrador:
7.5.5.7.1. Relatório resumo com informações sobre o progresso dos usuários:
7.5.5.7.1.1. Deve ser enviado no mínimo semanalmente;
7.5.5.7.1.2. Conter análise dos usuários por categoria de desempenho;
7.5.5.7.1.3. Conter link para relatório completo do treinamento;
7.5.5.7.1.4. Conter links com recomendações para alteração das categorias de treinamento baseado no desempenho do usuário.
7.5.5.7.2. Relatório geral detalhado da empresa:
7.5.5.7.2.1. Deve conter lista de administradores da plataforma;
7.5.5.7.2.2. O número de usuários (número geral e por status de treinamento);
7.5.5.7.2.3. Informações sobre uso de licenças;
7.5.5.7.2.4. Informações sobre categorias de desempenho;
7.5.5.7.2.5. Lista completa de usuários, especificando o grupo de treinamento pertencente;
7.5.5.7.2.6. A data em que o usuário consentiu em participar dos treinamentos;
7.5.5.7.2.7. As datas de conclusão planejadas e calculadas;
7.5.5.7.2.8. O número de unidades de treinamento com datas expiradas;
7.5.5.7.2.9. O número de testes não iniciados;
7.5.5.7.2.10. O número de testes a serem repetidos;
7.5.5.7.2.11. O número de certificados recebidos;

7.5.5.7.2.12. Exportar o relatório em formato XLSX.

7.5.5.7.2.13. Conter informações detalhadas sobre todos os alunos que estão em treinamento ou com treinamento suspenso.

7.5.5.7.3. Relatório geral sobre grupos de treinamento:

7.5.5.7.4. Deve incluir os principais dados sobre o progresso do treinamento para todos os grupos:

7.5.5.7.4.1. Número de usuários;

7.5.5.7.4.2. Usuários em treinamento ou com treinamento concluído;

7.5.5.7.4.3. Usuários sem atribuição de grupos;

7.5.5.7.4.4. Data de conclusão prevista, baseada na taxa real de treinamento dos usuários;

7.5.5.7.4.5. Porcentagem de usuários que concluíram.

7.5.5.7.5. Relatório sobre o grupo de treinamento, incluindo:

7.5.5.7.5.1. Diagrama da meta e do nível atual de conhecimento do grupo

7.5.5.7.5.2. Dados básicos sobre o progresso do treinamento:

7.5.5.7.5.2.1. Atribuído: número de usuário que foram adicionados ao programa e que receberam treinamento em um nível especificado;

7.5.5.7.5.2.2. Não iniciado: o número de usuários para os quais o treinamento foi atribuído, mas que ainda não iniciaram o treinamento neste nível;

7.5.5.7.5.2.3. Em treinamento: a quantidade de usuários que iniciaram o treinamento no nível indicado;

7.5.5.7.5.2.4. Nível concluído: o número de usuários que concluíram o treinamento no nível indicado.

7.5.5.7.5.2.5. Porcentagem concluído: a porcentagem de usuários (versus o número total de usuários) que alcançaram o nível alvo.

7.5.5.7.6. Relatório individual por usuário, incluindo:

7.5.5.7.6.1. Deve conter informações sobre o atendimento dos treinamentos por parte dos usuários;

7.5.5.7.6.2. Dinâmica de treinamento para os usuários;

7.5.5.7.6.3. Atividade diária dos usuários;

7.5.5.7.6.4. Histórico de treinamento do usuário em formato de tabela, incluindo as seguintes informações:

7.5.5.7.6.4.1. Data e horas;

7.5.5.7.6.4.2. Tipo de atividade (material de treinamento);

7.5.5.7.6.4.3. Unidade;

7.5.5.7.6.4.4. Nome do material de treinamento;

7.5.5.7.6.4.5. Status;
7.5.5.7.6.4.6. Tempo gasto (em minutos);
7.5.5.7.6.5. Tempo total gasto para treinamento;
7.5.5.7.6.6. Recomendações encaminhadas ao usuário;
7.5.5.7.6.7. Sessões agendadas;
7.5.5.7.6.8. Problemas de aprendizagem;
7.5.5.7.6.9. Nível de conhecimento do usuário;
7.5.5.7.6.10. Categoria de desempenho atual;

7.5.5.8. O usuário deverá receber e-mails semanais com relatórios de desempenho e de treinamento;

7.5.5.9. A plataforma deve definir no mínimo 5 (cinco) categorias de desempenho: “Antes do cronograma”, “Indo bem”, “Atrasado no cronograma”, “Muito atrasado no cronograma”, “Não terminará no prazo”.

7.5.5.10. Cada usuário que está participando do treinamento deverá ser atribuído a uma dessas categorias de desempenho:

7.5.5.10.1. Atrasado no cronograma;
7.5.5.10.2. Significativamente atrasado;
7.5.5.10.3. Impossível terminar no prazo;
7.5.5.10.4. Devem conter as subcategorias:
7.5.5.10.4.1. Não realizar os testes;
7.5.5.10.4.2. Falha nos testes;
7.5.5.10.4.3. Nunca entrou na plataforma.

7.5.5.11. Requisitos para definir categorias de desempenho do usuário:

7.5.5.11.1. “Não é possível terminar no prazo” caso o usuário não possa concluir o treinamento até a data de conclusão programada conforme especificado no cronograma de treinamento;
7.5.5.11.2. “Significativamente atrasado” se o usuário tiver 4 (quatro) ou mais unidades inacabadas;
7.5.5.11.3. “Atrasado na programação” se o usuário tiver de 1(uma) a 3(três) unidades inacabadas;
7.5.5.11.4. “Antecipado” se o usuário completou mais unidades que o necessário;
7.5.5.11.5. Em todos os outros casos, o usuário é atribuído à categoria “Vai bem”.

7.5.5.12. Requisitos para definir subcategorias de performance de usuários;

7.5.5.12.1. “Nunca acessou a plataforma” – Se o usuário não aceitou os termos e condições do treinamento;
7.5.5.12.2. “Não realizou os testes” – Se o usuário não iniciou os testes após término das lições;
7.5.5.12.3. “Testes falhos” – O usuário falhou em um ou mais testes ou

simulações de phishing após término das lições;

7.5.5.13. Requisitos para estatísticas de campanhas simuladas de phishing, incluindo no relatório:

7.5.5.13.1. Taxas de cliques;

7.5.5.13.2. Número e data/hora dos e-mails enviados;

7.5.5.13.3. Envio de email;

7.5.5.13.4. Resultado de falha para usuários;

7.5.5.14. Requisitos para objetivos e tarefas da plataforma de treinamento:

7.5.5.14.1. A plataforma de treinamento deve auxiliar na realização dos seguintes objetivos em uma organização:

7.5.5.14.1.1. Reduzir o risco de incidentes quando os funcionários usam recursos de TI, trocam dados pela Internet e trocam dados inadequadamente usando dispositivos móveis;

7.5.5.14.1.2. Minimizar os custos trabalhistas de gerenciamento de treinamento para funcionários.

7.5.5.14.2. A plataforma de treinamento deve resolver as seguintes tarefas:

7.5.5.14.2.1. Definir metas de treinamento e atribuir um programa de treinamento aos usuários;

7.5.5.14.2.2. Fornecer aos usuários os materiais de treinamento relevantes para o programa de treinamento;

7.5.5.14.2.3. Fornecer informações sobre o programa de treinamento na forma de relatório e diagramas;

7.5.5.15. Requisitos gerais para a plataforma de treinamento:

7.5.5.15.1. A plataforma deve incluir os seguintes elementos:

7.5.5.15.1.1. Interface gráfica de usuário do administrador;

7.5.5.15.1.2. Interface gráfica do usuário;

7.5.5.15.1.3. Materiais de treinamento (conteúdo);

7.5.5.15.1.4. Simulador de ataque de phishing:

7.5.5.15.1.4.1. Comunicando;

7.5.5.15.1.4.2. Configurações;

7.5.5.15.1.4.3. Suporte técnico;

7.5.5.15.1.5. O acesso à plataforma de treinamento deve ser feito via internet, utilizando protocolos HTTPS e HTTP.

7.5.5.16. O administrador da plataforma de treinamento deve ser capaz de gerenciar o processo de treinamento de todos os usuários;

7.5.5.17. A plataforma de treinamento deve permitir que o administrador crie e remova empresas;

7.5.5.18. A plataforma de treinamento deve ser capaz de atribuir uma empresa específica a um administrador e restringir o acesso desse administrador a

outras empresas;

7.5.5.19. A plataforma de treinamento deve ser capaz de atribuir privilégios diferentes para 4 funções de administrador. Cada administrador pode visualizar e/ou gerenciar apenas nas empresas às quais está atribuído;

7.5.5.20. O administrador deve ser capaz de configurar todos os parâmetros da empresa e parâmetros de perfil do usuário, inserir dados do usuário, definir um conjunto de grupos de treinamento em cada empresa, alterar o programa de treinamento no grupo de treinamento, distribuir usuários entre os grupos de treinamento, atribuir e controlar o treinamento do usuário.

7.5.5.21. A plataforma deverá enviar notificações automáticas aos usuários, nos requisitos abaixo:

7.5.5.21.1. Os funcionários de um grupo que iniciou o treinamento deverão receber um e-mail com convite para seguir um link exclusivo, gerado pela plataforma usando o nome de domínio especificado pelo Administrador nas configurações da empresa.

7.5.5.21.2. O usuário deve receber automaticamente relatórios semanais de treinamento por e-mail. Tais relatórios deverão incluir a categoria de desempenho atual do usuário e recomendações sobre as unidades de treinamento atribuídas.

7.5.6. **Requisitos para definir os parâmetros de uma empresa**

7.5.6.1. O administrador deve ser capaz de definir os seguintes parâmetros de uma empresa:

7.5.6.1.1. Nome da empresa;

7.5.6.1.2. Nome de domínio de quarto nível do nome de domínio do site onde os usuários dessa empresa são treinados;

7.5.6.1.3. Idioma padrão (em particular, o idioma usado no primeiro convite enviado ao usuário);

7.5.6.1.4. Nome e endereço de correspondência do funcionário que desempenha as funções de suporte técnico aos usuários;

7.5.6.1.5. Campos (ou atributos) do perfil do usuário nessa empresa. O administrador deve ser capaz de adicionar atributos personalizados ou excluir atributos que foram adicionados anteriormente;

7.5.6.1.6. Regras para alocar usuários automaticamente em grupos de treinamento;

7.5.6.1.7. Saudações nas mensagens que os usuários recebem da plataforma;

7.5.6.1.8. Nome de usuário mostrado e certificados emitidos quando as unidades de treinamento são concluídas.

7.5.7. **Requisitos para usar licenças de usuário**

7.5.7.1. O administrador deve ser capaz de adicionar ou excluir licenças.

7.5.7.2. A plataforma não deve estabelecer uma conexão direta entre um usuário específico e uma licença específica.

7.5.7.3. A plataforma deve controlar os seguintes parâmetros relacionados à Licença:

7.5.7.3.1. O número de usuários na fase ativa de treinamento;

7.5.7.3.2. O número de licenças disponíveis.

7.5.7.4. Quando o administrador atribui treinamento a um usuário, o número de licenças usadas deve aumentar;

7.5.7.5. Quando o administrador interromper ou suspender o treinamento de um usuário, o número total de licenças usadas deve diminuir.

7.5.8. **Requisitos para gerenciamento de treinamento**

7.5.8.1. O administrador deve ser capaz de atribuir um programa de treinamento, dependendo da posição do funcionário e do grau de risco de segurança cibernética (conforme definido pela organização).

7.5.8.2. A plataforma deve executar automaticamente as seguintes etapas:

7.5.8.2.1. Criar horários de aula para grupos e cada usuário, com base no nível de destino selecionado do grupo;

7.5.8.2.2. Enviar notificações por e-mail automaticamente aos usuários;

7.5.8.2.3. Enviar automaticamente lembretes aos usuários informando que eles podem prosseguir para aproxima tarefa em um determinado estágio;

7.5.8.2.4. Criar e ajustar um cronograma de treinamento individual para cada funcionário;

7.5.8.2.5. Atribuir todos os materiais de treinamento ao usuário;

7.5.8.2.6. Acompanhar o progresso do treinamento de cada usuário;

7.5.8.2.7. Fornecer relatórios de desempenho semanais aos usuários;

7.5.8.2.8. Enviar e-mails aos usuários com recomendações personalizadas, para que possam concluir o curso no prazo e com sucesso;

7.5.8.2.9. Enviar e-mails ao administrador com relatórios semanais, incluindo recomendações sobre como motivar um usuário para a comunicação fora da plataforma de treinamento.

7.5.9. **Requisitos para gerenciamento de usuários**

7.5.9.1. A plataforma deve permitir que o Administrador execute as seguintes tarefas:

7.5.9.1.1. Adicionar, editar, arquivar, restaurar, excluir um usuário ou grupo de usuários;

7.5.9.1.2. Adicionar usuários à plataforma importando uma lista de

usuários de um arquivo XSLX.

7.5.9.1.2.1. O arquivo modelo deve estar disponível no site da plataforma;

7.5.9.1.3. Criar grupos e transferir usuários entre estes;

7.5.9.2. A plataforma deve ser capaz de se integrar com o Microsoft Active Directory e com outros sistemas via OpenAPI para sincronizar listas de usuários.

7.5.10. **Requisitos para gerenciamento de grupos**

7.5.10.1. O programa de treinamento deve permitir que o Administrador use os grupos de treinamento que existem por padrão ou crie um número ilimitado de novos grupos de treinamento;

7.5.10.2. O programa de treinamento deve permitir que o Administrador altere os parâmetros de treinamento para grupos, como o nome do grupo, o conjunto de tópicos, o nível de destino de cada tópico (definição de quantas sessões o usuário deve realizar neste tópico), a intensidade (define quantos minutos por semana o usuário é recomendado utilizar na plataforma).

7.5.10.2.1. O administrador atribui o nível de treinamento alvo dependendo do risco que cada usuário específico no grupo específico pode representar para a empresa. Quanto maior o risco, maior o nível de destino precisa ser.

7.5.10.2.2. Os níveis (“Iniciante”,”Elementar”,”Intermediário”) são distribuídos respectivamente de acordo com o nível de risco – de baixo a alto.

7.5.10.3. Por padrão, a plataforma deve ter três grupos correspondentes aos três diferentes níveis de treinamento:

7.5.10.3.1. Iniciante: Para funcionários com acesso limitado aos sistemas corporativos de TI;

7.5.10.3.2. Elementar: Para funcionários com acesso total à rede corporativa, mas sem acesso a informações especialmente confidenciais.

7.5.10.3.3. Intermediário: Para funcionários que têm acesso a informações confidenciais e dados pessoais, bem como acesso de administrador em seus computadores.

7.5.10.4. A plataforma de treinamento deve permitir que o administrador crie regras para mover usuários automaticamente para grupos de treinamentos quando são adicionados à plataforma de treinamento.

7.5.10.5. Para cada grupo de treinamento, o cronograma de treinamento deve ser calculado automaticamente de acordo com a intensidade do treinamento, a data de início do treinamento e nível alvo para cada um dos

tópicos selecionados.

7.5.10.6. O cronograma de treinamento deve ser alterado de acordo com a intensidade de treinamento selecionada pelo Administrador da plataforma.

7.5.10.7. A plataforma de treinamento deve ser capaz de iniciar e interromper o treinamento de um grupo de usuários ou de um usuário específico.

7.5.10.8. A plataforma de treinamento deve ser capaz de iniciar o treinamento para todos os usuários de um grupo específico.

7.5.10.9. A plataforma de treinamento deve ser capaz de adicionar um usuários a um grupo de treinamento.

7.5.11. **Requisitos de metodologia de treinamento**

7.5.11.1. O programa de treinamento deve ser elaborado de acordo com os seguintes princípios:

7.5.11.1.1. Os materiais de formação devem constituir um programa de formação, ou seja, os conteúdos e a quantidade de conhecimentos e competências em segurança cibernética necessários à aprendizagem obrigatória, bem como a sua distribuição por tópico, seção e nível de dificuldade;

7.5.11.1.2. Ao passar dos tópicos, o material de aprendizagem aumenta o nível de dificuldade em relação a apresentação de técnicas cibercriminosas mais avançadas e das contra-medidas relacionadas;

7.5.11.1.3. Cada tópico deve ser apresentado pelo mesmo conjunto de materiais de treinamento;

7.5.11.1.4. A estrutura da aula deve ser a mesma para todos os tópicos;

7.5.12. **Requisitos para o conteúdo dos materiais de treinamento**

7.5.12.1. O programa de treinamento da plataforma deve incluir, no mínimo, os seguintes tópicos:

7.5.12.1.1. Senhas e contas;
7.5.12.1.2. Segurança de E-mail;
7.5.12.1.3. Navegação na Web;
7.5.12.1.4. Redes sociais e serviços de mensageria;
7.5.12.1.5. Segurança do PC:
7.5.12.1.6. Dispositivos móveis;
7.5.12.1.7. Informação Confidencial;
7.5.12.1.8. GDPR.

7.5.12.2. O programa de treinamento deve incluir lições com temas atuais que possam desenvolver as habilidades dos usuários nas seguintes áreas de segurança cibernética:

7.5.12.2.1. Phishing;
7.5.12.2.2. Links maliciosos;
7.5.12.2.3. Ransomware;

7.5.12.2.4. Arquivos perigosos;
7.5.12.2.5. Aplicações maliciosas;
7.5.12.2.6. Engenharia social;

7.5.13. **Requisitos para o programa de treinamento**

7.5.13.1. Cada tópico deve ser dividido em vários níveis dedicados à prática de um grupo específico de habilidades no campo da segurança cibernética.
7.5.13.2. Cada nível do programa deve corresponder a ameaças com vários graus de gravidade, desde ataques básicos e em larga escala até proteção contra-ataques complexos e direcionados.
7.5.13.3. Cada tópico deve incluir aulas (exercícios), material para reforço (e-mail), teste de conhecimento e simulação de um ataque de phishing.
7.5.13.4. Para concluir um tópico com sucesso, o usuário deve fazer o teste de conhecimento relacionado.
7.5.13.5. A transição para o próximo nível deve ser possível depois que todos os tópicos anteriores no nível apropriado foram realizados e o teste de conhecimento relacionado aprovado com sucesso.
7.5.13.6. O usuário deve ter a opção de passar em um tópico com antecedência, realizando com sucesso o teste de conhecimento antes de aprender os materiais do tópico.

7.5.14. **Requisitos para materiais de treinamento**

7.5.14.1. A estrutura de aulas (incluindo exercícios) para cada tópico deve ser a mesma em todos os tópicos e deve seguir a sequência lógica abaixo:
7.5.14.1.1. Um conjunto de ações a serem realizadas;
7.5.14.1.2. Porque um usuário deve realizar essas ações;
7.5.14.1.3. As consequências potenciais de ações incorretas;
7.5.14.1.4. Os sinais de perigo que um usuário deve identificar;
7.5.14.1.5. As ações que um usuário deve realizar ao detectar sinais de perigo;
7.5.14.1.6. O que fazer se as dúvidas permanecerem.
7.5.14.2. Os seguintes tipos de materiais de treinamento devem ser apresentados:
7.5.14.2.1. Aulas, incluindo parte teórica e exercícios práticos com feedback;
7.5.14.2.2. Testes de conhecimento;
7.5.14.2.3. Simulações de ataque de phishing;
7.5.14.2.4. Exercícios de reforço.
7.5.14.3. As aulas devem incluir:
7.5.14.3.1. Slides a serem estudados;
7.5.14.4. Devem conter:
7.5.14.4.1. Informações textuais e gráficas;

7.5.14.4.2. Botões para avançar e retornar aos slides;

7.5.14.4.3. Questões para autoavaliação;

7.5.14.4.4. Os exercícios de reforço devem consistir em coleção de conselhos ou recomendações para exercícios anteriores, bem como exemplos reais de consequências do não cumprimento das regras de segurança cibernética.

7.5.14.4.5. O teste deve consistir em questões às quais o usuário deve dar uma resposta ou múltipla escolha de opções.

7.5.14.4.6. Os resultados do teste devem indicar a aprovação ou não.

7.5.14.4.7. Deve ser possível definir um valor mínimo de acertos para êxito no teste.

7.5.14.4.8. Quando o teste for concluído, o usuário poderá dar feedback para cada questão, independentemente de ter respondido corretamente.

7.5.14.4.9. Os ataques simulados de phishing devem permitir que a reação do usuário à ameaça cibernética seja verificada;

7.5.14.4.10. Os materiais de treinamento devem ser adaptados para usuários que suas contas pessoais em um navegador de dispositivo móvel.

7.5.15. **Requisitos para funcionalidade de simulação de ataques phishing**

7.5.15.1. A plataforma de treinamento deve abranger duas opções de atribuição de ataques simulados de phishing:

7.5.15.1.1. Integrado ao caminho de aprendizagem automatizado para dominar especificamente o conjunto de habilidades criadas nas lições anteriores da unidade.

7.5.15.1.2. Possibilidade de criar uma companha de phishing separada para um grupo específico de usuário não relacionados a nenhuma atividade de treinamento;

7.5.15.1.3. Um ataque de phishing simulado deve ser semelhante a uma mensagem real na forma de um texto com layout, imagens (opcional) e um link. Quando clicado,o link deve redirecionar o usuário para uma página simulada especial;

7.5.15.1.4. A página simulada para qual o usuário foi redirecionado no ataque simulado de phishing deve conter uma explicação sobre o motivo pelo qual o usuário foi parar naquele site, uma descrição do email que o usuário receber, bem como recomendações sobre o reconhecimento de e-mails de phishing.

7.5.15.1.5. A plataforma deve conter pelo menos trinta modelos de phishing diferentes que são enviados aos usuários durante o treinamento;

7.5.15.1.6. A campanha deve possibilitar ser agendada ou ser enviada imediatamente;

7.5.15.1.7. O usuário deve receber um ataque simulado de phishing em até 4 dias da conclusão com sucesso, dos testes de conhecimento do tópico de treinamento relacionado;

7.5.15.1.8. Quando configurada separada do programa de aprendizagem, a campanha de phishing deverá incluir vários modelos para o grupo de pessoas para envio aleatório de um determinado modelo para cada funcionário.

7.5.15.1.9. O usuário deverá ser considerado como aprovado no ataque de phishing simulado se ele (a) não clicar no link do email e não for direcionado para a página simulada.

7.5.15.1.10. Caso o usuário falhe na simulação, esta deverá acontecer novamente dentro do prazo de 4 (quatro) dias (caso o phishing simulado esteja integrado no caminho de aprendizagem automatizado).

7.5.16. **Requisitos para o cronograma de treinamento**

7.5.16.1. O cronograma de treinamento deve ser baseado nos seguintes intervalos de tempo:

7.5.16.1.1. O material de reforço deve estar disponível em até 4 dias após realização dos exercícios teóricos e práticos;

7.5.16.1.2. O teste de conhecimento deve estar disponível em até 3 dias após o material de reforço;

7.5.16.1.3. A simulação de ataque de phishing deve ser enviada ao usuário em até 4 dias após conclusão bem-sucedida dos testes de conhecimento;

7.5.16.2. Os materiais de treinamento deverão ser disponibilizados ao usuário conforme prazo estipulado;

7.5.16.3. O cronograma de treinamento deve se readequar de forma automática à velocidades diferentes dos usuários;

7.5.16.4. O usuário deverá ser aprovado no teste para um tópico específico antes de passar para o próximo tópico;

7.5.16.5. O usuário deverá ser capaz de refazer o teste reprovado após conclusão do treinamento;

7.5.16.6. No caso do usuário falhar no ataque de phishing simulado, este deve ser reenviado automaticamente em até 4 dias ao usuário;

7.5.16.7. O cronograma de treinamento do usuário deve ser baseado na intensidade de treinamento, não restringindo o usuário de fazer as aulas teóricos em seu ritmo. Conforme a intensidade aumentar, as quantidades de materiais teóricos atribuídos ao usuário também aumentarão.

7.5.16.8. A plataforma deve calcular automaticamente a programação do usuário com base no programa de treinamento do grupo.

7.5.17. **Requisitos para a conta pessoal do usuário da plataforma**

7.5.17.1. Cada usuário deve ter uma conta pessoal única onde tarefas, histórico de treinamento, informações sobre desempenho e progresso estarão disponíveis;

7.5.17.2. A conta pessoal deve ser uma página da web acessível ao usuário através de um link exclusivo que o usuário recebe por meio de notificações por e-mail;

7.5.17.3. O histórico de treinamento deve incluir uma lista de todas as tarefas concluídas e seus respectivos resultados;

7.5.17.4. O usuário deverá ser capaz de retornar ao material preenchido anteriormente para repetir o treinamento;

7.5.17.5. Na conta pessoal do usuário, deverá haver informações sobre andamento e estatísticas sobre os materiais abordados;

7.5.17.6. As estatísticas de treinamento devem ser visíveis par ao usuário:

7.5.17.6.1. Informações sobre o nível sobre a habilidade alvo do usuário;

7.5.17.6.2. Porcentagem de habilidade adquiridas até o momento do número total de habilidades para um determinado nível alvo;

7.5.17.6.3. Data planejada de conclusão do treinamento;

7.5.17.6.4. Data prevista de conclusão;

7.5.17.7. A data prevista de conclusão do treinamento do usuário deve ser calculada de acordo com a programação do grupo do qual o usuário faz parte;

7.5.17.8. A data de conclusão da unidade no plano de treinamento do usuário deve ser determinada com base na data planejada do teste e o tempo que o usuário requer para fazer o teste;

7.5.17.9. Na página de treinamento do usuário deverá haver conselhos e recomendações que ajudarão o usuário a concluir o treinamento no prazo;

7.5.17.10. A conta pessoal do usuário deve ser totalmente adaptada para que possa ser usada em dispositivos móveis.

7.5.18. **Requisitos para certificados**

7.5.18.1. O usuário deve receber um certificado após a conclusão bem-sucedida de cada tópico realizado;

7.5.18.2. O tópico deve ser considerado concluído com êxito quando o usuário tiver concluído com êxito o teste e for aprovado na simulação de ataque de phishing;

7.5.18.3. O certificado deve ser apresentado em formato eletrônico na interface do usuário e estar disponível para download;

7.5.18.4. O administrador deve ter a possibilidade de escolher como representar o nome do funcionário e outros campos personalizados no certificado.

7.5.19. **Requisitos para customização**

7.5.19.1. Logo da instituição:

7.5.19.1.1. O Administrador deve ser capaz de adicionar o logotipo da empresa na conta da plataforma;

7.5.19.1.2. Saudações ao aluno:

7.5.19.1.3. O administrador deve ser capaz de personalizar a saudação do funcionário em notificações por e-mail enviadas aos alunos pela plataforma – como convites, lembretes e recomendações.

7.5.19.1.4. A possibilidade deve dar a capacidade de fazer essas saudações mais adequadas às especificidades do país e/ou cultura de diferentes clientes.

7.5.19.1.5. O administrador deve ser capaz de adicionar qualquer texto ou usar marcas para criar o texto necessário.

7.5.19.1.6. As tags devem incluir o nome completo do usuário, saudação curta e todos os campos personalizados criados para esta empresa.

7.5.19.2. Certificados dos alunos:

7.5.19.2.1. O administrador deve ser capaz de personalizar a aparência do nome do aluno no certificado;

7.5.19.2.2. O administrador deve ser capaz de adicionar qualquer texto ou usar marcas para criar o texto necessário;

7.5.19.2.2.1. As tags devem incluir o nome completo do usuário, saudação curta e todos os campos personalizados criados para esta empresa.

7.5.19.3. Personalização do programa educacional:

7.5.19.3.1. Este recurso deve dar ao administrador a possibilidade de gerenciar o processo de aprendizagem para a empresa:

7.5.19.3.1.1. Desativar/ativar os primeiros testes de teste que permitem ao usuário pular a teoria;

7.5.19.3.1.2. Desativar/ativar a simulação de phishing que é incluída automaticamente no caminho de aprendizagem;

7.5.19.3.1.3. Escolher o nível alvo e os tópicos a serem atribuídos ao grupo de usuários.

7.5.19.4. Personalização do caminho de aprendizagem:

7.5.19.4.1. Para cada grupo de treinamento, o administrador deve ser capaz de selecionar:

7.5.19.4.1.1. Tópicos que os alunos neste grupo precisam aprender (e pular aqueles que você não deseja treinar agora).

7.5.19.4.1.2. Nível alvo desejado para que os alunos atinjam em cada tópico específico.

7.5.19.5. Personalização de ataques de phishing simulados:

7.5.19.5.1. Possibilidade de personalizar template de phishing com assunto, textos e fotos e salvar na biblioteca;

7.5.19.5.2. Variedade de domínios de phishing e endereços de e-mail de remetentes para personalização.

7.6. **Serviços de Treinamento – ITEM 6.1 e 6.2**

7.6.1. **TREINAMENTO PARA SOLUÇÃO DE PROTEÇÃO – ITEM 6.1**

7.6.1.1. Consiste no fornecimento dos subsídios para que as equipes da CONTRATANTE obtenham os conhecimentos adicionais necessários para entender e utilizar as funcionalidades disponibilizadas pela Solução, tais como: arquitetura, configurações, funções e mecanismos de atualização e de distribuição de vacinas e customizações da Solução;

7.6.1.2. CONTRATADA deverá fornecer a transferência de conhecimento para os funcionários da CONTRATANTE mediante treinamento presencial, com carga horária mínima de 30 horas, que utilize os instrumentos conceituais e didáticos adequados a solução do fabricante da Solução. Deverá ser previsto o treinamento de pelo menos 5 -(cinco) membros das Equipes da CONTRATANTE;

7.6.1.3. O treinamento deverá ser ministrado por profissional com certificação oficial do fabricante da Solução, devendo estes apresentar diplomas e/ou certificações que estejam válidas pelo menos até o último dia da transferência de conhecimento. Estes certificados devem ser encaminhados ao setor de treinamentos da CONTRATANTE até o décimo dia útil anterior à data inicial da transferência de conhecimento;

7.6.1.4. O conteúdo programático do treinamento, bem como as datas e estimativa de tempo para realização das mesmas, deverá ser submetido ao gestor operacional do contrato para análise e aceite, devendo compreender no mínimo os seguintes tópicos:

7.6.1.4.1. Tipos de arquitetura possíveis;

7.6.1.4.2. Funcionalidades da solução implantada;

7.6.1.4.3. Implantação e arquitetura do sistema, com opções de expansão e aperfeiçoamento;

7.6.1.4.4. Utilização avançada do sistema, inclusive com metodologia de criação de políticas;

7.6.1.4.5. Utilização e customização da solução;

7.6.1.4.6. Monitoração;

7.6.1.4.7. Gerenciamento de incidentes;

7.6.1.4.8. Utilização dos gráficos e relatórios;

7.6.1.4.9. Interpretação dos gráficos e relatórios;

7.6.1.5. Outros conhecimentos necessários ao entendimento e utilização avançada da Solução, conforme a CONTRATANTE e a CONTRATADA julgarem necessário;

7.6.1.6. Quaisquer custos relativos ao procedimento de treinamento já estão incluídos no valor ofertado;

7.6.1.7. Esta atividade de treinamento poderá ser realizada pelo fabricante da solução proposta. Todavia, a CONTRATADA será a responsável pelo recebimento, gerenciamento e execução de tais demandas, sendo a CONTRATADA o canal de acesso da CONTRATANTE para solicitações desta natureza;

7.6.2. **TREINAMENTO PARA RESPOSTA À INCIDENTES – ITEM 6.2**

7.6.2.1. O serviço consiste no fornecimento dos subsídios para que as esquipes da CONTRATANTE obtenham os conhecimentos adicionais necessários para entender e utilizar técnicas para resposta à incidentes;

7.6.2.2. A CONTRATADA deverá fornecer a transferência de conhecimento para os funcionários da CONTRATANTE mediante treinamento presencial e oficial do Fabricante, com carga horária mínima de 40 horas, que utilize os instrumentos conceituais e didáticos adequados para Resposta a Incidente. Deverá ser previsto o treinamento para até 05 (cinco) participantes;

7.6.2.3. O treinamento deverá ser ministrado por profissional com certificação oficial do fabricante da Solução, devendo estes apresentar diplomas e/ou

certificações que estejam válidas pelo menos até o último dia da transferência de conhecimento. Estes certificados devem ser encaminhados ao setor de treinamentos da CONTRATANTE até o décimo dia útil anterior à data inicial da transferência de conhecimento;

7.6.2.4. O conteúdo programático do treinamento, bem como as datas e estimativa de tempo para realização das mesmas, deverá ser submetido ao gestor operacional do contrato para análise e aceite, devendo compreender no mínimo os seguintes tópicos:

7.6.2.5. Introdução à resposta a incidente;

7.6.2.6. Detecção e análise primária;

7.6.2.7. Análise Digital;

7.6.2.8. Criação de regras de detecção (YARA, Snort, Bro);

7.6.2.9. Diferenciar APTs de outras ameaças;

7.6.2.10. Entendimento das técnicas de vários atacantes e anatomia de ataque direcionado;

7.6.2.11. Aplicar métodos específicos de monitoramento e detecção;

7.6.2.12. Seguindo o fluxo de trabalho de resposta a incidente;

7.6.2.13. Reconstruir a cronologia e a lógica do incidente;

7.6.2.14. Criação de regras de detecção e relatórios;

7.6.3. Quaisquer custos relativos ao procedimento de treinamento já estão incluídos no valor total deste objeto;

7.6.4. Esta atividade de treinamento poderá ser realizada pelo fabricante da solução proposta. Todavia, a CONTRATADA será a responsável pelo recebimento, gerenciamento e execução de tais demandas, sendo A CONTRATADA o canal de acesso da CONTRATANTE para solicitações desta natureza;

7.7. **Serviço de Consultoria e Suporte Técnico – ITEM 7**

7.7.1. Caberá a CONTRATADA a prestação dos serviços de consultoria e suporte técnico na Solução de Proteção de Endpoints fornecidos pelo prazo de 36 (trinta e seis) meses, compreendendo suporte telefônico, remoto ou local;

7.7.2. Em sua essência, tais serviços visam auxiliar a equipe técnica da CONTRATANTE na implantação, administração e na operação do sistema, no

âmbito das atividades que exijam conhecimentos com maior grau de complexidade e que possam impactar negativamente no negócio caso sejam executadas sem sucesso;

7.7.3. A CONTRATADA deverá disponibilizar horas técnicas, conforme definido na tabela de itens, de suporte ou de consultoria ao longo da execução do Contrato, podendo estas ser utilizadas a qualquer tempo, mediante solicitação;

7.7.4. Os serviços serão solicitados sob demanda mediante a abertura de chamado efetuada por técnicos da CONTRATANTE, via chamada telefônica, ou por e-mail, no horário das 9h às 19h (horário de Brasília), de segunda a sexta-feira, informando a modalidade de atendimento no momento da solicitação;

7.7.5. As horas utilizadas no mês, serão enviadas pela CONTRATADA até o dia 10 de cada mês subsequente a finalização do chamado ao Fiscal do Contrato da CONTRATANTE para ateste de sua efetiva execução;

7.7.6. Após o recebimento do ateste a CONTRATADA deverá emitir a Nota Fiscal para o devido pagamento das horas utilizadas;

7.7.7. As horas técnicas deverão ser prestadas por técnicos devidamente certificados para prestar serviços de consultoria na ferramenta adquirida;

7.7.8. O Suporte Técnico será realizado na modalidade remoto, via telefone, acesso remoto aos equipamentos, Mensagem Instantânea, Website, e com possibilidade de atendimento on-site na sede da CONTRATANTE para casos em que a CONTRATADA julgar necessário e havendo a concordância da PMM, no Regime de Suporte técnico 8x5, com Garantia de Tempo de Resposta (SLA): A Garantia de tempo de resposta, será realizada conforme critérios de prioridades abaixo:

7.7.8.1. Prioridade A - SERVIÇO INDISPONÍVEL: até 8 horas úteis;

7.7.8.2. Prioridade B - FUNCIONAMENTO PARCIAL: até 24 hora

7.7.8.3. Prioridade C - SERVIÇO NORMAL: até 48 horas.

7.7.9. O suporte remoto deverá contemplar, no mínimo:

7.7.9.1. Esclarecimento de dúvidas de utilização, administração e operação dos softwares fornecidos e utilizados pela CONTRATANTE;

7.7.9.2. Poderá ser solicitado o envio de procedimentos para resolver

problemas de utilização, administração e operação dos softwares fornecidos e utilizados pela CONTRATANTE;

7.7.9.3. Fornecer orientação sobre a necessidade de realizar atualização de software para resolver problemas reportados;

7.7.9.4. A análise, elaboração e implantação de projetos que envolvam softwares de antivírus e anti-spyware em uso e os que porventura venham a ser utilizados na CONTRATANTE;

7.7.9.5. Auxílio na gestão de políticas de segurança da solução CONTRATADA com vistas à prevenção e combate de vírus de computador, spywares e outras ameaças, sendo desde a avaliação do ambiente atual com ações reativas a emergências e/ou novo projeto com implementação tecnológica atualizada para o mesmo fim;

7.7.9.6. Avaliação de vulnerabilidades, prevenção de vírus de computador, spywares e outras ameaças, do ambiente computacional da CONTRATANTE;

7.7.9.7. A implementação de filtros, políticas, e outros recursos disponíveis na solução de endpoint CONTRATADA, a fim de impedir a proliferação de ameaças identificadas e que não disponham, em determinado momento, de vacina;

7.7.9.8. O auxílio na auditoria e análise de logs.

8. DA EXECUÇÃO DO CONTRATO

8.1. Regime de execução será por empreitada por preço unitário;

8.2. CONTRATAÇÃO DAS LICENÇAS (ITENS 1 a 5)

8.2.1. A contratação das licenças será por demanda e conveniência da CONTRATANTE através da emissão de Pedido de Compra – PC, vinculado ao respectivo Contrato.

8.2.2. Todas as licenças devem possuir validade de 36 meses;

8.3. CONTRATAÇÃO DE TREINAMENTO (ITEM 6)

8.3.1. A contratação dos treinamentos será por demanda e conveniência da CONTRATANTE através da emissão de Autorização de Execução de Serviço – AES, vinculada ao respectivo contrato, informando o quantitativo de treinamento

solicitados;

8.4. CONTRATAÇÃO DE SERVIÇO DE CONSULTORIA E SUPORTE TÉCNICO NA SOLUÇÃO DE PROTEÇÃO AVANÇADA (ITEM 7)

8.4.1. A contratação do serviço de consultoria e suporte técnico será por demanda e conveniência da CONTRATANTE através da emissão de Autorização de Execução de Serviço – AES, vinculada ao respectivo contrato, informando o quantitativo de horas solicitadas;

8.5. A atividade de fiscalização será realizada para assegurar o efetivo cumprimento das obrigações contratuais assumidas e a qualidade dos serviços prestados à CONTRATANTE;

8.6. Para tanto, o fiscal a ser designado pela CONTRATANTE deverá:

8.6.1. acompanhar, fiscalizar e atestar a execução dos serviços contratados;

8.6.2. indicar as eventuais glosas das faturas;

8.6.3. informar à Administração da CONTRATANTE o eventual descumprimento dos compromissos pactuados, que poderá ensejar a aplicação de penalidades.

8.7. Em audiência inaugural do contrato serão apresentados, por parte da CONTRATADA, o preposto indicado e, por parte da CONTRATANTE, o fiscal que fará o acompanhamento e a fiscalização da execução do contrato;

8.8. Nessa audiência serão definidos e formalizados os protocolos de comunicação entre a CONTRATANTE e CONTRATADA, para efeito da fiscalização do contrato;

8.9. Serão ainda ratificados os procedimentos decorrentes deste Termo de Referência para:

8.9.1. Emissão das Autorizações para Execução de Serviço;

8.9.2. Verificação do atendimento dos requisitos estabelecidos no Termo de Referência;

8.9.3. Atestação das faturas;

8.9.4. Descontos, multas e aplicação das demais sanções previstas;

8.9.5. Renovação do contrato;

8.9.6. Encerramento do contrato;

9. DAS CONDIÇÕES DE PAGAMENTO

9.1. O pagamento será efetuado mediante apresentação da Nota Fiscal/Fatura, sendo:

a) No caso de serviços prestados por banco de horas e/ou treinamento será considerado os serviços efetivamente prestados, que ocorrerá até o 15º (décimo quinto) dia útil do mês subsequente, com os descontos legais (retenções) do serviço apurados para o mês faturado.

b) Para casos referente a entrega de produtos (licenças de software) o pagamento será integral a quantidade adquirida para 36 meses e ocorrerá até o 15º (décimo quinto) dia útil do mês subsequente, com os descontos legais (retenções) no mês seguinte a entrega do produto.

9.2. O pagamento será de acordo com a apuração da quantidade de licenças solicitadas pelo Pedido de Compra – PC ou serviços demandados por Autorização de Execução de Serviço – AES;

9.3. A solicitação de mais licenças poderá ser realizada em qualquer momento.

9.4. O valor a ser pago pelo consumo dos **itens 1 a 5**, será calculado de acordo com a regra abaixo:

9.4.1. **Valor a pagar** = Quantidade de licenças adquiridas x Valor unitário de cada licença;

9.5. Para os serviços de treinamento **item 6**:

9.5.1. **Valor a Pagar** = Quantidade de turmas com treinamento concluído x Valor unitário de cada treinamento;

9.6. Para os serviços de consultoria **item 7:**

9.6.1. O valor será pago após a conclusão do serviço e corresponde à quantidade de horas demandadas e entregues, multiplicadas pelo valor unitário da hora, como descrito abaixo:

9.6.1.1. **Valor a Pagar =** ∑ de horas entregues x Valor unitário da hora

9.6.2. A quantidade de horas demandadas será definida na Autorização de Execução de Serviço–AES;

10. DAS OBRIGAÇÕES DA CONTRATANTE

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

10.2. Exercer o acompanhamento e a fiscalização dos serviços, por servidor especialmente designado, anotando em registro próprio as falhas detectadas, indicando dia, mês e ano, bem como o nome dos empregados eventualmente envolvidos, e encaminhando os apontamentos à autoridade competente para as providências cabíveis;

10.3. Notificar a Contratada por escrito da ocorrência de eventuais imperfeições no curso da execução dos serviços, fixando prazo para a sua correção;

10.4. Além dos contratos administrativos, o CONTRATANTE não aceitará assinar contratos com o FABRICANTE para o recebimento das licenças decorrentes deste processo, ficando a CONTRATADA obrigada a efetuar os seus pedidos cientes desta condição, bem como comprovar através do site do fabricante que as licenças adquiridas estão devidamente registradas no nome do CONTRATANTE;

10.5. A empresa deverá apresentar, obrigatoriamente, comprovação de que possui em seu quadro técnico, no mínimo, 1 (um) profissional com a certificação técnica do fabricante. Esta exigência se faz necessário dado a complexidade do projeto.

11. DAS OBRIGAÇÕES DA CONTRATADA

11.1. A contratada deve cumprir todas as obrigações constantes neste Termo e seus anexos, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto e, ainda;

11.2. Manter, durante toda execução do contrato, compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas;

11.3. Ter pleno conhecimento de todas as condições e peculiaridades inerentes aos serviços objeto deste Termo de Referência, não podendo invocar, posteriormente, desconhecimento para cobrança de serviços extras;

11.4. Executar os serviços e concluir todos os serviços contratados nos prazos estabelecidos neste Termo de Referência e nas Ordens de Serviço;

11.5. Responsabilizar-se integralmente pela sua equipe técnica, primando pela

qualidade, desempenho, eficiência e produtividade, visando à execução dos trabalhos durante todo o Contrato, dentro dos prazos estipulados, sob pena de ser considerada infração passível de aplicação de penalidades previstas, caso os prazos e condições não sejam cumpridas;

11.6. Fornecer, sem custos adicionais para o Contratante, quaisquer atualizações de patches, releases e novas versões dos softwares, durante a vigência da garantia contratual;

11.7. Comunicar a CONTRATANTE, por escrito, quaisquer anormalidades que ponham em risco o êxito e o cumprimento dos prazos da execução dos serviços, propondo as ações corretivas necessárias para a execução dos mesmos;

11.8. Atender às solicitações emitidas pela Fiscalização quanto ao fornecimento de informações e/ou documentação.

12. DA VIGÊNCIA

12.1. A validade da Ata de Registro de Preços será de 12 (doze) meses, a contar da sua publicação;

12.2. A vigência do contrato para a prestação dos serviços deste Termo de Referência será de 36 (trinta e seis) meses, podendo ser prorrogado nos termos da legislação vigente.

13. DA QUALIFICAÇÃO TÉCNICA

13.1. A LICITANTE deverá apresentar:

13.1.1. No mínimo 01 (um) atestado de aptidão técnica, fornecido por pessoa jurídica de direito público ou privado, que comprove a boa e regular execução, compatível ao objeto do edital e seus anexos, em condições compatíveis de quantidade e prazos;

13.1.2. Poderá apresentar tantos atestados de aptidão técnica quantos julgar necessários para comprovar que já executou objeto semelhante ao da licitação;

13.1.3. No caso de pessoa jurídica de direito público, o(s) atestado(s) deverá (ão) ser assinados (s) pelo titular da pasta ou pelo responsável do setor competente do órgão. Para pessoa jurídica de direito privado, o (s) atestados (s) deverá (ão) ser assinados pelo representante legal;

13.1.4. Para efeito de julgamento objetivo, considerar-se-á para comprovação de aptidão técnica, que a licitante tenha executado ou esteja executando quantitativo não inferior a 20% (vinte por cento) da quantidade total de licenças do item 1 da tabela de lote único, referente ao(s) item(s) para o(s) qual(is) está apresentando sua proposta de preços;

14. SANÇÕES ADMINISTRATIVAS

14.1. O serviço a ser prestado deverá seguir as especificações contidas neste Termo de Referência. O descumprimento total ou parcial de qualquer obrigação estabelecida sujeitará a CONTRATADA às sanções legais aplicáveis, garantida a prévia e ampla defesa;

14.2. Além das penalidades legalmente previstas e sem prejuízo das mesmas, a CONTRATADA ficará sujeita às sanções a seguir relacionadas:

14.2.1. Advertência;

14.2.2. Multa de 10% (dez por cento) sobre o valor do contrato na hipótese de perda de dados, utilização indevida dos mesmos ou falha que possibilite a utilização dos dados por terceiros não autorizados, respondendo adicionalmente por perdas e danos pertinentes;

14.2.3. Pela rescisão do contrato por iniciativa da CONTRATADA, sem justa causa, multa de 10% (dez por cento) do valor total atualizado do contrato, sem prejuízo do pagamento de outras multas que já tenham sido aplicadas e de responder por perdas e danos que a rescisão ocasionar à CONTRATANTE;

14.2.4. Suspensão temporária de participação em licitação e impedimento de contratar com a CONTRATANTE pelo prazo de até 02 (dois) anos;

14.2.5. O valor da multa, apurado após regular procedimento administrativo, será descontado dos pagamentos eventualmente devidos pela CONTRATANTE, da Garantia ou cobrados judicialmente;

15. **MATRIZ DE RISCO**

A seguir relacionamos os riscos inerentes à contratação dos objetos do TR.

Descrição	Impacto	Responsável	Prazo p/ ajustes	Tratativa / Penalidade
Não cumprimento de cláusulas contratuais	Alto	CONTRATADA ou CONTRATANTE	72h	Sanções conforme TR, CONTRATO e/ou legislação em vigor.
Falha ou ausência de parte na entrega de qualquer Etapa do Objeto	Alto	CONTRATADA	72h	Suspensão do pagamento da NF até entrega total da Etapa do Objeto.
Descumprimento dos prazos na execução dos serviços	Médio	CONTRATADA	72h	Sanções conforme TR, CONTRATO e/ou legislação em vigor.
Denúncia de falha no atendimento	Médio	CONTRATADA	Imediato	Sanções conforme TR, CONTRATO e/ou legislação em vigor.
Qualidade do serviço afetado com baixa performance	Baixo	CONTRATADA	Imediato	Recuperar a qualidade do serviço conforme abertura de chamado.
Cobranças indevidas	Baixo	CONTRATADA	No ato do faturamento	Glosa no valor do serviço não executado.

Legenda:

Impacto alto: suspensão total do serviço por um turno ou mais. A PRODAM poderá disponibilizar recursos próprios para não interromper o fluxo dos serviços. O fornecedor poderá ser punido conforme cláusulas contratuais, caso seja apurada a sua responsabilidade.

Impacto médio: somente parte dos serviços ou parte dos clientes será afetada pela falta da prestação do serviço ou pela falha na prestação do serviço. A PRODAM poderá disponibilizar recursos próprios para não interromper os serviços mais críticos. O fornecedor poderá ser punido conforme cláusulas contratuais, caso seja apurada a sua responsabilidade.

Impacto baixo: o serviço poderá sofrer atraso, mas não será interrompido. A PRODAM não precisará disponibilizar recursos para regularizar o fluxo normal dos serviços. Não há a necessidade de punir o prestador do serviço, a menos que a falta se torne um problema frequente.

Quanto ao disposto nas alíneas “b” e “c” do Art. 42-X (Matriz de Riscos) da Lei 13.303/16 (Lei das Estatais), não há, identificada neste Termo de Referência, qualquer fração do objeto em que

haverá liberdade da CONTRATADA para inovar em soluções metodológicas ou tecnológicas, em obrigações de resultado ou em termos de modificação das soluções previamente delineadas neste documento.

Manaus, 01 de novembro de 2022

Salim Silva David
Gerência de Infraestrutura e Serviços

Maurício Mizobe
Diretor Técnico

Visto os autos, no uso de minhas atribuições,
APROVO o presente Termo de Referência.

Lincoln Nunes da Silva
Diretor Presidente PRODAM S.A.

PREGÃO ELETRÔNICO SRP 11/2022

Anexo 01-A – MODELO DE PROPOSTA DE PREÇOS

O preço deverá ser composto de acordo com a tabela abaixo:

ITEM	DESCRIÇÃO	Referência	Quantidade	Valor Unitário (R$)	Valor Total (R$)
1	Aquisição de Licenças da Solução de Proteção Avançada para *Endpoints* e Servidores Físicos com validade de 36 meses	Licença	20.000		
2	Aquisição de Licenças da Solução de Proteção Avançada para Ambientes Virtuais com validade de 36 meses	Licença	1.000		
3	Aquisição de Licenças da Solução de Proteção para Mobile com validade de 36 meses	Licença	1.000		
4	Aquisição de Licença da Solução de descoberta avançada de ameaças em nível de rede, com capacidade de análise de até 1 Gbit/s de Throughput, com validade de 36 meses	Licença	1		
5	Aquisição de Licença de Plataforma automatizada de conscientização em Segurança da Informação com validade de 36 meses	Usuário	2.500		
6	TREINAMENTOS				
6.1	Serviço de treinamento da Solução de Proteção	Turma	4		
6.2	Serviço de treinamento para resposta à incidentes	Turma	1		
7	Serviço de Consultoria e Suporte Técnico na Solução de Proteção Avançada	Hora	2.100		
VALOR GLOBAL DA PROPOSTA:					

Validade da Proposta: 90 (noventa) dias.

PREGÃO ELETRÔNICO SRP Nº 11/2022

ANEXO 2 - DOCUMENTOS PARA HABILITAÇÃO

1. DOCUMENTOS PARA HABILITAÇÃO

1.1. A arrematante será avaliada quanto ao cumprimento dos requisitos de participação no certame através de consulta efetuada pelo pregoeiro em algum dos seguintes cadastros:

1.1.1. Cadastro Nacional de Empresas Inidôneas e Suspensas – CEIS, no endereço eletrônico: www.portaldatransparencia.gov.br/sancoes/ceis;

1.1.2. Cadastro Nacional de Empresas Punidas – CNEP, no endereço eletrônico: www.portaldatransparencia.gov.br/sancoes/cnep

1.1.3. Outros sistemas cadastrais pertinentes com disposição para consulta.

1.2. Constatada a existência de sanção, o Pregoeiro reputará o licitante inabilitado, por falta de condição de participação e examinará as mesmas circunstâncias para o segundo colocado.

1.3. Caso atendidas as condições de participação, a arrematante terá seus documentos de habilitação verificada por meio do SICAF, nos documentos por ele abrangidos em relação à habilitação jurídica, à regularidade fiscal e trabalhista, à qualificação econômica financeira e habilitação técnica.

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

1.5. Havendo a necessidade de envio de documentos de habilitação complementares, necessários à confirmação daqueles exigidos neste Edital e já apresentados, o licitante será convocado a encaminhá-los, em formato digital, via sistema, no prazo de 2 (duas) horas.

1.6. Se o arrematante desatender às exigências habilitatórias, o pregoeiro examinará a documentação do licitante subsequente e, assim, sucessivamente até a apuração de documentação que atenda os termos do edital.

1.7. **Habilitação Jurídica:**

1.7.1. Registro comercial, no caso de empresa individual;

1.7.2. Ato constitutivo (Estatuto ou Contrato Social em vigor), devidamente registrado no Órgão competente, acompanhado de documento comprobatório da eleição dos atuais administradores;

1.7.3. Inscrição do Ato Constitutivo, no caso de Sociedades Civis, acompanhada de prova de designação da diretoria em exercício.

1.8. **Qualificação Econômico-Financeira:**

1.8.1. Certidão negativa ou positiva com efeito negativa de existência de ação de recuperação judicial de falência ou concordata, expedida pelo Cartório de Distribuição da sede da licitante;

1.8.2. Cópia do balanço patrimonial e demonstrações contábeis da licitante, do último exercício social, devidamente registrados na Junta Comercial, **na forma da lei**[1]. Em se tratando de empresas regidas pela Lei 6.404 de 15/12/1976, essa comprovação deverá ser feita através da publicação na Imprensa Oficial, apresentando a boa situação financeira da licitante, vedada a sua substituição por balancetes ou balanços provisórios. Os demonstrativos poderão ser atualizados por índices oficiais quando encerrado há mais de três meses da data prevista para realização desta licitação. (Devem-se incluir no balanço patrimonial os Termos de Abertura e Encerramento). **Deverá comprovar que possui capital social registrado ou patrimônio líquido mínimo igual ou superior, a 10% do valor global de sua proposta.**

1.8.2.1. A comprovação do subitem 1.8.2 deverá ser feita através do Balanço Patrimonial do último exercício publicado (contendo termo de abertura e encerramento), assinado por profissional devidamente habilitado pelo conselho de classe **OU** através da alteração do capital social em momento anterior à apresentação da proposta**.**

1.8.3. Comprovação da boa situação financeira da licitante, aferida com base nos índices de Liquidez Geral (ILG), iguais ou maiores que um (>1), aplicando a seguinte fórmula:

$$\frac{\text{ATIVO CIRCULANTE + REALIZÁVEL A LONGO PRAZO}}{\text{PASSIVO CIRCULANTE + PASSIVO NÃO CIRCULANTE}}$$

1.8.3.1. A comprovação do subitem 1.8.3 deverá ser feita através do Balanço Patrimonial do último exercício publicado (contendo termo de abertura e encerramento), assinado por profissional devidamente habilitado pelo conselho de classe.

1.8.4. A comprovação de que o profissional está devidamente habilitado, exigida nos itens 1.8.2.1 e 1.8.3.1, deverá ser comprovada por meio de emissão de certidão de regularidade profissional no devido conselho de classe.

1.9. **Regularidade Fiscal e Trabalhista:**

1.9.1. Inscrição no Cadastro Nacional de Pessoa Jurídica (CNPJ), do Ministério da Fazenda;

1.9.2. Certidões de regularidade fiscal e previdenciária apresentando Certidão Negativa de ou Positiva com Efeitos de Negativa de Débitos relativos a Créditos Tributários Federais e à Dívida Ativa da União **(portaria conjunta PGFN/RFB nº 1751/2014)**, Fazendas Estadual, Municipal ou do Distrito

---

[1] ***Na forma da lei:***

- Indicação do número das páginas e número do livro onde estão inscritos o Balanço Patrimonial e as Demonstrações Contábeis no Livro Diário, acompanhados do respectivo Termo de Abertura e Termo de Encerramento do mesmo - § 2º do art. 1.184 da Lei 10.406/02; Art. 1.180, lei 10.406/02; art. 177 da lei 6.404/76;

- Assinatura do contador e do titular ou representante legal da Entidade no Balanço Patrimonial e a Demonstração do Resultado do Exercício - § 2º do art. 1.184 da lei 10.406/02; § 4º do art. 177 da lei 6.404/76.

- Prova de registro na Junta Comercial ou Cartório (carimbo, etiqueta ou chancela da Junta Comercial) – art. 1.181, lei 10.406/02; resolução CFC nº 563/83; § 2º do art. 1.184 da lei 10.406/02.

- Demonstração de escrituração Contábil/Fiscal/Pessoal regular – NBC T 2 (Resolução CFC 563/83; art. 179, lei 10.406/02; art. 177 da lei 6.404/76; OU as empresas obrigadas ao envio do SPED CONTÁBIL deverão apresentar o recibo de entrega e o termos de abertura e de encerramento constantes na escrituração contábil digital.

- Boa situação financeira – art. 7.1, inciso V da IN/MARE 05/95

Federal do domicílio/sede da licitante.

1.9.3. Prova de regularidade relativa ao Fundo de Garantia Por Tempo de Serviço (FGTS) demonstrando situação regular no cumprimento dos encargos sociais instituídos por lei;

1.9.4. Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do artigo 642-A da Consolidação das Leis do Trabalho, acrescentado pelo Decreto-Lei nº 12.440 de 7 de julho de 2011, e na Resolução Administrativa nº 1470/2011 do Tribunal Superior do Trabalho, de 24 de agosto de 2011, em validade.

1.10. **Qualificação Técnico-operacional:**

1.10.1. No mínimo 01 (um) atestado de aptidão técnica, fornecido por pessoa jurídica de direito público ou privado, que comprove a boa e regular execução, compatível ao objeto do edital e seus anexos, em condições compatíveis de quantidade e prazos

1.10.2. Poderá apresentar tantos atestados de aptidão técnica quantos julgar necessários para comprovar que já executou objeto semelhante ao da licitação;

1.10.3. No caso de pessoa jurídica de direito público, o(s) atestado(s) deverá (ão) ser assinados (s) pelo titular da pasta ou pelo responsável do setor competente do órgão. Para pessoa jurídica de direito privado, o (s) atestados (s) deverá (ão) ser assinados pelo representante legal;

1.10.4. Para efeito de julgamento objetivo, considerar-se-á para comprovação de aptidão técnica, que a licitante tenha executado ou esteja executando quantitativo não inferior a 20% (vinte por cento) da quantidade total de licenças do item 1 da tabela de lote único, referente ao(s) item(s) para o(s) qual(is) está apresentando sua proposta de preços;

1.11. Declaração de inexistência de fato superveniente impeditivo de habilitação, conforme Anexo 4 – Modelo de Declaração de Fato Superveniente Impeditivo da Habilitação.

1.12. Declaração da empresa de que não possui, em seu quadro de pessoal, empregado (s) menor (es) de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre e, menores de 16 (dezesseis) anos em qualquer trabalho, salvo na condição de aprendiz, a partir de 14 (quatorze) anos, nos termos do artigo 7º, inciso XXXIII, da Constituição Federal, conforme Anexo 5 – Modelo de Declaração Quanto ao Cumprimento às Normas Relativas ao Trabalho do Menor.

1.13. O Pregoeiro reserva-se o direito de solicitar das licitantes, em qualquer tempo, no curso da licitação, quaisquer esclarecimentos sobre documentos já entregues, fixando-lhes prazo para atendimento.

1.14. O pregoeiro poderá convocar o licitante para enviar documento complementar, em formato digital, por meio de funcionalidade disponível no sistema, no prazo de 2 (duas) horas, sob pena de desclassificação.

1.15. Dentre os documentos passíveis de solicitação pelo Pregoeiro, destacam-se os que contenham as características do material ofertado, a exemplo de catálogos, folhetos ou propostas, ou planilhas de custos retificadas (em caso de contratação de serviços), encaminhados por meio eletrônico, ou, se for o caso, por outro meio e prazo indicados pelo pregoeiro, sem prejuízo do seu ulterior envio pelo sistema

eletrônico, sob pena de não aceitação da proposta.

1.16. Sem prejuízo da obrigatoriedade de envio por meio do sistema do site https://www.gov.br/compras/pt-br/, o pregoeiro poderá solicitar o envio para o e-mail: licitacoes@prodam.am.gov.br.

1.17. Os documentos de habilitação deverão estar em nome da licitante, com o número do CNPJ e respectivo endereço referindo-se ao local da sede da empresa licitante. Não se aceitará, portanto, que alguns documentos se refiram à matriz e outros à filial.

PREGÃO ELETRÔNICO SRP Nº 11/2022

ANEXO 3 – MINUTA DA ATA DE REGISTRO DE PREÇOS

Aos xxx dias do mês de xxxx do ano de dois mil e vinte e xx (xx/xx/20xx), nesta cidade de Manaus, Capital do Estado do Amazonas, República Federativa do Brasil, presentes, de um lado, a PRODAM – Processamento de Dados Amazonas S.A., pessoa jurídica de direito privado, sociedade de economia mista, criada pela Lei n.º 941, de 10/07/1970, com seus atos constitutivos registrados na Junta Comercial do Estado do Amazonas, sob o n.º 13300001038, e com inscrição estadual n.º 05.341.162-5, inscrição municipal n.º 673801 e CNPJ n.º 04.407.920/0001-80, neste ato representada por seu Diretor-Presidente Sr. **LINCOLN NUNES DA SILVA**, brasileiro, união estável, administrador, portador da Cédula de Identidade n.º XXXXXXX SSP/AM e do CPF n.º XXX.XXX.XXX-XX, residente e domiciliado nesta cidade, no uso das atribuições que lhe confere o Estatuto Social, em seu artigo 34, inciso XVI, conforme atesta a Ata de da Reunião Extraordinária do Conselho de Administração PRODAM, datada de 30/11/2020, e registrada na JUCEA/AM, em data de 18/12/2020, sob o nº 1085793, considerando julgamento da licitação na modalidade de Pregão, na forma Eletronica, para REGISTRO DE PREÇOS n° XX/20XX, publicada no Diário Oficial do Estado do Amazonas de XX/XX/XXXX, processo administrativo, SIGED 01.05.016503.002933/2022-29, RESOLVE registrar os preços da empresa indicada e qualificada nesta ATA, de acordo com a classificação por ela alcançada e na quantidade cotada, sujeitando-se as partes às normas contidas na Lei nº 13.303, de 30.06.2016, Decreto Estadual nº 39.032, de 24.05.2018, Lei nº 10.520, de 17.07.2002, Lei Complementar nº 123, de 14.12.2006, Decreto Estadual nº 21.178, de 27.09.2000, Decreto nº. 5.450, de 31 de maio de 2005, Decreto Estadual nº 24.818, de 27.01.2005, Decreto Estadual nº 40.674, de 14.05.2019, Decreto nº 10.024 de 20.09.2019 e alterações e RILC - Regulamento Interno de Licitações e Contratos da PRODAM e ainda, pelo estabelecido no presente Edital e seus Anexos, e em conformidade com as disposições a seguir:

1. **DO OBJETO:** Fornecimento de Solução de Segurança Avançada para Endpoints e Servidores, com proteção integrada contra ataques complexos, direcionados e descoberta avançada de ameaças em nível de rede, com capacidade de respostas automatizadas a incidentes, bem como serviços de instalação, configuração, treinamento, serviços de consultoria e suporte técnico em sistemas de segurança na solução fornecida para prevenção de vírus de computador, spywares, APT e outras ameaças.

2. **DO FORNECEDOR REGISTRADO:** a partir desta data, fica registrado na PRODAM, observada a ordem de classificação, os preços dos fornecedores a seguir relacionados, objetivando o compromisso discriminado no Anexo deste

instrumento, nas condições estabelecidas no ato convocatório:

2.1 Fornecedor: XXXXXXXXXXXXXXX, CNPJ nº xxxxxxxxx/xxxxx- xx, com sede na xxxxxxxxxx, nº xxx, bairro, CEP xxxxxxx, Cidade/ESTADO, telefone (XX) XXXXXXXX, E-mail: xxxxxxxxxxxxxxxxxxx, representada por xxxxxxxxxx, Xx. XXXXXXXXXXXXXXXX, nacionalidade, profissão, estado civil, residente e domiciliado xxxxxxxxxx, nº xxx, bairro, CEP xxxxxxx, Cidade/ESTADO, RG nº xxxxxxx XXX/XXe CPF nº XXXXXXXXXXX.

2.2 Fornecedor: XXXXXXXXXXXXXXXXXXXXXXXXXXXXX, CNPJ nº xxxxxxxxx/xxxxx- xx, com sede na xxxxxxxxxx, nº xxx, bairro, CEP xxxxxxx, Cidade/ESTADO, telefone (XX) XXXXXXXX/ XXXXXXXX, E-mail: xxxxxxxxxxxxxxxxxxxxxxxxx, representada por xxxxxxxxxx, Xx. XXXXXXXXXXXXXXXX, nacionalidade, profissão, estado civil, residente e domiciliado xxxxxxxxxx, nº xxx, bairro, CEP xxxxxxx, Cidade/ESTADO, RG nº xxxxxxx XXX/XXe CPF nº XXXXXXXXXXX.

2.3. (...)

3. **CADASTRO DE RESERVA**
   3.1. A PRODAM utilizará o cadastro de reserva, no caso de impossibilidade de atendimento pelo primeiro colocado da ata, nas hipóteses previstas nos art. 24 do Decreto Estadual nº 40.674, de 14.05.2019.
   3.2. As empresas que integrarem o cadastro de reserva somente terão sua proposta, bem como sua documentação habilitatória, analisada, para fins de aceitação e habilitação, quando houver necessidade de contratação de fornecedor remanescente, nas hipóteses mencionadas.

4. **DA EXPECTATIVA DO FORNECIMENTO:** o ajuste com o fornecedor registrado será formalizado pela PRODAM mediante emissão de Pedido de Compra e ou Autorização para Execução do Serviço, observadas as disposições contidas no **Edital do Pregão SRP nº 11/2022.**

   4.1. O compromisso de entrega só estará caracterizado mediante o comprovado recebimento, pelo Fornecedor, de Pedido de Compra e ou Autorização para Execução do Serviço, decorrente desta Ata de Registro de Preços e Edital do Pregão SRP nº 11/2022.
   4.2. O fornecedor registrado fica obrigado a atender todos os pedidos efetuados durante a validade desta Ata de Registro de Preços.

5. **DO CONTROLE DOS PREÇOS REGISTRADOS:**

   5.1. A PRODAM adotará a prática de todos os atos necessários ao controle e

administração da presente Ata.

5.2. Os preços registrados e a indicação dos respectivos fornecedores detentores da Ata serão publicados na imprensa oficial e divulgados em meio eletrônico.

6. **DA READEQUAÇÃO DOS PREÇOS REGISTRADOS:** a qualquer tempo, o preço registrado poderá ser revisto em decorrência de eventual redução daqueles existentes no mercado, cabendo a PRODAM convocar os fornecedores registrados para negociar o novo valor.
   6.1. Caso o fornecedor registrado se recuse a baixar os preços registrados, a PRODAM poderá cancelar o registro ou convocar todos os fornecedores registrados para oferecerem novos envelopes de propostas, gerando novo julgamento e adjudicação para esse fim.
   6.2. Durante o período de validade da Ata de Registro de Preços, os preços não serão reajustados, ressalvada a superveniência de normas gerais ou estaduais aplicáveis à espécie.
   6.3. O diferencial de preço entre a proposta inicial do fornecedor detentor da Ata e a pesquisa de mercado efetuada pela PRODAM à época da abertura da proposta, bem como eventuais descontos por ela concedidos, serão mantidos durante a vigência da Ata de Registro de Preços.

7. **DO CANCELAMENTO DO REGISTRO DE PREÇOS:** o fornecedor registrado terá o seu registro cancelado quando:
   7.1. descumprir as condições da Ata de Registro de Preços;
   7.2. não aceitar reduzir seus preços registrados na hipótese de se tornarem superiores aos praticados no mercado;
   7.3. houver razões de interesse público.
   7.4. O cancelamento de registro, nas hipóteses previstas, assegurados o contraditório e a ampla defesa e, será formalizado por despacho da autoridade competente.
   7.5. O fornecedor registrado poderá solicitar o cancelamento de seu registro de preço na ocorrência de caso fortuito ou de força maior comprovados.

8. **DA VALIDADE DA ATA DE REGISTRO DE PREÇOS:** A presente Ata terá validade de 12 (doze) meses contada a partir da data de sua assinatura.

9. **DO PRAZO DA EXECUÇÃO DA PRESTAÇÃO DOS SERVIÇOS:** o prazo de entrega e execução dos serviços será conforme item 8.2.3 do termo de referência.

10. **DA DIVULGAÇÃO DA ATA DE REGISTRO DE PREÇOS:** A presente Ata será divulgada no portal da internet www.prodam.am.gov.br.

11. **DO FORO:** as dúvidas decorrentes da presente Ata serão dirimidas no Foro de Manaus, com renúncia de qualquer outro.

E por estarem de acordo com as disposições contidas na presente Ata, assinam este instrumento a PRODAM e o fornecedor registrado, na pessoa dos seus representantes legais, que vai assinada, em 2 (duas) vias, de igual e teor e forma.

MANAUS, XX de XXXX de 20XX.

Pela **PRODAM S.A.**	Pela **XXXXXXXXXXXXXXXXXX**
Lincoln Nunes da Silva Diretor-Presidente	**XXXXXXXXXXXXXXXXXX** Representante legal

REVISÃO E APROVAÇÃO:

Assessor Jurídico

PREGÃO ELETRÔNICO SRP Nº 11/2022

ANEXO DA MINUTA DA ATA DE REGISTRO DE PREÇOS Nº XX/20XX

GRUPO ÚNICO

ITEM	DESCRIÇÃO	Unidade	Quantidade	Valor unitáro	Valor total
1	Aquisição de Licenças da Solução de Proteção Avançada para *Endpoints* e Servidores Físicos com validade de 36 meses	Licença	20.000		
2	Aquisição de Licenças da Solução de Proteção Avançada para Ambientes Virtuais com validade de 36 meses	Licença	1.000		
3	Aquisição de Licenças da Solução de Proteção para Mobile com validade de 36 meses	Licença	1.000		
4	Aquisição de Licença da Solução de descoberta avançada de ameaças em nível de rede, com capacidade de análise de até 1 Gbit/s de Throughput, com validade de 36 meses	Licença	1		
5	Aquisição de Licença de Plataforma automatizada de conscientização em Segurança da Informação com validade de 36 meses	Usuário	2.500		
6	Treinamentos				
6.1	Serviço de treinamento da SoluçãodeProteção	Turma	4		
6.2	Serviço de treinamento para resposta à incidentes	Turma	1		
7	Serviço de Consultoria e SuporteTécnico na Solução de ProteçãoAvançada	Hora	2.100		

Pela **PRODAM S.A.**

Lincoln Nunes da Silva
Diretor-Presidente

Pela **XXXXXXXXXXXXXXXXXXX**

XXXXXXXXXXXXXXXXXXX
Representante legal

VALOR TOTAL DA ATA: R$ XXXXXXXXX (XXXXXXXXXXXXXXX)

PREGÃO ELETRÔNICO SRP Nº 11/2022

ANEXO 4

Modelo de declaração de fato superveniente impeditivo de habilitação

_____
(Nome da Empresa)

CNPJ/MF Nº _____, sediada

_____
(Endereço Completo)

declara, sob as penas da Lei, que até a presente data inexistem fatos impeditivos para sua habilitação no presente processo ciente da obrigatoriedade de declarar ocorrências posteriores.

_____
(Local e Data)

_____
(Nome e Número da Carteira de Identidade do Declarante)

OBS: Está declaração deverá ser emitida em papel timbrado da empresa proponente e carimbada com o número do CNPJ.

PREGÃO ELETRÔNICO SRP Nº 11/2022

ANEXO 5

Modelo de declaração quanto ao cumprimento às normas relativas ao trabalho do menor

_____

(Nome da Empresa)

CNPJ/MF Nº _____,
sediada.

_____

(Endereço Completo)

Declaro que não possuímos, em nosso Quadro de Pessoal, empregados menores de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre e em qualquer trabalho, menores de 16 (dezesseis) anos, salvo na condição de aprendiz, a partir de 14 (quatorze) anos, em observância ao artigo 7º, inciso XXXIII, da Constituição Federal

_____

(Local e Data)

_____

(Nome e Número da Carteira de Identidade do Declarante)

OBS: 1) Esta declaração deverá ser emitida em papel timbrado da empresa proponente e carimbada com o número do CNPJ.

2) Se a empresa licitante possuir menores de 14 anos aprendizes deverá declarar essa condição.

PREGÃO ELETRÔNICO SRP Nº 11/2022

ANEXO 6 - TABELA DE PREÇO MÁXIMO

Deverá ser respeitado o valor máximo de cada ITEM, sob pena de desclassificação.

ITEM	DESCRIÇÃO	Referência	Quantidade	Valor Unitário (R$)	Valor Total (R$)
1	Aquisição de Licenças da Solução de Proteção Avançada para *Endpoints* e Servidores Físicos com validade de 36 meses	Licença	20.000	278,47	5.569.400,00
2	Aquisição de Licenças da Solução de Proteção Avançada para Ambientes Virtuais com validade de 36 meses	Licença	1.000	2442,92	2.442.920,00
3	Aquisição de Licenças da Solução de Proteção para Mobile com validade de 36 meses	Licença	1.000	176,57	176.570,00
4	Aquisição de Licença da Solução de descoberta avançada de ameaças em nível de rede, com capacidade de análise de até 1 Gbit/s de Throughput, com validade de 36 meses	Licença	1	594.736,93	594.736,93
5	Aquisição de Licença de Plataforma automatizada de conscientização em Segurança da Informação com validade de 36 meses	Usuário	2.500	199,55	498.875,00
6	TREINAMENTOS				
6.1	Serviço de treinamento da Solução de Proteção	Turma	4	98.183,33	392.733,32
6.2	Serviço de treinamento para resposta à incidentes	Turma	1	458.600,00	458.600,00
7	Serviço de Consultoria e Suporte Técnico na Solução de Proteção Avançada	Hora	2.100	583,33	1.224.993,00
VALOR GLOBAL DA PROPOSTA:				R$ 11.358.828,25	

PREGÃO ELETRÔNICO SRP Nº 11/2022

ANEXO 7 – MINUTA DE CONTRATO

TERMO DE CONTRATO PARA FORNECIMENTO DE SOLUÇÃO DE SEGURANÇA AVANÇADA PARA *ENDPOINTS* E SERVIDORES, COM PROTEÇÃO INTEGRADA CONTRA ATAQUES COMPLEXOS, DIRECIONADOS E DESCOBERTA AVANÇADA DE AMEAÇAS EM NÍVEL DE REDE, COM CAPACIDADE DE RESPOSTAS AUTOMATIZADAS A INCIDENTES, CELEBRADO ENTRE A PRODAM – PROCESSAMENTO DE DADOS AMAZONAS S/A E A EMPRESA XXXXXXXXXXXXXXXXXXX, NA FORMA ABAIXO:

Aos xxxxxx dias do mês de xxxxx do ano de dois mil e xx (xx/xx/20xx), nesta cidade de Manaus, Capital do Estado do Amazonas, República Federativa do Brasil, presentes, de um lado, a **PRODAM – Processamento de Dados Amazonas S.A.**, doravante designada **CONTRATANTE**, pessoa jurídica de direito privado, sociedade de economia mista, criada pela Lei nº 941, de 10/07/1970, com seus atos constitutivos registrados na Junta Comercial do Estado do Amazonas, sob o nº 13300001038, e com inscrição estadual nº 05.341.162-5,inscrição municipal nº 673801 e C.N.P.J. nº 04.407.920/0001-80, neste ato representada por seu Diretor-Presidente, Sr. **XXXXXXXXXXXXXXXXXXXXXXXXXXXXX**, nacionalidade, estado civil, profissão, portador da Cédula de Identidade nº XXXX XXXXX/XX e do CPF nº XXX.XXX.XXX-XX, residente e domiciliado XXXXXXXXXXXXX, no uso das atribuições que lhe confere o Estatuto Social, em seu artigo 34, inciso XVI, conforme atesta a Ata de da Reunião Extraordinária do Conselho de Administração PRODAM, datada de 04/01/2019 e registrada na JUCEA sob o nº 977468, e de outro lado, a **XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.**, doravante designada simplesmente **CONTRATADA**, com sede em XXXXXXXX, na XXXXXXXXXXXX, nº XXX, Bairro XXXXXXXXXXXXXXXXX, CEP: XXXXXXX, XXXXXX/XX, inscrita no CNPJ nº XX.XXX.XXX/XXXX-XX, inscrição municipal nº 63031-01, neste ato representada por XXXXXXXXX, Sr**. XXXXXXXXXXXXXXXXXXXXXXXXXXXXX**, nacionalidade, estado civil, profissão, portador da Cédula de Identidade nº XXXX XXXXX/XX e do CPF nº XXX.XXX.XXX-XX, residente e domiciliado XXXXXXXXXXXXX, tendo em vista o que consta no Procedimento de Licitação, Pregão Eletrônico SRP nº 11/2022, tudo em conformidade Lei nº 13.303, de 30.06.2016, Decreto nº 10.024, de 20.09.2019 Decreto Estadual nº 39.032, de 24.05.2018, Lei nº 10.520, de 17.07.2002, Lei Complementar nº 123, de 14.12.2006, Decreto Estadual nº 21.178, de 27.09.2000, Decreto Estadual nº 24.818, de 27.01.2005, e alterações e RILC - Regulamento Interno de Licitações e Contratos da PRODAM, aplicando-se subsidiariamente as disposições estabelecidas no

presente instrumento convocatório e seusAnexos, resolvem as partes celebrar o presente Contrato, doravante simplesmente denominado **"CONTRATO**", que se regerá de acordo com as seguintes cláusulas e condições, abaixo descritas, mutuamente aceitas e reciprocamente outorgadas, por si e sucessores:

CLÁUSULA PRIMEIRA: DO OBJETO CONTRATADO

1.1 Fornecimento de Solução de Segurança Avançada para *Endpoints* e Servidores, com proteção integrada contra ataques complexos, direcionados e descoberta avançada de ameaças em nível de rede, com capacidade de respostas automatizadas a incidentes, bem como serviços de instalação, configuração, treinamento, serviços de consultoria e suporte técnico em sistemas de segurança na solução fornecida para prevenção de vírus de computador, *spywares*, APT e outras ameaças.

CLÁUSULA SEGUNDA: DAS CARACTERISTICAS E ESPECIFICAÇÕES DO OBJETO

2.1 A solução deverá atender as especificações contidas no item 7 do Termo de Referência do Edital do Pregão Eletrônico SRP nº 11/2022, parte integrante deste contrato.

2.2 Contratação das Licenças (ITENS 1 A 5 do Termo de Referência do Edital do Pregão Eletrônico SRP nº 11/2022)

2.2.1 A contratação das licenças será por demanda e conveniência da CONTRATANTE através da emissão de Pedido de Compra – PC, vinculado ao respectivo Contrato;

2.2.2 Todas as licenças devem possuir validade de 36 meses;

2.2.3 O prazo de entrega das licenças será de até 15 dias corridos;

2.3 Contratação de Treinamento (ITEM 6 do Termo de Referência do Edital do Pregão Eletrônico SRP nº 11/2022)

2.3.1 A contratação dos treinamentos será por demanda e conveniência da CONTRATANTE através da emissão de Autorização de Execução de Serviço – AES, vinculada ao respectivo contrato, informando o quantitativo de treinamento solicitados;

2.3.2 O calendário de aplicação dos agendamentos deve ser definido em reunião entre o gestor de contrato da CONTRATANTE e o preposto da CONTRATADA;

2.4 Contratação de serviço de consultoria e suporte técnico na solução de proteção avançada (ITEM 7 do Termo de Referência do Edital do Pregão Eletrônico SRP nº 11/2022)

2.4.1 A contratação do serviço de consultoria e suporte técnico será por demanda e conveniência da CONTRATANTE através da emissão de Autorização de Execução de Serviço – AES, vinculada ao respectivo contrato, informando o quantitativo de horas solicitadas;

2.4.2 Deverá ser acordado, em reunião específica, entre o Gestor de Contratos da CONTRATANTE e o preposto da CONTRATADA o cronograma de entrega dos serviços demandados para execução;

2.5 A atividade de fiscalização será realizada para assegurar o efetivo cumprimento das

obrigações contratuais assumidas e a qualidade dos serviços prestados à CONTRATANTE;

2.6 Para tanto, o fiscal a ser designado pela CONTRATANTE deverá:

2.6.1 Acompanhar, fiscalizar e atestar a execução dos serviços contratados;

2.6.2 Indicar as eventuais glosas das faturas;

2.6.3 Informar à Administração da CONTRATANTE o eventual descumprimento dos compromissos pactuados, que poderá ensejar a aplicação de penalidades;

2.7 Em audiência inaugural do contrato serão apresentados, por parte da CONTRATADA, o preposto indicado e, por parte da CONTRATANTE, o fiscal que fará o acompanhamento e a fiscalização da execução do contrato;

2.8 Nessa audiência serão definidos e formalizados os protocolos de comunicação entre a CONTRATANTE e CONTRATADA, para efeito da fiscalização do contrato;

2.9 Serão ainda ratificados os procedimentos decorrentes deste Contrato para:

2.9.1 Emissão das Autorizações para Execução de Serviço;

2.9.2 Verificação do atendimento dos requisitos estabelecidos neste Contrato;

2.9.3 Atestação das faturas;

2.9.4 Descontos, multas e aplicação das demais sanções previstas;

2.9.5 Renovação do contrato;

2.9.6 Encerramento do contrato.

CLÁUSULA TERCEIRA: DAS CONDIÇÕES DE GARANTIA E SUPORTE

3.1 A CONTRADA deverá cumprir com as garantias solicitadas no Termo de Referência do Edital do Pregão Eletrônico SRP nº 11/2022, parte integrante deste contrato;

CLÁUSULA QUARTA: DO REGIME DE EXECUÇÃO DO CONTRATO

4.1 Os serviços ora contratados serão executados sob o regime de empreitada por preço unitário.

CLÁUSULA QUINTA: DO PREÇO DOS SERVIÇOS

5.1 O valor Global do objeto contratado é de R$ XXXXXXX (XXXXXXXXXXXXXX) que será da apuração do produto da quantidade demandada de itens da Ata de Registro de Preços nº xx/20xx, conforme quadro abaixo:

ITEM	DESCRIÇÃO	Unidade	Quantidade	Valor unitáro	Valor total

1	Aquisição de Licenças da Solução de Proteção Avançada para *Endpoints* e Servidores Físicos com validade de 36 meses	Licença	20.000		
2	Aquisição de Licenças da Solução de Proteção Avançada para Ambientes Virtuais com validade de 36 meses	Licença	1.000		
3	Aquisição de Licenças da Solução de Proteção para Mobile com validade de 36 meses	Licença	1.000		
4	Aquisição de Licença da Solução de descoberta avançada de ameaças em nível de rede, com capacidade de análise de até 1 Gbit/s de Throughput, com validade de 36 meses	Licença	1		
5	Aquisição de Licença de Plataforma automatizada de conscientização em Segurança da Informação com validade de 36 meses	Usuário	2.500		
6	Treinamentos				
6.1	Serviço de treinamento da Soluçãode Proteção	Turma	4		
6.2	Serviço de treinamento para resposta à incidentes	Turma	1		
7	Serviço de Consultoria e SuporteTécnico na Solução de ProteçãoAvançada	Hora	2.100		

5.2 O pagamento será efetuado mediante apresentação da Nota Fiscal/Fatura, sendo:

5.2.1 No caso de serviços prestados por banco de horas e/ou treinamento será considerado os serviços efetivamente prestados, que ocorrerá até o 15º (décimo quinto) dia útil do mês subsequente, com os descontos legais (retenções) do serviço apurados para o mês faturado;

5.2.2 Para casos referentes a entrega de produtos (licenças de software) o pagamento será integral a quantidade adquirida para 36 meses e ocorrerá até o 15º (décimo quinto) dia útil do mês subsequente, com os descontos legais (retenções) no mês seguinte a entrega do produto;

5.3 É condição obrigatória para a realização do pagamento, que a contratada apresente a

Nota Fiscal do objeto licitado para que a contratante realize o pagamento no prazo de 30 (trinta) dias, devidamente atestada pelo fiscal e mediante comprovação de regularidade para com as Fazendas Federal, Estadual e Municipal, com a Seguridade Social e com o FGTS.

5.4 O pagamento será de acordo com a apuração da quantidade de licenças solicitadas pelo Pedido de Compra – PC ou serviços demandados por Autorização de Execução de Serviço – AES;

5.5 A solicitação de mais licenças poderá ser realizada em qualquer momento.

5.6 O valor a ser pago pelo consumo dos itens 1 a 5, será calculado de acordo com a regra abaixo:

5.6.1 Valor a pagar = Quantidade de licenças adquiridas x Valor unitário de cada licença;

5.7 Para os serviços de treinamento item 6:

5.7.1 Valor a Pagar = Quantidade de turmas com treinamento concluído x Valor unitário de cada treinamento;

5.8 Para os serviços de consultoria item 7:

5.8.1 O valor será pago após a conclusão do serviço e corresponde à quantidade de horas demandadas e entregues, multiplicadas pelo valor unitário da hora, como descrito abaixo:

5.8.1.1 Valor a pagar = ∑ de horas entregues x Valor unitário da hora;

5.8.2 A quantidade de horas demandadas será definida na Autorização de Execução de Serviço–AES;

CLÁUSULA SEXTA: DO REAJUSTAMENTO

6.1 A CONTRATADA poderá solicitar revisão dos preços dos itens deste Contrato durante o aniversário do mesmo, com base no Índice de Custo de Tecnologia da Informação (ICTI) acumulado de 12 (doze) meses, calculado e divulgado pelo Instituto de Pesquisa Econômica Aplicada (IPEA).

CLÁUSULA SÉTIMA: DO PRAZO DA PRESTAÇÃO DOS SERVIÇOS

7.1 O prazo da prestação dos serviços ora contratados é de **36 (trinta e seis) meses**, contados a partir do dia **xx/xx/20xx até xx/xx/20xx**, podendo ser prorrogado mediante justificativa por escrito e prévia autorização da **CONTRATANTE**, por iguais e sucessivos períodos, se conveniente para a Administração, até o limite de 60 (sessenta) meses, nos termos do art. 71 da Lei nº 13.303/2016 e legislação pertinente;

7.2 De comum acordo, as partes poderão suspender a execução do objeto deste contrato, quando, justificadamente, por motivo imperioso e extraordinário, se fizer necessário;

7.3 A suspensão será formalizada através de Termo Aditivo ou Apostila, onde será definida a expectativa de prazo do reinício da execução, bem como dos correspondentes pagamentos, devendo, quando aplicável, ser firmado novo Cronograma de execução.

CLÁUSULA OITAVA: DOS RECURSOS FINANCEIROS

8.1 As despesas com a execução do presente Contrato correrão por recursos financeiros próprios da **CONTRATANTE**.

CLÁUSULA NONA: DAS OBRIGAÇÕES DA CONTRATADA

9.1 A contratada deve cumprir todas as obrigações constantes neste Contrato e seus anexos, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto e, ainda;

9.2 Manter, durante toda execução do contrato, compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas;

9.3 Ter pleno conhecimento de todas as condições e peculiaridades inerentes aos serviços objeto deste Termo, não podendo invocar, posteriormente, desconhecimento para cobrança de serviços extras;

9.4 Executar os serviços e concluir todos os serviços contratados nos prazos estabelecidos neste Termo e nas Ordens de Serviço;

9.5 Responsabilizar-se integralmente pela sua equipe técnica, primando pela qualidade, desempenho, eficiência e produtividade, visando à execução dos trabalhos durante todo o Contrato, dentro dos prazos estipulados, sob pena de ser considerada infração passível de aplicação de penalidades previstas, caso os prazos e condições não sejam cumpridas;

9.6 Fornecer, sem custos adicionais para o Contratante, quaisquer atualizações de patches, releases e novas versões dos softwares, durante a vigência da garantia contratual;

9.7 Comunicar a CONTRATANTE, por escrito, quaisquer anormalidades que ponham em risco o êxito e o cumprimento dos prazos da execução dos serviços, propondo as ações corretivas necessárias para a execução dos mesmos;

9.8 Atender às solicitações emitidas pela Fiscalização quanto ao fornecimento de informações e/ou documentação;

9.9 A empresa deverá apresentar, obrigatoriamente, comprovação de que possui em seu quadro técnico, no mínimo, 1 (um) profissional com a certificação técnica do fabricante. Esta exigência se faz necessário dado a complexidade do projeto.

CLÁUSULA DÉCIMA: DAS OBRIGAÇÕES DA CONTRATANTE

10.1 Exigir o cumprimento de todas as obrigações assumidas pela Contratada, de acordo com as cláusulas contratuais e os termos de sua proposta;

10.2 Exercer o acompanhamento e a fiscalização dos serviços, por servidor especialmente designado, anotando em registro próprio as falhas detectadas, indicando dia, mês e ano, bem como o nome dos empregados eventualmente envolvidos, e encaminhando os apontamentos à autoridade competente para as providências cabíveis;

10.3 Notificar a Contratada por escrito da ocorrência de eventuais imperfeições no curso da execução dos serviços, fixando prazo para a sua correção;

10.4 Além dos contratos administrativos, o CONTRATANTE não aceitará assinar contratos com o FABRICANTE para o recebimento das licenças decorrentes deste processo, ficando a CONTRATADA obrigada a efetuar os seus pedidos cientes desta condição, bem como comprovar através do site do fabricante que as licenças adquiridas estão devidamente registradas no nome do CONTRATANTE.

CLÁUSULA DÉCIMA PRIMEIRA: DAS PENALIDADES CABÍVEIS

11.1 O serviço a ser prestado deverá seguir as especificações contidas neste Contrato e do Anexo 1 – Termo de Referência, do Edital Pregão Eletrônico SRP nº 11/2022.

11.2 Além das penalidades legalmente previstas e sem prejuízo das mesmas, a CONTRATADA ficará sujeita às sanções a seguir relacionadas:

a) Advertência;

b) Multa de 10% (dez por cento) sobre o valor do contrato na hipótese de perda de dados, utilização indevida dos mesmos ou falha que possibilite a utilização dos dados por terceiros não autorizados, respondendo adicionalmente por perdas e danos pertinentes;

c) Pela rescisão do contrato por iniciativa da CONTRATADA, sem justa causa, multa de 10% (dez por cento) do valor total atualizado do contrato, sem prejuízo do pagamento de outras multas que já tenham sido aplicadas e de responder por perdas e danos que a rescisão ocasionar à CONTRATANTE;

d) Suspensão temporária de participação em licitação e impedimento de contratar com a CONTRATANTE pelo prazo de até 02 (dois) anos;

e) Valor da multa, apurado após regular procedimento administrativo, será descontado dos pagamentos eventualmente devidos pela CONTRATANTE, da Garantia ou cobrados judicialmente;

11.3 A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa à Contratada.

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

CLÁUSULA DÉCIMA SEGUNDA: DOS RECURSOS

12.1 A **CONTRATADA**, notificada da sanção que poderá lhe ser aplicada, terá o prazo de 5 (cinco) dias úteis, a contar do recebimento da Notificação, para apresentar defesa prévia;

12.2 Contra as decisões que tiveram aplicado penalidades, a **CONTRATADA** poderá, sempre com efeito suspensivo:

i. Interpor recursos para a autoridade imediatamente superior, no prazo de 5 (cinco) dias úteis da ciência que tiver da decisão que aplicar as penalidades de advertência e de multa;

ii. Interpor recursos para a autoridade imediatamente superior, no prazo de 5 (cinco)

dias úteis da ciência de publicação no Diário Oficial da decisão de suspensão do direito de licitar, impedimento de contratar ou rescindir administrativamente o contrato;

iii. Formular pedido de reconsideração à autoridade que aplicou a sanção de declaração de inidoneidade para licitar ou contratar, no prazo de 10 (dez) dias úteis da publicação no Diário Oficial do Estado.

12.3 A autoridade competente, ouvida a FISCALIZAÇÃO, decidirá pela procedência ou não do Recurso. A decisão deverá ser comunicada à **CONTRATADA**;

CLÁUSULA DÉCIMA TERCEIRA: DA RESCISÃO

13.1 Constituem motivos para a rescisão do presente contrato:

13.1.1 UNILATERALMENTE, pela CONTRATANTE em razão:

13.1.1.1 do não cumprimento por parte da CONTRATADA de cláusulas contratuais, especificações ou prazos;

13.1.1.2 do cumprimento irregular de cláusulas contratuais, especificações ou prazos;

13.1.1.3 da lentidão do seu cumprimento, levando a PRODAM a comprovar a impossibilidade da conclusão da obra, do serviço ou do fornecimento, nos prazos estipulados;

13.1.1.4 do atraso injustificado no início da prestação dos serviços;

13.1.1.5 da paralisação dos serviços sem justa causa e prévia comunicação à CONTRATANTE;

13.1.1.6 da subcontratação feita contrariamente ao artigo 78 da Lei nº 13.303, de 30 de junho de 2016, assim como a associação do fornecedor com outrem, a cessão ou transferência, total ou parcial, bem como a fusão, cisão ou incorporação, quando não admitidas no instrumento convocatório e no contrato ou, quando admitidas, se causarem prejuízo à execução do contrato;

13.1.1.7 do desatendimento das determinações regulares da FISCALIZAÇÃO ou de seus superiores;

13.1.1.8 do cometimento reiterado de faltas na sua execução, anotadas pelo Gestor ou Fiscal do contrato;

13.1.1.9 da decretação de falência ou a instauração de insolvência civil;

13.1.1.10 da dissolução da sociedade ou o falecimento do contratado;

13.1.1.11 de alteração social ou de modificação da finalidade ou da estrutura da empresa que prejudique a execução do contrato;

13.1.1.12 de interesse público, ou pela ocorrência de caso fortuito ou de força maior, regularmente comprovada, impeditiva da execução deste contrato.

13.1.2 AMIGAVELMENTE pelas partes, desde que haja conveniência para a CONTRATANTE;

13.1.3 JUDICIALMENTE, nos termos da legislação em vigor.

13.2 A rescisão de que trata o item 13.1.1, desta cláusula, será determinada por ato unilateral e escrito da CONTRATANTE, não cabendo à CONTRATADA indenização de qualquer natureza.

13.3 A declaração de rescisão administrativa, precedida de autorização escrita e fundamentada da autoridade competente, será sempre feita independentemente de prévia notificação ou interpelação judicial ou extrajudicial e operará seus efeitos a partir da publicação do ato administrativo no órgão de divulgação oficial estadual.

13.4 A rescisão amigável, precedida de autorização escrita e fundamentada da autoridade competente, será reduzida a termo no processo administrativo.

13.5 Qualquer um desses casos de rescisão contratual serão formalmente motivados nos autos do processo, assegurado o CONTRADITÓRIO e a AMPLA DEFESA.

13.6 Os casos fortuitos e/ou motivos de força maior serão excludentes da responsabilidade das Partes de acordo com o disposto no artigo 393 do Código Civil Brasileiro;

13.7 A CONTRATADA DEVERÁ se responsabilizar por quaisquer prejuízos advindos de não cumprimento dos serviços contratados, isentando a CONTRATANTE de quaisquer responsabilidades de seus atos; e ainda estará sujeita a todas as multas e penalidades legais previstas neste Contrato e na legislação vigente.

CLÁUSULA DÉCIMA QUARTA: DO RECONHECIMENTO DOS DIREITOS DA CONTRATANTE

14.1 As causas de rescisão previstas neste Instrumento acarretam, no que couber, as seguintes consequências, sem prejuízo das sanções pertinentes, reconhecendo a **CONTRATADA**, desde já, os direitos da **CONTRATANTE** de:

i. Assunção imediata do objeto deste contrato no estado em que se encontrar, por ato seu;

ii. Ocupação e utilização dos equipamentos, material e pessoal empregados na execução do contrato, necessários à sua continuidade, os quais serão devolvidos ou ressarcidos posteriormente, mediante avaliação, inclusive na hipótese da necessidade de acautelar apuração administrativa de faltas contratuais da **CONTRATADA**;

iii. Retenção dos créditos decorrentes do contrato, até o limite dos prejuízos causados à **CONTRATANTE**.

CLÁUSULA DÉCIMA QUINTA: DAS ALTERAÇÕES DO PRESENTE CONTRATO

15.1 O Presente Contrato poderá ser alterado conforme artigo 81 da lei nº 13.303 de 30 de junho de 2016.

15.2 As alterações poderão ser realizadas por Termos Aditivos.

15.3 Nenhuma alteração poderá ser realizada sem o acordo da **CONTRATANTE** e **CONTRATADA**, vedado a alteração que viole a obrigação de nova licitação.

CLÁUSULA DÉCIMA SEXTA: DO CONTROLE

16.1 A **CONTRATANTE** providenciará, nos prazos legais, a remessa de informações do presente contrato via sistema ao **TRIBUNAL DE CONTAS DO ESTADO DO AMAZONAS.**

CLÁUSULA DÉCIMA SÉTIMA: DA DOCUMENTAÇÃO

17.1 A **CONTRATADA** fica obrigada a manter, durante toda a vigência do Contrato, em compatibilidade com as obrigações por ela assumidas, inclusive na possibilidade de renovação contratual, todas as condições de habilitação e qualificação exigidas na Licitação.

CLÁUSULA DÉCIMA OITAVA: DA MATRIZ DE RISCO

18.1 A seguir relacionamos os riscos inerentes à contratação dos objetos deste Contrato:

Descrição	Impacto	Responsável	Prazo p/ ajustes	Tratativa / Penalidade
Não cumprimento de cláusulas contratuais	Alto	CONTRATADA ou CONTRATANTE	72h	Sanções conforme TR, CONTRATO e/ou legislação em vigor.
Falha ou ausência de parte na entrega de qualquer Etapa do Objeto	Alto	CONTRATADA	72h	Suspensão do pagamento da NF até entrega total da Etapa do Objeto.
Descumprimento dos prazos na execução dos serviços	Médio	CONTRATADA	72h	Sanções conforme TR, CONTRATO e/ou legislação em vigor.
Denúncia de falha no atendimento	Médio	CONTRATADA	Imediato	Sanções conforme TR, CONTRATO e/ou legislação em vigor.
Qualidade do serviço afetado com baixa performance	Baixo	CONTRATADA	Imediato	Recuperar a qualidade do serviço conforme abertura de chamado.

Legenda:

Impacto alto: suspensão total do serviço por um turno ou mais. A PRODAM poderá disponibilizar recursos próprios para não interromper o fluxo dos serviços. O fornecedor poderá ser punido conforme cláusulas contratuais, caso seja apurada a sua responsabilidade.

Impacto médio: somente parte dos serviços ou parte dos clientes será afetada pela falta da prestação do serviço ou pela falha na prestação do serviço. A PRODAM poderá disponibilizar recursos próprios para não interromper os serviços mais críticos. O fornecedor poderá ser punido conforme cláusulas contratuais, caso seja apurada a sua responsabilidade.

Impacto baixo: o serviço poderá sofrer atraso, mas não será interrompido. A PRODAM não precisará disponibilizar recursos para regularizar o fluxo normal dos serviços. Não há a necessidade de punir o prestador do serviço, a menos que a falta se torne um problema frequente.

Quanto ao disposto nas alíneas “b” e “c” do Art. 42-X (Matriz de Riscos) da Lei

13.303/16 (Lei das Estatais), não há, identificada neste Termo de Referência, qualquer fração do objeto em que haverá liberdade da CONTRATADA para inovar em soluções metodológicas ou tecnológicas, em obrigações de resultado ou em termos de modificação das soluções previamente delineadas neste documento.

CLÁUSULA DÉCIMA NONA: DA FISCALIZAÇÃO

19.1 Será designado representante para acompanhar e fiscalizar a entrega do serviço executado, anotando em registro próprio todas as ocorrências relacionadas com a execução e determinando o que for necessário à regularização de falhas ou defeitos observados.

19.2 A fiscalização de que trata este item não exclui nem reduz a responsabilidade da Contratada, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas ou vícios redibitórios, e, na ocorrência desta, não implica em corresponsabilidade da Administração ou de seus agentes e prepostos.

19.3 O representante da Administração anotará em registro próprio todas as ocorrências relacionadas com a execução do contrato, indicando dia, mês e ano, bem como o nome dos funcionários eventualmente envolvidos, determinando o que for necessário à regularização das falhas ou defeitos observados e encaminhando os apontamentos à autoridade competente para as providências cabíveis.

CLÁUSULA VIGÉSIMA: DO FORO

20.1 O foro do presente contrato é o da capital do Estado do Amazonas, com expressa renúncia dos contratantes de qualquer outro que tenha ou venha a ter, por mais privilegiado que seja.

CLÁUSULA VIGÉSIMA PRIMEIRA: DOS CASOS OMISSOS

21.1 Os casos omissos serão decididos pela **CONTRATANTE**, segundo as disposições contidas na Lei nº 13.303 de 30 de junho de 2016 e demais alterações, pelas normas de Direito Privado e no Regulamento Interno de Licitações e Contratos da PRODAM e demais normas aplicáveis.

CLÁUSULA VIGÉSIMA SEGUNDA: DA PUBLICAÇÃO

22.1 A **CONTRATANTE** deve, nesta data, providenciar a publicação, em forma de extrato, do presente contrato, no Diário Oficial do Estado do Amazonas, na forma do artigo 31 da Lei nº 13.303 de 30 de junho de 2016.

CLÁUSULA VIGÉSIMA TERCEIRA: DAS NORMAS APLICÁVEIS

23.1 O presente contrato rege-se por toda a legislação aplicável à espécie e ainda pelas disposições que a complementarem, alterarem ou regulamentarem, inclusive nos casos omissos, cujas normas, desde já, entendem-se como integrantes do presente termo, especialmente a Lei nº 13.303 de 30 de junho de 2016 e o Regulamento de Licitações e Contratos da **CONTRATANTE**.

23.2 A **CONTRATANTE** e a **CONTRATADA** declaram conhecer todas essas normas e

concordam em sujeitar-se às estipulações, sistemas de penalidades e demais regras delas constantes, mesmo que não expressamente transcritas no presente instrumento.

23.3 De tudo, para constar, foi lavrado o presente termo, em 02 (duas) vias de igual teor e forma, na presença das testemunhas abaixo, para que produza seus legítimos e legais efeitos.

Manaus, XX de XXXX de 20xx

Pela CONTRATANTE **Pela CONTRATADA**

TESTEMUNHAS:

REVISÃO E APROVAÇÃO:
Assessor Jurídico

PREGÃO ELETRÔNICO SRP Nº 11/2022

ANEXO 7-A – ANEXO DA MINUTA DE CONTRATO

TERMO DE RESPONSABILIDADE E CONFIDENCIALIDADE PARA FORNECEDORES E PARCEIROS

Considerando:

(i) a intenção das partes de realizar acordo comercial ou acordo de cooperação técnica a título oneroso ou não oneroso;

(ii) a possibilidade de que a CONTRATADA tenha acesso a informações confidenciais técnicas e ou estratégicas das quais a CONTRATANTE é proprietária e ou custodiante;

(iii) a necessidade, da CONTRATANTE, de resguardar a segurança de tais informações, garantindo sua confidencialidade; e

(iv) a necessidade, da CONTRATANTE, de estabelecer regras para o manuseio e tratamento de tais informações, bem com definir o modo como estas poderão ser usadas e deverão ser protegidas.

Resolvem, na presença das testemunhas adiante nominadas, firmar o presente instrumento, vinculado ao [contrato, acordo, convênio ou ajuste], com os seguintes termos e condições:

DO OBJETO

CLÁUSULA PRIMEIRA. O objeto deste Termo é a proteção de informações confidenciais disponibilizadas pela CONTRATANTE em razão da celebração de contrato para prestação de serviços com a CONTRATADA.

DAS DEFINIÇÕES

CLÁUSULA SEGUNDA. Para os fins deste instrumento, considera-se:

(i) CONTRATO: todo e qualquer ajuste entre órgãos ou entidades da Administração Pública e particulares, em que haja acordo de vontades para a formação de vínculo e estipulação de obrigações recíprocas, seja qual for a denominação utilizada;

(ii) CONTRATANTE: órgão ou entidade da Administração Pública signatária do instrumento contratual;

(iii) CONTRATADA: pessoa física ou jurídica signatária de contrato com a Administração

Pública;

(iv) INFORMAÇÃO DA CONTRATANTE: qualquer informação, elaborada ou não por parte da CONTRATADA, ou ainda, revelada pela CONTRATANTE à CONTRATADA, que esteja relacionada às atividades de prestação de serviços à CONTRATANTE, seus clientes ou fornecedores e das quais a CONTRATANTE seja proprietária e ou custodiante, e que por determinação legal seja classificada como “dados pessoais” ou confidenciais.

CLÁUSULA TERCEIRA. Não são consideradas informações da CONTRATANTE:

(i) habilidades gerais, ou experiência adquirida durante o período da execução do contrato ao qual este Termo está vinculado, quando a CONTRATADA poderia razoavelmente ter tido a expectativa de adquiri-las em situação similar ou prestando serviços a outras empresas;

(ii) informação conhecida publicamente sem a violação deste Termo ou de instrumentos similares; ou

(iii) informação cuja revelação seja exigida por lei ou regulamento, autoridade governamental ou judiciária, devendo a CONTRATADA providenciar para que, antes de tal revelação, seja a CONTRATANTE notificada da exigência (dentro dos limites possíveis diante das circunstâncias) e lhe seja proporcionada oportunidade de discuti-la.

DA INEXISTÊNCIA DE OBRIGAÇÕES CONFLITUOSAS

CLÁUSULA QUARTA. A CONTRATADA declara que:

(i) o cumprimento de seus deveres como prestadora de serviços da CONTRATANTE não violará nenhum acordo ou outra obrigação de manter informações de propriedade de terceiros, não importando a natureza de tais informações;

(ii) não está vinculada a nenhum acordo ou obrigação com terceiros, o qual esteja ou possa estar em conflito com as obrigações assumidas perante a CONTRATANTE ou que possa afetar os interesses desta nos serviços por ela realizados; e

(iii) não trará ao conhecimento de qualquer empregado, administrador ou consultor da CONTRATANTE informações confidenciais – técnicas e ou estratégicas – de propriedade de terceiros, bem como não utilizará tais informações enquanto persistir qualquer espécie de vínculo contratual entre a CONTRATANTE e a CONTRATADA e mesmo após encerrado este vínculo.

DA INFORMAÇÃO DA CONTRATANTE

CLÁUSULA QUINTA. Para os propósitos deste Termo, toda e qualquer informação da CONTRATANTE repassada à CONTRATADA, por qualquer meio, durante a execução dos

serviços contratados, constitui informação privilegiada e, como tal, tem caráter de estrita confidencialidade, e que por determinação legal seja classificada como “dados pessoais” ou confidenciais, só podendo ser utilizada para fins de execução do contrato ao qual este Termo é vinculado.

CLÁUSULA SEXTA. Para os propósitos deste Termo, toda e qualquer informação incluída para processamento pela CONTRATANTE no sistema da CONTRATADA é e permanecerá de propriedade exclusiva da CONTRATANTE. Essa informação será tratada e protegida como tal, de acordo com o estabelecido neste Termo e legislação pertinente e que por determinação legal seja classificada como “dados pessoais” ou confidenciais.

CLÁUSULA SÉTIMA. Como consequência do conhecimento de informação da CONTRATANTE, a CONTRATADA deverá guardar segredo a respeito dos negócios realizados, obrigando-se desde já a:

(i) não destruir, usar, copiar, transferir ou revelar a nenhuma pessoa ou entidade qualquer informação da CONTRATANTE, sem a sua prévia e expressa autorização;

(ii) tomar todas as precauções razoáveis para impedir a destruição, uso, cópia, transferência ou revelação inadvertida de qualquer informação da CONTRATANTE;

(iii) providenciar a devolução de todas as informações da CONTRATANTE, em qualquer meio em que estiverem armazenadas, que estejam sob sua posse e controle, dentro do prazo de 05 (cinco) dias úteis, a contar da data da extinção do vínculo contratual.

CLÁUSULA OITAVA. É expressamente vedado à CONTRATADA repassar qualquer informação da CONTRATANTE, inclusive a terceiros contratados para executar atividades decorrentes do contrato ao qual este Termo está vinculado, exceto mediante autorização prévia e expressa da CONTRATANTE, ou quando amparada por Lei ou determinação Judicial.

DAS DISPOSIÇÕES GERAIS

CLÁUSULA NONA. A CONTRATADA declara-se inteiramente responsável pelos atos praticados por seus empregados, durante e após a execução do contrato ao qual este Termo está vinculado, que impliquem no descumprimento de suas cláusulas.

CLÁUSULA DÉCIMA. **CLÁUSULA DÉCIMA**. As obrigações da CONTRATADA produzirão efeitos a partir da data da assinatura do instrumento contratual ao qual este Termo está vinculado. Qualquer violação ou ameaça de violação a este Termo irá constituir justa causa para imediata rescisão do contrato de prestação de serviços firmado, assegurados a ampla defesa e o contraditório. A rescisão não exime o infrator das penalidades previstas nos artigos 927 e seguintes do Código Civil, artigos 153 e 154 do Código Penal, assegurado o contraditório garantido pelo artigo 5º, inciso IV, da Constituição Federal da República.

CLÁUSULA DÉCIMA PRIMEIRA. As obrigações da CONTRATADA derivadas deste Termo permanecerão em vigor e produzirão seus regulares efeitos pelos próximos 5 anos ou por prazo determinado por lei, mesmo após a extinção do contrato ao qual este Termo está vinculado, conforme cada uma de suas disposições, continuando válidas e com efeito, a despeito de qualquer violação de suas cláusulas ou do contrato de prestação de serviços firmado.

CLÁUSULA DÉCIMA SEGUNDA. A CONTRATADA compromete-se a treinar os seus empregados envolvidos na prestação dos serviços à CONTRATANTE, de forma a que os mesmos estejam comprometidos e aptos a resguardar toda e qualquer informação da CONTRATANTE, nas condições estabelecidas neste Termo.

CLÁUSULA DÉCIMA TERCEIRA. A omissão ou tolerância da CONTRATANTE em exigir da CONTRATADA o estrito cumprimento das condições deste Termo não constituirá novação ou renúncia, nem afetará os seus direitos, que poderão ser exercidos a qualquer tempo.

CLÁUSULA DÉCIMA QUARTA. As Partes elegem o foro da Comarca de Manaus, Capital do Estado do Amazonas, para dirimir quaisquer dúvidas originadas do presente Termo, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

E, por assim estarem de acordo, assinam o presente instrumento em 02 (duas) vias de igual teor e para um só efeito, na presença de 02 (duas) testemunhas.

Manaus, _____/_____/_____

_____
PRODAM – Processamento de Dados Amazonas S.A.
CONTRATANTE

_____
[NOME DA EMPRESA CONTRATADA]
CONTRATADA

_____
Nome Testemunha 1
CPF ___.___.___-__

_____
Nome Testemunha 2
CPF ___.___.___-__