



AMAZONAS

GOVERNO DO ESTADO

Nível de Classificação
Público

Grupo de acesso
PÚBLICO

PREGÃO ELETRÔNICO SRP Nº 05/2023

DOCUMENTO DE ORIGEM: SIGED 971/2023-28

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 eventual fornecimento de licenciamento de antivírus Kaspersky para compor “prateleira” de produtos e serviços a serem comercializados pela PRODAM a seus clientes e consumidos pela própria PRODAM, 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 SRP Nº 05/2023

2.1.2 Recebimento das propostas: de 28/06/2023 a 10/07/2023;

2.1.3 Abertura das propostas: dia 10/07/2023 às 10h, de Brasília;

2.1.4 Início da sessão de disputa de preços: dia 10/07/2023 às 10h30, 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



AMAZONAS

GOVERNO DO ESTADO

Nível de Classificação
Público

Grupo de acesso
PÚBLICO

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 05/2023-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.



AMAZONAS

GOVERNO DO ESTADO

Nível de Classificação

Público

Grupo de acesso

PÚBLICO

- 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;



AMAZONAS

GOVERNO DO ESTADO

Nível de Classificação
Público

Grupo de acesso
PÚBLICO

- 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



AMAZONAS

GOVERNO DO ESTADO

Nível de Classificação
Público

Grupo de acesso
PÚBLICO

- 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.

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

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 8 – 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.
- 15.7 O fornecedor que se enquadrar nos limites e valores estabelecidos na Lei Estadual nº 4.370/2018 deverá possuir o Programa de Integridade de Compliance para contratar com a Administração Pública:
 - 15.7.1 Se a empresa possuir o Programa de Integridade implantado deverá apresentar, **no momento da assinatura do contrato**, declaração emitida por empresa legalmente habilitada, informando sua existência nos termos do Art. 9º da citada lei, e a apresentação do checklist (**Anexo 7**) devidamente preenchido.
 - 15.7.2 Caso a empresa não possua o Programa, a implantação deverá ocorrer no prazo de 180 (cento e oitenta) dias corridos, conforme artigo 5º da Lei nº 4.370/2018, contados a partir da data de celebração do contrato, comprovando por meio de declaração, emitida por empresa legalmente habilitada sob pena de multa e rescisão contratual, conforme artigo 6º da lei supracitada.

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



AMAZONAS

GOVERNO DO ESTADO

Nível de Classificação

Público

Grupo de acesso

PÚBLICO

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 Prodram, 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;
 - 20.14.4 **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** – Checklist – Programa de Integridade;
 - 20.14.7 **Anexo 8** – Minuta de Contrato

Manaus (AM), 26 de junho de 2023.

Gilson de Sena da Silva
Pregoeiro

PREGÃO ELETRÔNICO SRP 05/2023

ANEXO 1 – TERMO DE REFERÊNCIA

1. OBJETO DA CONTRATAÇÃO

1.1. Formação de registro de preços para eventual contratação de licenciamento de antivírus Kaspersky para compor “prateleira” de produtos e serviços a serem comercializados pela PRODAM a seus clientes e consumidos pela própria PRODAM.

2. JUSTIFICATIVA

2.1. A PRODAM presta serviço de tecnologia da informação, comunicação e segurança da informação para grande parte dos órgãos do Estado bem como para o setor privado desta forma necessita dispor de ferramentas de segurança da informação para evitar a exploração de vulnerabilidades no ambiente tecnológico de seus clientes 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.

2.2. Esta necessidade pertence a um nicho de mercado o qual a PRODAM busca ampliar sua participação. Isto se dá através de comercialização de soluções capazes de atender as demandas dos seus clientes bem como requisitos técnicos estudados em Provas de Conceito realizadas em seu parque tecnológico.

2.3. 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 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, identificação e resposta a incidentes, sendo desejável que se integre a outras camadas de segurança de rede.

2.4. Portanto, devido as responsabilidades da PRODAM e de seu objetivo comercial, buscase manter altos níveis de proteção para o ambiente de redes de computadores da PRODAM, de seu datacenter e dos seus clientes contratando serviços de proteção de “endpoints” (antivírus).

3. JUSTIFICATIVA DA ESCOLHA DA SOLUÇÃO:

A Lei nº 13.303, de 30 de junho de 2016, em seu Art. 47, estabelece o seguinte:

Art. 47. A empresa pública e a sociedade de economia mista, na licitação para aquisição de bens, poderão:

I - indicar marca ou modelo, nas seguintes hipóteses:

- a) em decorrência da necessidade de padronização do objeto;*
- b) quando determinada marca ou modelo comercializado por mais de um fornecedor constituir o único capaz de atender o objeto do contrato;*

Corroborando com o citado acima, a Súmula 270/TCU, de 11 Abr 12, tem como precedentes os Acórdãos nº 1.547/2004-1ª Câmara; nº 2.984/2008-2ª Câmara; nº 2664/2007-Plenário; nº 1.698/2007-Plenário; nº 1.521/2003-Plenário; nº 322/2002-Plenário; as Decisões nº 516/2002-Plenário e nº 664/2001-Plenário, sendo a mesma aprovada pelo Acórdão nº 0849 – TCU – Plenário, 11 de abril de 2012.

A solução já está implantada em alguns clientes. Uma eventual substituição de marca resultaria não somente no descarte precoce de licenças em plenas condições de uso como envolveria esforços de dimensionamento, projeto, instalação, configuração, customização, remoção e treinamento dos técnicos e analistas de TIC.

A necessidade desta demanda ser de um mesmo fabricante se dá também pela busca iminente por padronização, maior compatibilidade e condições de execução de gerenciamento centralizado.

Adicionalmente, no estudo técnico preliminar foi realizada prova de conceito que evidenciou maior conformidade da solução sugerida. O relatório de testes concluiu que: “A POC, evidenciou que o Kaspersky foi a solução que mais se adaptou ao ambiente do legado computacional da PRODAM (estações mais antigas com o sistema operacional Windows XP, Windows 7 e Windows 8). Foi verificado que não houve comprometimento da performance, tanto nos equipamentos quanto nos sistemas/software. Também foi verificado que esta solução permitiu utilizar a console conforme configuração das necessidades locais.”

Considerando que o software de antivírus reside ativo no sistema para maior proteção, sua forma de funcionamento pode afetar o desempenho do equipamento, o que resulta em degradação da experiência do usuário e consequentemente redução da produtividade do equipamento;

Considerando que nos testes de bancada o produto do fabricante Kaspersky se mostrou mais eficiente para computadores de diversos sistemas operacionais, inclusive sistemas antigos;

Considerando que o universo de clientes a ser alcançado com a comercialização deste produto, onde há grande variedade de Sistemas Operacionais em funcionamento;

Desta forma, recomenda-se que se faça licitação nomeada para compra do produto da fabricante Kaspersky.

4. RESULTADOS ESPERADOS:

- 4.1. Proteger Endpoints e Servidores de camada de proteção contra vírus, malwares e ameaças cibernéticas;
- 4.2. Garantir a integridade das informações sob custódia da empresa; 3.3. Proporcionar facilidade na gestão da solução de segurança dos endpoints e servidores; 3.4. Disponibilizar ambiente para gestão e atualização da solução;
- 4.5. Disponibilizar informações úteis sobre as estações de trabalho e dispositivos móveis;
- 4.6. Gerar dados e informações para maior eficiência das equipes de tratamento e resposta a incidentes com a oferta dos serviços de EDR;
- 4.7. Dar maior agilidade da detecção e eliminação de acesso a arquivos e links infectados;
- 4.8. Dar maior aderência com a legislação e orientações relacionadas à proteção de dados pessoais e a segurança das informações;
- 4.9. Atender a demanda de soluções de endpoint e servidores para os clientes.
- 4.10. Criar uma “prateleira” de produtos de segurança passível de ser ofertada como serviço aos clientes da PRODAM;
- 4.11. Reduzir o tempo de indisponibilidade de serviços computacionais relacionados à ataques cibernéticos;
- 4.12. Redução de custos em escala através de contratação padronizada evitando várias aquisições de produtos incompatíveis e com requisitos diversos;
- 4.13. Redução de custos, simplificando a gestão de segurança para poupar tempo e garantir produtividade e eficiência administrativa;

5. ITENS DE CONTRATAÇÃO:

- 5.1. Tabela de itens para eventual contratação;

| ITEM | DESCRIÇÃO | UNIDADE | QUANTIDADE MÁXIMA |
|------|--|---------|-------------------|
| 1 | Kaspersky Endpoint Detection and Response Optimum – com validade de 36 meses | Licença | 5.000 |
| 2 | Kaspersky Hybrid Cloud Security Enterprise Server – com validade de 36 meses | Licença | 500 |

5.2. O agrupamento dos itens em um lote único, leva em consideração questões técnicas, bem como o ganho de economia em escala, sem prejuízo a ampla competitividade, uma vez que existem no mercado várias revendas autorizadas pelo fabricante da solução, com capacidade de fornecer os itens na forma em que estão agrupados 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”

6. EXECUÇÃO DO CONTRATO E SUA FISCALIZAÇÃO:

6.1. Regime de execução será por empreitada por preço unitário;

6.2. Contratação das licenças:

6.2.1. A contratação das licenças será por demanda e conveniência da CONTRATANTE através da emissão de Pedido de Compra – PC, vinculado ao respectivo Contrato.

6.2.2. Todas as licenças devem oferecer validade, atualizações e suporte de software por 36 meses;

6.2.3. O prazo de entrega das licenças será de até 15 dias corridos;

6.3. A atividade de fiscalização será realizada para assegurar o efetivo cumprimento das obrigações contratuais assumidas e a qualidade dos serviços prestados à CONTRATANTE;

6.4. Para tanto, o fiscal a ser designado pela CONTRATANTE deverá:

6.4.1. acompanhar, fiscalizar e atestar a execução dos serviços contratados;

6.4.2. indicar as eventuais glosas das faturas;

6.4.3. informar à Administração da CONTRATANTE o eventual descumprimento dos compromissos pactuados, que poderá ensejar a aplicação de penalidades.

6.5. 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;

6.6. Nessa audiência serão definidos e formalizados os protocolos de comunicação entre a CONTRATANTE e CONTRATADA, para efeito da fiscalização do contrato;

6.7. Serão ainda ratificados os procedimentos decorrentes deste Termo de Referência para:

- 6.7.1. Emissão dos Pedidos de Compra;
- 6.7.2. Verificação do atendimento dos requisitos estabelecidos no Termo de Referência;
- 6.7.3. Atestação das faturas;
- 6.7.4. Descontos, multas e aplicação das demais sanções previstas;
- 6.7.5. Renovação do contrato;
- 6.7.6. Encerramento do contrato;

7. CONDIÇÕES DE PAGAMENTO:

- 6.1. O pagamento ocorrerá de acordo com a apuração da quantidade de licenças solicitadas pelo Pedido de Compra – PC;
- 6.2. O pagamento será efetuado mediante apresentação da Nota Fiscal/Fatura e ocorrerá até o 15º (décimo quinto) dia útil do mês subsequente, com os descontos legais (retenções).
- 6.3. O valor a ser pago pelo consumo das licenças será calculado de acordo com a regra abaixo:
 - 6.3.1. Valor a pagar = Quantidade de licenças adquiridas * Valor unitário de cada licença;

8. REAJUSTE ANUAL:

- 8.1. A CONTRATADA poderá solicitar revisão dos preços dos itens de contrato em cada aniversário do contrato, 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).
- 8.2. A solicitação será avaliada pela CONTRATANTE;

9. VIGÊNCIA:

- 9.1. A validade da Ata de Registro de Preços será de 12 (doze) meses, a contar da sua publicação;
- 9.2. A vigência dos contratos oriundos das atas será de 36 (trinta e seis) meses, podendo ser prorrogado nos termos da legislação vigente;

10. SANÇÕES ADMINISTRATIVAS:

- 10.1. 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;
- 10.2. Além das penalidades legalmente previstas e sem prejuízo das mesmas, a CONTRATADA ficará sujeita às sanções a seguir relacionadas:

10.2.1. Advertência;

10.2.2. 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;

10.2.3. Suspensão temporária de participação em licitação e impedimento de contratar com a CONTRATANTE pelo prazo de até 02 (dois) anos;

10.3. 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;

10.4. O valor da multa, apurado após regular procedimento administrativo, será descontado dos pagamentos eventualmente devidos pela CONTRATANTE, da Garantia ou cobrados judicialmente;

11. 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 deles;

11.8. Atender às solicitações emitidas pela Fiscalização quanto ao fornecimento de informações e/ou documentação.

12. OBRIGAÇÕES DO CONTRATANTE:

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

12.2. 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;

12.3. Notificar a Contratada por escrito da ocorrência de eventuais imperfeições no curso da execução dos serviços, fixando prazo para a sua correção;

12.4. 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;

13. QUALIFICAÇÃO TÉCNICA:

13.1. Deverá apresentar 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;

13.2. Poderá apresentar tantos atestados de aptidão técnica quantos julgar necessários para comprovar que já executou objeto semelhante ao da licitação;

13.3. 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;

13.4. 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 10% (dez 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;

13.5. Para a assinatura do contrato, 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.



Nível de Classificação
Público

Grupo de acesso
PÚBLICO

14. MATRIZ DE RISCO:

| 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.

15. ESPECIFICAÇÕES TÉCNICAS

15.1. Especificações para o Item 1 – Kaspersky Endpoint Detection and Response Optimum – com validade por 36 meses

15.1.1. Servidor de Administração e Console Administrativa

15.1.1.1. Compatibilidade mínima:

15.1.1.2. Microsoft Windows Server 2008 (Todas edições);

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

15.1.1.4. Microsoft Windows Server 2016 x64

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

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

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

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

15.1.1.9. Microsoft Windows 10 (Todas edições x32);

15.1.1.10. Microsoft Windows 10 (Todas edições x64);

15.1.1.11. Características:

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

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

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

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

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

15.1.1.17. 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;

15.1.1.18. 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;

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

- 15.1.1.20. 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;
- 15.1.1.21. Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria;
- 15.1.1.22. Deve armazenar histórico das alterações feitas em políticas;
- 15.1.1.23. 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;
- 15.1.1.24. Deve ter a capacidade de comparar a política atual com a anterior, informando quais configurações foram alteradas;
- 15.1.1.25. A solução de gerência deve permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas;
- 15.1.1.26. Através da solução de gerência, deve ser possível verificar qual licença está aplicada para determinado computador;
- 15.1.1.27. Capacidade de instalar remotamente a solução de segurança em smartphones e tablets de sistema iOS e Android;
- 15.1.1.28. Capacidade de instalar remotamente qualquer "app" em smartphones e tablets de sistema iOS;
- 15.1.1.29. A solução de gerência centralizada deve permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle;
- 15.1.1.30. 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;
- 15.1.1.31. Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux e Mac) protegidos pela solução antivírus;
- 15.1.1.32. Capacidade de gerenciar smartphones e tablets (Android e iOS) protegidos pela solução de segurança;
- 15.1.1.33. Capacidade de instalar atualizações em computadores de teste antes de instalar nos demais computadores da rede;
- 15.1.1.34. Capacidade de gerar pacotes customizados (auto executáveis) contendo a licença e configurações do produto;
- 15.1.1.35. Capacidade de atualizar os pacotes de instalação com as últimas vacinas;
- 15.1.1.36. 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;

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

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

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

15.1.1.40.Nome do computador;

15.1.1.41.Nome do domínio;

15.1.1.42.Range de IP;

15.1.1.43.Sistema Operacional;

15.1.1.44.Máquina virtual.

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

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

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

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

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

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

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

15.1.1.52.Deve fornecer as seguintes informações dos computadores:

15.1.1.53.Se o antivírus está instalado;

15.1.1.54.Se o antivírus está iniciado;

- 15.1.1.55. Se o antivírus está atualizado;
- 15.1.1.56. Minutos/horas desde a última conexão da máquina com o servidor administrativo;
- 15.1.1.57. Minutos/horas desde a última atualização de vacinas;
- 15.1.1.58. Data e horário da última verificação executada na máquina;
- 15.1.1.59. Versão do antivírus instalado na máquina;
- 15.1.1.60. Se é necessário reiniciar o computador para aplicar mudanças;
- 15.1.1.61. Data e horário de quando a máquina foi ligada;
- 15.1.1.62. Quantidade de vírus encontrados (contador) na máquina;
- 15.1.1.63. Nome do computador;
- 15.1.1.64. Domínio ou grupo de trabalho do computador;
- 15.1.1.65. Data e horário da última atualização de vacinas;
- 15.1.1.66. Sistema operacional com Service Pack;
- 15.1.1.67. Quantidade de processadores;
- 15.1.1.68. Quantidade de memória RAM;
- 15.1.1.69. Usuário(s) logado(s) naquele momento, com informações de contato (caso disponíveis no Active Directory);
- 15.1.1.70. Endereço IP;
- 15.1.1.71. Aplicativos instalados, inclusive aplicativos de terceiros, com histórico de instalação, contendo data e hora que o software foi instalado ou removido;
- 15.1.1.72. Atualizações do Windows Updates instaladas;
- 15.1.1.73. Informação completa de hardware contendo: processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de áudio, adaptadores de rede, monitores, drives de CD/DVD;
- 15.1.1.74. Vulnerabilidades de aplicativos instalados na máquina;
- 15.1.1.75. Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterá-las;
- 15.1.1.76. Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como:
- 15.1.1.77. Alteração de Gateway Padrão;
- 15.1.1.78. Alteração de subrede;
- 15.1.1.79. Alteração de domínio;

- 15.1.1.80.Alteração de servidor DHCP;
- 15.1.1.81.Alteração de servidor DNS;
- 15.1.1.82.Alteração de servidor WINS;
- 15.1.1.83.Alteração de subrede;
- 15.1.1.84.Resolução de Nome;
- 15.1.1.85.Disponibilidade de endereço de conexão SSL;
- 15.1.1.86.Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet;
- 15.1.1.87.Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes;
- 15.1.1.88.Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus;
- 15.1.1.89.Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos;
- 15.1.1.90.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;
- 15.1.1.91.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;
- 15.1.1.92.Capacidade de exportar relatórios para os seguintes tipos de arquivos: PDF, HTML e XML;
- 15.1.1.93.Capacidade de gerar traps SNMP para monitoramento de eventos;
- 15.1.1.94.Capacidade de enviar e-mails para contas específicas em caso de algum evento;
- 15.1.1.95.Listar em um único local, todos os computadores não gerenciados na rede;
- 15.1.1.96.Deve encontrar computadores na rede através de no mínimo três formas: Domínio, Active Directory e subredes;
- 15.1.1.97.Deve possuir compatibilidade com Microsoft NAP, quando instalado em um Windows 2008 Server;
- 15.1.1.98.Capacidade de baixar novas versões do antivírus direto pela console de gerenciamento, sem a necessidade de importá-los manualmente

15.1.1.99. 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;

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

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

15.1.1.102. 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);

15.1.1.103. 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;

15.1.1.104. 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;

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

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

15.1.1.107. Nome do vírus;

15.1.1.108. Nome do arquivo infectado;

15.1.1.109. Data e hora da detecção;

15.1.1.110. Nome da máquina ou endereço IP;

15.1.1.111. Ação realizada.

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

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

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

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

- 15.1.1.116. Capacidade de realizar inventário de hardware de todas as máquinas clientes;
15.1.1.117. Capacidade de realizar inventário de aplicativos de todas as máquinas clientes;
15.1.1.118. Capacidade de diferenciar máquinas virtuais de máquinas físicas.

15.1.2. Software para Estações Windows

15.1.2.1. Compatibilidade mínima:

- 15.1.2.2. Microsoft Windows XP Professional x86;
15.1.2.3. Microsoft Windows Vista x86 / x64 SP2;
15.1.2.4. Microsoft Windows 7 Professional/Enterprise/Ultimate x86 / x64 e posterior;
15.1.2.5. Microsoft Windows 8 Professional/Enterprise x86 / x64;
15.1.2.6. Microsoft Windows 8.1 Pro / Enterprise x86 / x64;
15.1.2.7. Microsoft Windows 10 Pro / Enterprise x86 / x64;
15.1.2.8. Microsoft Windows Server 2012 R2 Standard x64;
15.1.2.9. Microsoft Windows Server 2012 Foundation x64;
15.1.2.10. Microsoft Windows Server 2012 Standard x64;
15.1.2.11. Microsoft Small Business Server 2011 Standard x64;
15.1.2.12. Microsoft Windows Server 2008 R2 Standard/Enterprise x64 SP1;
15.1.2.13. Microsoft Windows Server 2008 Standard/Enterprise x86/x64 SP2;
15.1.2.14. Microsoft Windows Server 2016 x64

15.1.2.15. Características:

- 15.1.2.16. Deve prover as seguintes proteções:
15.1.2.17. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
15.1.2.18. Antivírus de Web (módulo para verificação de sites e downloads contra vírus);
15.1.2.19. Antivírus de E-mail (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos);
15.1.2.20. O Endpoint deve possuir opção para rastreamento por linha de comando, parametrizável, com opção de limpeza;
15.1.2.21. Firewall com IDS;
15.1.2.22. Autoproteção (contra-ataques aos serviços/processos do antivírus);
15.1.2.23. Controle de dispositivos externos;

- 15.1.2.24. Controle de acesso a sites por categoria, ex: Bloquear conteúdo adulto, sites de jogos, etc;
- 15.1.2.25. Controle de acesso a sites por horário;
- 15.1.2.26. Controle de acesso a sites por usuários;
- 15.1.2.27. Controle de acesso a websites por dados, ex: Bloquear websites com conteúdos de vídeo e áudio;
- 15.1.2.28. Controle de execução de aplicativos;
- 15.1.2.29. Controle de vulnerabilidades do Windows e dos aplicativos instalados;
- 15.1.2.30. Capacidade de escolher quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
- 15.1.2.31. 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);
- 15.1.2.32. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;
- 15.1.2.33. 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;
- 15.1.2.34. 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;
- 15.1.2.35. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);
- 15.1.2.36. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
- 15.1.2.37. 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;
- 15.1.2.38. Ter a capacidade de fazer detecções por comportamento, identificando ameaças avançadas sem a necessidade de assinaturas;
- 15.1.2.39. Capacidade de verificar somente arquivos novos e alterados;
- 15.1.2.40. Capacidade de verificar objetos usando heurística;
- 15.1.2.41. Capacidade de agendar uma pausa na verificação;

- 15.1.2.42. Deve permitir a filtragem de conteúdo de URL avançada efetuando a classificação dos sites em categorias;
- 15.1.2.43. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;
- 15.1.2.44. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
- 15.1.2.45. Perguntar o que fazer, ou;
- 15.1.2.46. Bloquear acesso ao objeto;
- 15.1.2.47. Apagar o objeto ou tentar desinfecá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
- 15.1.2.48. Caso positivo de desinfecção:
- 15.1.2.49. Restaurar o objeto para uso;
- 15.1.2.50. Caso negativo de desinfecção:
- 15.1.2.51. Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);
- 15.1.2.52. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
- 15.1.2.53. Capacidade de verificar e-mails recebidos e enviados nos protocolos POP3, POP3S, IMAP, NNTP, SMTP e MAPI;
- 15.1.2.54. Capacidade de verificar links inseridos em e-mails contra phishings;
- 15.1.2.55. Capacidade de verificar tráfego nos browsers: Internet Explorer, Firefox, Google Chrome e Opera;
- 15.1.2.56. Capacidade de verificação de corpo e anexos de e-mails usando heurística;
- 15.1.2.57. O antivírus de e-mail, ao encontrar um objeto potencialmente perigoso, deve:
- 15.1.2.58. Perguntar o que fazer, ou;
- 15.1.2.59. Bloquear o e-mail;
- 15.1.2.60. Apagar o objeto ou tentar desinfecá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
- 15.1.2.61. Caso positivo de desinfecção:
- 15.1.2.62. Restaurar o e-mail para o usuário;
- 15.1.2.63. Caso negativo de desinfecção:
- 15.1.2.64. Mover para quarentena ou apagar o objeto (de acordo com a configuração pré-estabelecida pelo administrador);

- 15.1.2.65. Caso o e-mail conter código que parece ser, mas não é definitivamente malicioso, o mesmo deve ser mantido em quarentena;
- 15.1.2.66. Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados;
- 15.1.2.67. Capacidade de filtrar anexos de e-mail, apagando-os ou renomeando-os de acordo com a configuração feita pelo administrador;
- 15.1.2.68. Capacidade de verificação de tráfego HTTP/HTTPS e qualquer script do Windows Script Host (JavaScript, Visual Basic Script, etc), usando heurísticas;
- 15.1.2.69. Deve ter suporte total ao protocolo Ipv6;
- 15.1.2.70. Capacidade de alterar as portas monitoradas pelos módulos de Web e E-mail;
- 15.1.2.71. Na verificação de tráfego web, caso encontrado código malicioso o programa deve:
- 15.1.2.72. Perguntar o que fazer, ou;
- 15.1.2.73. Bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio, ou;
- 15.1.2.74. Permitir acesso ao objeto;
- 15.1.2.75. O antivírus de web deve realizar a verificação de, no mínimo, duas maneiras diferentes, sob escolha do administrador;
- 15.1.2.76. Verificação on-the-fly, onde os dados são verificados enquanto são recebidos em tempo-real, ou;
- 15.1.2.77. Verificação de buffer, onde os dados são recebidos e armazenados para posterior verificação;
- 15.1.2.78. Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus de web;
- 15.1.2.79. 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;
- 15.1.2.80. Deve possuir módulo que analise cada macro de VBA executada, procurando por sinais de atividade maliciosa;
- 15.1.2.81. 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;
- 15.1.2.82. Deve possuir módulo de bloqueio de Phishing, com atualizações incluídas nas vacinas, obtidas pelo Anti-Phishing Working Group (<http://www.antiphishing.org/>);

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

15.1.2.84. 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;

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

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

15.1.2.87. 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.

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

15.1.2.89. Discos de armazenamento locais;

15.1.2.90. Armazenamento removível;

15.1.2.91. Impressoras;

15.1.2.92. CD/DVD;

15.1.2.93. Drives de disquete;

15.1.2.94. Modems;

15.1.2.95. Dispositivos de fita;

15.1.2.96. Dispositivos multifuncionais;

15.1.2.97. Leitores de smart card;

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

15.1.2.99. Wi-Fi;

15.1.2.100. Adaptadores de rede externos;

15.1.2.101. Dispositivos MP3 ou smartphones;

15.1.2.102. Dispositivos Bluetooth;

15.1.2.103. Câmeras e Scanners.

15.1.2.104. 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;

- 15.1.2.105. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por usuário;
- 15.1.2.106. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por agendamento;
- 15.1.2.107. Capacidade de habilitar “logging” em dispositivos removíveis tais como Pendrive, Discos externos, etc.
- 15.1.2.108. Capacidade de configurar novos dispositivos por Class ID/Hardware ID;
- 15.1.2.109. 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);
- 15.1.2.110. O controle de aplicações deve ter a capacidade de criar regras seguindo os seguintes modos de operação:
- 15.1.2.111. Black list: Permite a execução de qualquer aplicação, exceto pelas especificadas por regras.
- 15.1.2.112. White list: Impede a execução de qualquer aplicação, exceto pelas especificadas por regras.
- 15.1.2.113. Capacidade de bloquear execução de aplicativo que está em armazenamento externo;
- 15.1.2.114. 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;
- 15.1.2.115. 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;
- 15.1.2.116. 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.
- 15.1.2.117. Capacidade de voltar ao estado anterior do sistema operacional após um ataque de malware.
- 15.1.2.118. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros.
- 15.1.2.119. Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning).
- 15.1.2.120. Capacidade de integração com o Windows Defender Security Center.

- 15.1.2.121. Capacidade de integração com a Antimalware Scan Interface (AMSI).
- 15.1.2.122. Capacidade de detecção de arquivos maliciosos executados em Subsistema Windows para Linux (WSL).
- 15.1.2.123. Deve possuir módulo que monitora e bloqueia atividades potencialmente maliciosas, baseado no comportamento do usuário e Machine Learning.
- 15.1.2.124. O módulo deve ser capaz de agir nos seguintes estados:
- 15.1.2.125. Aprendizado: coleta informações sobre as atividades executadas pelo usuário.
- 15.1.2.126. Bloqueio: bloqueia as atividades potencialmente maliciosas que não sejam compatíveis com a rotina do usuário.
- 15.1.2.127. Notificação: notifica sobre as atividades potencialmente maliciosas que não sejam compatíveis com a rotina do usuário.

15.1.3. Software para Estações MacOS X

15.1.3.1. Compatibilidade mínima:

- 15.1.3.2. macOS High Sierra 10.13
- 15.1.3.3. macOS Sierra 10.12
- 15.1.3.4. Mac OS X 10.11 (El Capitan);
- 15.1.3.5. Mac OS X 10.10 (Yosemite);
- 15.1.3.6. Mac OS X 10.9 (Mavericks);

15.1.3.7. Características:

- 15.1.3.8. Deve prover proteção residente para arquivos (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
- 15.1.3.9. Possuir módulo de web-antivírus para proteger contra ameaças durante navegação na internet com possibilidade de analisar endereços https;
- 15.1.3.10. Possuir módulo de bloqueio à ataques na rede;
- 15.1.3.11. Possibilidade de bloquear a comunicação entre a máquina atacante e os demais computadores por tempo definido pelo administrador;
- 15.1.3.12. Capacidade de criar exclusões para computadores que não devem ser monitorados pelo módulo de bloqueio à ataques na rede;
- 15.1.3.13. Possibilidade de importar uma chave no pacote de instalação;
- 15.1.3.14. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;

- 15.1.3.15. Deve possuir suportes a notificações utilizando o Growl;
- 15.1.3.16. 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);
- 15.1.3.17. Capacidade de voltar para a base de dados de vacina anterior;
- 15.1.3.18. Capacidade de varrer a quarentena automaticamente após cada atualização de vacinas;
- 15.1.3.19. 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;
- 15.1.3.20. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);
- 15.1.3.21. 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;
- 15.1.3.22. Capacidade de verificar somente arquivos novos e alterados;
- 15.1.3.23. Capacidade de verificar objetos usando heurística;
- 15.1.3.24. Capacidade de agendar uma pausa na verificação;
- 15.1.3.25. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
- 15.1.3.26. Perguntar o que fazer, ou;
- 15.1.3.27. Bloquear acesso ao objeto;
- 15.1.3.28. Apagar o objeto ou tentar desinfecá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
- 15.1.3.29. Caso positivo de desinfecção:
- 15.1.3.30. Restaurar o objeto para uso;
- 15.1.3.31. Caso negativo de desinfecção:
- 15.1.3.32. Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);
- 15.1.3.33. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
- 15.1.3.34. Capacidade de verificar arquivos de formato de email;



AMAZONAS

GOVERNO DO ESTADO

Nível de Classificação

Público

Grupo de acesso

PÚBLICO

15.1.3.35. 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;

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

15.1.4. Estações de trabalho Linux

15.1.4.1. Compatibilidade:

15.1.4.2. Plataforma 32-Bits:

15.1.4.3. Ubuntu 14.04.5 LTS

15.1.4.4. Ubuntu 16.04.4 LTS

15.1.4.5. Ubuntu 17.10.1

15.1.4.6. Red Hat® Enterprise Linux® 6.9

15.1.4.7. CentOS-6.9

15.1.4.8. Debian GNU/Linux 8.10

15.1.4.9. Debian GNU/Linux 9.4

15.1.4.10. AltLinux 8.0.0

15.1.4.11. AltLinux 8.2*

15.1.4.12. GosLinux 6.6

15.1.4.13. Plataforma 64-Bits:

15.1.4.14. Ubuntu 14.04.5 LTS

15.1.4.15. Ubuntu 16.04.4 LTS

15.1.4.16. Ubuntu 17.10.1

15.1.4.17. Ubuntu 18.04

15.1.4.18. Red Hat® Enterprise Linux® 6.9

15.1.4.19. Red Hat® Enterprise Linux® 7.4

15.1.4.20. CentOS-6.9

15.1.4.21. CentOS-7.4

15.1.4.22. Debian GNU/Linux 8.10

15.1.4.23. Debian GNU/Linux 9.4

15.1.4.24. OracleLinux 7.4

WWW.PRODAM.AM.GOV.BR

Instagram: @prodam_am

Facebook: ProdAmAmazonas

Fone: (92) 2121-6500

Whatsapp: (92) 99115-9496

sacp@prodam.am.gov.br

Rua Jonathas Pedrosa, n°1937.

Praça 14 de Janeiro. Manaus -AM.

CEP 69020-110

PRODAM

15.1.4.25.SUSE® Linux Enterprise Server 12 SP3

15.1.4.26.openSUSE® 42.3

15.1.4.27. Características:

15.1.4.28.Deve prover as seguintes proteções:

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

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

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

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

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

15.1.4.34.Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfetar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;

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

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

15.1.4.37.Alta;

15.1.4.38.Média;

15.1.4.39.Baixa;

15.1.4.40.Recomendado;

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

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

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

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

15.1.4.45. 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;

15.1.4.46. Capacidade de verificar objetos usando heurística;

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

15.1.4.48. Possibilidade de

15.1.4.49. 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).

15.1.5. Servidores Windows

15.1.5.1. Compatibilidade:

15.1.5.2. Plataforma 32-bits:

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

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

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

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

15.1.5.7. Plataforma 64-bits:

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

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

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

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

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

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

15.1.5.14. Microsoft Windows Storage Server 2008 R2;

15.1.5.15. Microsoft Windows Storage Server 2008 SP2 Standard Edition;

15.1.5.16. Microsoft Windows Storage Server SP2 Workgroup Edition;

- 15.1.5.17. Microsoft Windows Hyper-V Server 2008 R2 SP1 e posterior;
- 15.1.5.18. Microsoft Windows Server 2012 Essentials / Standard / Foundation / Datacenter;
- 15.1.5.19. Microsoft Windows Server 2012 R2 Essentials / Standard / Foundation / Datacenter;
- 15.1.5.20. Microsoft Windows Server 2012 Core Essentials / Standard / Foundation / Datacenter;
- 15.1.5.21. Microsoft Windows Server 2012 R2 Core Essentials / Standard / Foundation / Datacenter;
- 15.1.5.22. Microsoft Windows Storage Server 2012 (Todas edições);
- 15.1.5.23. Microsoft Windows Storage Server 2012 R2 (Todas edições);
- 15.1.5.24. Microsoft Windows Hyper-V Server 2012;
- 15.1.5.25. Microsoft Windows Hyper-V Server 2012 R2;
- 15.1.5.26. Windows Server 2016 Essentials/Standard/Datacenter/MultiPoint Premium Server;
- 15.1.5.27. Windows Server 2016 Core Standard / Datacenter;
- 15.1.5.28. Windows Storage Server 2016;
- 15.1.5.29. Windows Hyper-V Server 2016.
- 15.1.5.30. Características:**
- 15.1.5.31. Deve prover as seguintes proteções:
- 15.1.5.32. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
- 15.1.5.33. Auto-proteção contra-ataques aos serviços/processos do antivírus;
- 15.1.5.34. Firewall com IDS;
- 15.1.5.35. Controle de vulnerabilidades do Windows e dos aplicativos instalados;
- 15.1.5.36. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
- 15.1.5.37. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;
- 15.1.5.38. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
- 15.1.5.39. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);

- 15.1.5.40. Gerenciamento de tarefa (criar ou excluir tarefas de verificação);
- 15.1.5.41. Leitura de configurações;
- 15.1.5.42. Modificação de configurações;
- 15.1.5.43. Gerenciamento de Backup e Quarentena;
- 15.1.5.44. Visualização de relatórios;
- 15.1.5.45. Gerenciamento de relatórios;
- 15.1.5.46. Gerenciamento de chaves de licença;
- 15.1.5.47. Gerenciamento de permissões (adicionar/excluir permissões acima);
- 15.1.5.48. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras;
- 15.1.5.49. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;
- 15.1.5.50. 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.
- 15.1.5.51. 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;
- 15.1.5.52. Bloquear malwares tais como Cryptlockers mesmo quando o ataque vier de um computador sem antivírus na rede
- 15.1.5.53. Capacidade de resumir automaticamente tarefas de verificação que tenham sido paradas por anormalidades (queda de energia, erros, etc);
- 15.1.5.54. Capacidade de automaticamente pausar e não iniciar tarefas agendadas caso o servidor esteja rodando com fonte ininterrupta de energia (uninterruptible Power supply – UPS);
- 15.1.5.55. Em caso de erros, deve ter capacidade de criar logs e traces automaticamente, sem necessidade de outros softwares;
- 15.1.5.56. Capacidade de configurar níveis de verificação diferentes para cada pasta, grupo de pastas ou arquivos do servidor;
- 15.1.5.57. Capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado no servidor;
- 15.1.5.58. Capacidade de criar uma lista de máquina que nunca serão bloqueadas mesmo quando infectadas;

- 15.1.5.59. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;
- 15.1.5.60. 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;
- 15.1.5.61. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
- 15.1.5.62. 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;
- 15.1.5.63. Capacidade de verificar somente arquivos novos e alterados;
- 15.1.5.64. Capacidade de escolher qual tipo de objeto composto será verificado (ex: arquivos comprimidos, arquivos auto descompressores, .PST, arquivos compactados por compactadores binários, etc.);
- 15.1.5.65. Capacidade de verificar objetos usando heurística;
- 15.1.5.66. Capacidade de configurar diferentes ações para diferentes tipos de ameaças;
- 15.1.5.67. Capacidade de agendar uma pausa na verificação;
- 15.1.5.68. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;
- 15.1.5.69. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
- 15.1.5.70. Perguntar o que fazer, ou;
- 15.1.5.71. Bloquear acesso ao objeto;
- 15.1.5.72. Apagar o objeto ou tentar desinfecá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
- 15.1.5.73. Caso positivo de desinfecção:
- 15.1.5.74. Restaurar o objeto para uso;
- 15.1.5.75. Caso negativo de desinfecção:
- 15.1.5.76. Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);
- 15.1.5.77. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
- 15.1.5.78. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;



AMAZONAS

GOVERNO DO ESTADO

Nível de Classificação

Público

Grupo de acesso

PÚBLICO

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

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

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

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

15.1.5.83. 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.

15.1.6. Servidores Linux

15.1.6.1. Compatibilidade:

15.1.6.2. Plataforma 32-bits:

15.1.6.3. Red Hat® Enterprise Linux® 6.9 Server

15.1.6.4. CentOS-6.9

15.1.6.5. Ubuntu 14.04.5 LTS

15.1.6.6. Ubuntu 16.04.2 LTS

15.1.6.7. Ubuntu 17.10.1

15.1.6.8. Debian GNU / Linux 8.10

15.1.6.9. Debian GNU / Linux 9.4

15.1.6.10. Plataforma 64-bits:

15.1.6.11. Red Hat® Enterprise Linux® 6.9 Server

15.1.6.12. Red Hat® Enterprise Linux® 7.4 Server

15.1.6.13. Red Hat® Enterprise Linux® 7.5 Server

15.1.6.14. CentOS-6.9

15.1.6.15. CentOS-7.4

15.1.6.16. CentOS-7.5

15.1.6.17. Ubuntu 14.04.5 LTS

15.1.6.18. Ubuntu 16.04.4 LTS

15.1.6.19. Ubuntu 17.10.1

15.1.6.20. Ubuntu 18.04

WWW.PRODAM.AM.GOV.BR

Instagram: @prodam_am

Facebook: ProdAmAmazonas

Fone: (92) 2121-6500

Whatsapp: (92) 99115-9496

sacp@prodam.am.gov.br

Rua Jonathas Pedrosa, n°1937.

Praça 14 de Janeiro. Manaus -AM.

CEP 69020-110

PRODAM

15.1.6.21. Debian GNU / Linux 8.10

15.1.6.22. Debian GNU / Linux 9.4

15.1.6.23. SUSE® Linux Enterprise Server 12 SP3

15.1.6.24. Oracle Linux 7.4

15.1.6.25. SUSE® Linux Enterprise Server 12 SP2

15.1.6.26. OpenSUSE® 42.3

15.1.6.27. Amazon Linux AMI

15.1.6.28. Características:

15.1.6.29. Deve prover as seguintes proteções:

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

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

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

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

15.1.6.34. Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfetar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;

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

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

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

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

15.1.6.39. 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;

15.1.6.40. Capacidade de verificar objetos usando heurística;



- 15.1.6.41. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;
- 15.1.6.42. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;
- 15.1.6.43. Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).

15.1.7. Criptografia

15.1.7.1. Compatibilidade

- 15.1.7.2. Microsoft Windows 7 Ultimate SP1 ou superior x86/x64;
- 15.1.7.3. Microsoft Windows 7 Enterprise SP1 ou superior x86/x64;
- 15.1.7.4. Microsoft Windows 7 Professional SP1 ou superior x86/x64;
- 15.1.7.5. Microsoft Windows 8 Enterprise x86/x64;
- 15.1.7.6. Microsoft Windows 8 Pro x86/x64;
- 15.1.7.7. Microsoft Windows 8.1 Pro x86/x64;
- 15.1.7.8. Microsoft Windows 8.1 Enterprise x86/x64;
- 15.1.7.9. Microsoft Windows 10 Enterprise x86/x64;
- 15.1.7.10. Microsoft Windows 10 Pro x86/x64;
- 15.1.7.11. Microsoft Windows Vista x86/x64 SP2 ou superior;
- 15.1.7.12. Microsoft Windows XP Professional x86 SP3 ou superior

15.1.7.13. Características

- 15.1.7.14. 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;
- 15.1.7.15. Utilizar, no mínimo, algoritmo AES com chave de 256 bits;
- 15.1.7.16. Capacidade de criptografar completamente o disco rígido da máquina, adicionando um ambiente de pré-boot para autenticação do usuário;
- 15.1.7.17. Capacidade de utilizar Single Sign-On para a autenticação de pré-boot;
- 15.1.7.18. Permitir criar vários usuários de autenticação pré-boot;
- 15.1.7.19. Capacidade de criar um usuário de autenticação pré-boot comum com uma senha igual para todas as máquinas a partir da console de gerenciamento;
- 15.1.7.20. Capacidade de criptografar drives removíveis de acordo com regra criada pelo administrador, com as opções:

- 15.1.7.21. Criptografar somente os arquivos novos que forem copiados para o disco removível, sem modificar os arquivos já existentes;
- 15.1.7.22. Criptografar todos os arquivos individualmente;
- 15.1.7.23. Criptografar o dispositivo inteiro, de maneira que não seja possível listar os arquivos e pastas armazenadas;
- 15.1.7.24. Criptografar o dispositivo em modo portátil, permitindo acessar os arquivos em máquinas de terceiros através de uma senha;
- 15.1.7.25. 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;
- 15.1.7.26. Capacidade de criar regras de exclusões para que certos arquivos ou pastas nunca sejam criptografados;
- 15.1.7.27. Capacidade de selecionar aplicações que podem ou não ter acesso aos arquivos criptografados;
- 15.1.7.28. Verifica compatibilidade de hardware antes de aplicar a criptografia;
- 15.1.7.29. Possibilita estabelecer parâmetros para a senha de criptografia;
- 15.1.7.30. Bloqueia o reuso de senhas;
- 15.1.7.31. Bloqueia a senha após um número de tentativas pré-estabelecidas;
- 15.1.7.32. Capacidade de permitir o usuário solicitar permissão a determinado arquivo criptografado para o administrador mediante templates customizados;
- 15.1.7.33. Permite criar exclusões para não criptografar determinados “discos rígidos” através de uma busca por nome do computador ou nome do dispositivo
- 15.1.7.34. Permite criptografar as seguintes pastas pré-definidas: “meus documentos”, “Favoritos”, “Desktop”, “Arquivos temporários” e “Arquivos do outlook”;
- 15.1.7.35. Permite utilizar variáveis de ambiente para criptografar pastas customizadas;
- 15.1.7.36. Capacidade de criptografar arquivos por grupos de extensão, tais como: Documentos do office, Document, arquivos de audio, etc;
- 15.1.7.37. Permite criar um grupo de extensões de arquivos a serem criptografados;
- 15.1.7.38. Capacidade de criar regra de criptografia para arquivos gerados por aplicações;
- 15.1.7.39. Permite criptografia de dispositivos móveis mesmo quando o endpoint não possuir comunicação com a console de gerenciamento.
- 15.1.7.40. Capacidade de deletar arquivos de forma segura após a criptografia;

- 15.1.7.41. Capacidade de criptografar somente o espaço em disco utilizado;
- 15.1.7.42. Deve ter a opção de criptografar arquivos criados a partir de aplicações selecionadas pelo administrador;
- 15.1.7.43. Capacidade de bloquear aplicações selecionadas pelo administrador de acessarem arquivos criptografados;
- 15.1.7.44. Deve permitir criptografar somente o espaço utilizado em dispositivos removíveis tais como pendrives, HD externo, etc;
- 15.1.7.45. Capacidade de criptografar discos utilizando a criptografia BitLocker da Microsoft;
- 15.1.7.46. Deve ter a opção de utilização de TPM para criptografia através do BitLocker;
- 15.1.7.47. Capacidade de fazer "Hardware encryption";

15.1.8. Gerenciamento de Sistemas

- 15.1.8.1. Capacidade de criar imagens de sistema operacional remotamente e distribuir essas imagens para computadores gerenciados pela solução e para computadores bare-metal;
- 15.1.8.2. Deve possibilitar a utilização de servidores PXE na rede para deploy de imagens;
- 15.1.8.3. Capacidade de detectar softwares de terceiros vulneráveis, criando assim um relatório de softwares vulneráveis;
- 15.1.8.4. 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;
- 15.1.8.5. Capacidade de gerenciar licenças de softwares de terceiros;
- 15.1.8.6. Capacidade de registrar mudanças de hardware nas máquinas gerenciadas;
- 15.1.8.7. Capacidade de gerenciar um inventário de hardware, com a possibilidade de cadastro de dispositivos (ex: router, switch, projetor, acessório, etc), informando data de compra, local onde se encontra, service tag, número de identificação e outros;
- 15.1.8.8. Possibilita fazer distribuição de software de forma manual e agendada;
- 15.1.8.9. Suporta modo de instalação silenciosa;
- 15.1.8.10. Suporte a pacotes MSI, exe, bat, cmd e outros padrões de arquivos executáveis;
- 15.1.8.11. Possibilita fazer a distribuição através de agentes de atualização;
- 15.1.8.12. Utiliza tecnologia multicast para evitar tráfego na rede;

- 15.1.8.13. Possibilita criar um inventário centralizado de imagens;
- 15.1.8.14. Capacidade de atualizar o sistema operacional direto da imagem mantendo os dados do usuário;
- 15.1.8.15. Suporte a WakeOnLan para deploy de imagens;
- 15.1.8.16. Capacidade de atuar como servidor de atualização do Windows podendo fazer deploy de patches;
- 15.1.8.17. Suporta modo de teste, podendo atribuir alguns computadores para receberem as atualizações de forma automática para avaliação de alterações no comportamento;
- 15.1.8.18. Capacidade de gerar relatórios de vulnerabilidades e patches;
- 15.1.8.19. Possibilita criar exclusões para aplicação de patch por tipo de sistema operacional, Estação de trabalho e Servidor ou por grupo de administração;
- 15.1.8.20. Permite iniciar instalação de patch e correções de vulnerabilidades ao reiniciar ou desligar o computador;
- 15.1.8.21. Permite baixar atualizações para o computador sem efetuar a instalação
- 15.1.8.22. Permite o administrador instalar somente atualizações aprovadas, instalar todas as atualizações (exceto as bloqueadas) ou instalar todas as atualizações incluindo as bloqueadas;
- 15.1.8.23. Capacidade de instalar correções de vulnerabilidades de acordo com a severidade;
- 15.1.8.24. Permite selecionar produtos a serem atualizados pela console de gerenciamento;
- 15.1.8.25. Permite selecionar categorias de atualizações para serem baixadas e instaladas, tais como: atualizações de segurança, ferramentas, drivers, etc;
- 15.1.8.26. Capacidade de adicionar caminhos específicos para procura de vulnerabilidades e updates em arquivos;
- 15.1.8.27. Capacidade de instalar atualizações ou correções somente em computadores definidos, em grupos definidos ou em uma porcentagem de computadores conforme selecionado pelo administrador;
- 15.1.8.28. Capacidade de configurar o reinício do computador após a aplicação das atualizações e correções de vulnerabilidades;
- 15.1.8.29. Deve permitir selecionar o idioma das aplicações que serão atualizadas;
- 15.1.8.30. Permitir agendar o sincronismo entre a console de gerenciamento e os sites da Microsoft para baixar atualizações recentes;

15.1.9. Detecção e Resposta

15.1.9.1. Compatibilidade

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

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

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

15.1.9.5. Windows 10 RS4 (version 1803) Home / Professional / Education / Enterprise 32-bit / 64-bit

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

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

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

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

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

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

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

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

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

15.1.9.15. Características:

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

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

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

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

15.1.9.20. 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).



AMAZONAS

GOVERNO DO ESTADO

Nível de Classificação

Público

Grupo de acesso

PÚBLICO

15.1.9.21.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:

15.1.9.22.Isolar o host;

15.1.9.23.Iniciar uma varredura nas áreas críticas;

15.1.9.24.Quarentenar o objeto;

15.1.9.25.Capacidade de integração com a solução de sandbox;

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

15.1.9.27.Detecções provenientes da solução de endpoint;

15.1.9.28.Detecções provenientes da solução de sandbox;

15.1.9.29.Processos;

15.1.9.30.Alterações de registro;

15.1.9.31.DLL's

15.1.9.32.Conexões remotas;

15.1.9.33.Criação de arquivos;

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

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

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

15.1.9.37.Prevenir a execução de um arquivo;

15.1.9.38.Quarentenar um arquivo;

15.1.9.39.Iniciar uma varredura por IoC;

15.1.9.40.Parar um processo;

15.1.9.41.Executar um processo;

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

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

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

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

15.1.9.46.Deve possuir as seguintes opções de gerenciamento:

15.1.9.47.Via console administrativa;

15.1.9.48.Via interface web;

15.1.9.49.Gerenciamento baseado em nuvem;

15.1.9.50.Gerenciamento via linha de comando.

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

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

15.2. Especificações para o Item 2 – Kaspersky Hybrid Cloud Security Enterprise Server – com validade por 36 meses

15.2.1. Requisitos Gerais

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

15.2.1.2. Software antivírus sem agente para ambientes virtuais;

15.2.1.3. Software antivírus baseado em agente para ambientes virtuais;

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

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

15.2.1.6. Documentação do administrador;

15.2.1.7. Compatibilidade com a rede a ser protegida.

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

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

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

15.2.2. Requisitos para antivírus em ambientes virtualizados baseado em agente (conector)

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

15.2.2.2. Microsoft Windows Server 2019 Hyper-V

- 15.2.2.3. Microsoft Windows Server 2016 Hyper-V.
- 15.2.2.4. Microsoft Windows Server 2012 R2 Hyper-V
- 15.2.2.5. Citrix XenServer 7.1 LTSR.
- 15.2.2.6. VMware ESXi 7.0.
- 15.2.2.7. VMware ESXi 6.7.
- 15.2.2.8. VMware ESXi 6.5.
- 15.2.2.9. VMware ESXi 6.0.
- 15.2.2.10. KVM (Kernel-based Virtual Machine) com um dos seguintes sistemas operacionais:
- 15.2.2.11. Ubuntu Server 16.04 LTS.
- 15.2.2.12. Ubuntu Server 18.04 LTS.
- 15.2.2.13. Ubuntu Server 20.04 LTS
- 15.2.2.14. Red Hat Enterprise Linux Server 7.6.
- 15.2.2.15. CentOS 7.6.
- 15.2.2.16. Proxmox 5.4.
- 15.2.2.17. Proxmox 6.1.
- 15.2.2.18. Proxmox 6.2.
- 15.2.2.19. Skala-R Virtualization 7.0.8 hypervisor.
- 15.2.2.20. HUAWEI FusionCompute CNA 6.3.1 hypervisor.
- 15.2.2.21. Nutanix AHV 5.10 hypervisor.
- 15.2.2.22. O Antivírus baseado em agente deve prover proteção para as máquinas virtuais no Vmware hypervisor nos seguintes sistemas operacionais:
- 15.2.2.23. Windows 7 Professional / Enterprise Service Pack 1 (32 / 64-bit)
- 15.2.2.24. Windows 8.1 Update 1 Professional / Enterprise (32 / 64-bit)
- 15.2.2.25. Windows 10 Desktop Pro / Enterprise / 2016 LTSC / RS4 / 2019 LTSC / 19H1 / 19H2 / 20H1 / 20H2 (32 / 64-bit);
- 15.2.2.26. Windows Server 2008 R2 Service Pack 1 Standard / Enterprise / Datacenter (Desktop experience / Core);
- 15.2.2.27. Windows Server 2012 Standard / Datacenter / Essentials;
- 15.2.2.28. Windows Server 2012 R2 (64-bit);
- 15.2.2.29. Windows Server 2016 (64-bit);

- 15.2.2.30.Windows Server 2019 (64-bit);
- 15.2.2.31. Debian GNU / Linux 8.11 (32 / 64-bit);
- 15.2.2.32. Debian GNU / Linux 9.8 (64-bit);
- 15.2.2.33. Ubuntu Server 16.04 LTS (64-bit);
- 15.2.2.34. Ubuntu Server 18.04 LTS (64-bit);
- 15.2.2.35. CentOS 6.10 (64-bit);
- 15.2.2.36. CentOS 7.7 (64-bit);
- 15.2.2.37.CentOS 8.1 (64-bit);
- 15.2.2.38.ALT Linux 8 (64-bit);
- 15.2.2.39.ALT Linux 7.0.6 (64-bit);
- 15.2.2.40. Red Hat Enterprise Linux Server 6.10 (64-bit);
- 15.2.2.41. Red Hat Enterprise Linux Server 7.7 (64-bit);
- 15.2.2.42.Red Hat Enterprise Linux Server 8.1 (64-bit);
- 15.2.2.43. SUSE Linux Enterprise Server 15 (64-bit);
- 15.2.2.44.Oracle Linux 7.6 (64-bit);
- 15.2.2.45.A Suite VMware tools deve ser instalada para prover integração entre o Hypervisor, máquinas virtuais e o conector;
- 15.2.2.46.O antivírus baseado em agente deve prover as seguintes funcionalidades:
- 15.2.2.47.Antivírus e monitoramento residente;
- 15.2.2.48.Proteção contra rootkits e auto dialers a sites pagos;
- 15.2.2.49.Proteção de pastas compartilhadas contra criptografia externa;
- 15.2.2.50.Ao detectar criptografia externa, deve criar automaticamente um backup do arquivo;
- 15.2.2.51.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;
- 15.2.2.52.Deve permitir substituir automaticamente os arquivos modificados pelos seus backups;
- 15.2.2.53.Verificação por heurística para detectar e bloquear malwares desconhecidos;
- 15.2.2.54.Capacidade de pausar varreduras automaticamente em horários predefinidos;

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

15.2.2.56. 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;

15.2.2.57. 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;

15.2.2.58. 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;

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

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

15.2.2.61. Capacidade de detectar e bloquear sites de phishing;

15.2.2.62. Proteção contra ameaças não conhecidas baseadas no comportamento;

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

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

15.2.2.65. 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;

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

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

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

15.2.2.69. 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;

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

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

15.2.2.72. Fornecedores confiáveis;

15.2.2.73. Componentes do sistema operacional;

15.2.2.74. Aplicações de virtualização;

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

15.2.2.76. Permitir a verificação em máquinas Linux;

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

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

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

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

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

15.2.2.82. Utilizando Multicast;

15.2.2.83. Selecionando Servidor de integração;

15.2.2.84. Utilizando uma lista de appliances virtuais

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

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

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

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

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

15.2.2.90. Verificação automática;

15.2.2.91. Verificar os arquivos no acesso ou na modificação;

15.2.2.92. Somente no acesso;

15.2.2.93. 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;

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

15.2.2.95. 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);

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

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

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

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

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

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

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

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

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

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

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

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

15.2.2.108. Salvar o backup dos arquivos deletados;

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

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

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

15.2.2.112. Suportar rollback do banco de dados de definições;

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

15.2.3. Requisitos para administração centralizada, monitoramento e update do software para ambientes virtualizados:

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

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

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

15.2.3.4. Microsoft Windows 10 Education RS3;

15.2.3.5. Microsoft Windows 10 Education RS4;

15.2.3.6. Microsoft Windows 10 Education RS5;

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

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

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

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

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

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

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

15.2.3.14. Microsoft Windows Server 2016 x64;

15.2.3.15. **Bancos de dados suportados pela console de administração centralizada:**

15.2.3.16. Microsoft SQL Server 2012 Express 64-bit;

15.2.3.17. Microsoft SQL Server 2014 Express 64-bit;

15.2.3.18. Microsoft SQL Server 2016 Express 64-bit;

15.2.3.19. Microsoft SQL Server 2017 Express 64-bit;

15.2.3.20. Microsoft SQL Server 2019 Express 64-bit;

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

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

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

- 15.2.3.24. Microsoft SQL Server 2019 (todas as edições) 64-bit;
- 15.2.3.25. MySQL Standard Edition 5.7 32-bit/64-bit;
- 15.2.3.26. MySQL Enterprise 5.7 32-bit/64-bit;
- 15.2.3.27. MariaDB Server 10.3 32-bit/64-bit;

15.2.4. Requisitos para o Console de administração instalado em ambientes virtuais

- 15.2.4.1. Vmware Workstation 16 Pro;
 - 15.2.4.2. Vmware Workstation 15 Pro;
 - 15.2.4.3. Microsoft Hyper-V Server 2012 64-bit;
 - 15.2.4.4. Microsoft Hyper-V Server 2012 R2 64-bit;
 - 15.2.4.5. Microsoft Hyper-V Server 2016 64-bit;
 - 15.2.4.6. Microsoft Hyper-V Server 2019 64-bit;
 - 15.2.4.7. VMware vSphere 6.7;
 - 15.2.4.8. VMware vSphere 7.1;
 - 15.2.4.9. Citrix XenServer 8.x;
 - 15.2.4.10. Citrix XenServer 7.1 LTSR;
 - 15.2.4.11. Parallels Desktop 16;
 - 15.2.4.12. Oracle VM VirtualBox 6.x;
- 15.2.5. O Console de administração centralizada deve prover as seguintes funcionalidades:
- 15.2.5.1. Deve ser compatível com Microsoft SCVMM;
 - 15.2.5.2. Capacidade de desativar a interface local do agente (conector) para diminuir uso de memória;
 - 15.2.5.3. Instalação do antivírus a partir de uma única distribuição;
 - 15.2.5.4. Seleção de instalação dependendo do número de pontos protegidos;
 - 15.2.5.5. Capacidade de ler informações do AD para obter dados sobre as contas dos computadores na organização;
 - 15.2.5.6. Capacidade de fazer a instalação automática através dos grupos gerenciados;
 - 15.2.5.7. Capacidade de realocar computadores de acordo com endereço IP, tipo do sistema operacional e localização no AD;
 - 15.2.5.8. Instalação centralizada;
 - 15.2.5.9. Remoção centralizada (manual ou automática) de aplicações incompatíveis através do servidor de administração;

- 15.2.5.10. Capacidade de instalar o antivírus de diferentes formas: GPO, agente de administração;
- 15.2.5.11. Capacidade de atualizar pacotes de instalação com as últimas atualizações;
- 15.2.5.12. Atualizar de forma automática a versão do antivírus e as definições;
- 15.2.5.13. Procurar automaticamente por vulnerabilidades nas aplicações e sistemas operacionais presentes da rede;
- 15.2.5.14. Capacidade de proibir instalação/execução de aplicações;
- 15.2.5.15. Capacidade de gerenciar I/O de dispositivos externos;
- 15.2.5.16. Gerenciar a atividade do usuário na internet;
- 15.2.5.17. Capacidade de testar as atualizações antes de aplicar para o ambiente;
- 15.2.5.18. Capacidade de executar instalações automáticas baseado no sistema de proteção dedicado, tais como: Vmware ESXi, Microsoft Hyper-V, Citrix XenServer virtualization ou hypervisor;
- 15.2.5.19. Criar os usuários baseados em RBAC;
- 15.2.5.20. Criar a hierarquia dos servidores de administração e tem capacidade de gerenciar cada um deles através de uma única console de gerenciamento;
- 15.2.5.21. Capacidade de criar servidores de administração lógicos, sem a necessidade de ter um servidor adicional para gerenciamento;
- 15.2.5.22. Distribuir automaticamente licenças nos computadores gerenciados;
- 15.2.5.23. Criar o inventário de software e hardware dos computadores gerenciados na rede;
- 15.2.5.24. Instalação centralizada de aplicações de terceiros;
- 15.2.5.25. Capacidade de eleger um computador na rede para ser responsável por atualizar outros computadores dentro da rede;
- 15.2.5.26. Capacidade de gerar relatórios gráficos;
- 15.2.5.27. Capacidade de exportar relatórios para PDF, XML e CSV;
- 15.2.5.28. Capacidade de criar contas internas para autenticar no console de administração;
- 15.2.5.29. Capacidade de criar backup de forma automática ou manual;
- 15.2.5.30. Suporta Windows Failover Clustering;
- 15.2.5.31. Console WEB para gerenciar a aplicação;
- 15.2.5.32. Sistema para controle de virus outbreak.



AMAZONAS

GOVERNO DO ESTADO

Nível de Classificação

Público

Grupo de acesso

PÚBLICO

- 15.2.5.33. Capacidade de gerenciar permissões de administradores;
- 15.2.5.34. Capacidade de deletar atualizações já baixadas;
- 15.2.5.35. Capacidade de distribuir correções de vulnerabilidades em computadores clientes sem instalar atualizações;
- 15.2.5.36. Capacidade de eleger automaticamente um agente de atualização de acordo com uma análise de rede.
- 15.2.5.37. Capacidade de manter um histórico das alterações;
- 15.2.5.38. Permite comparar alterações feitas no console de administração;
- 15.2.5.39. Deve permitir o rollback de alterações feitas nas políticas através de uma única seleção, sem ter a necessidade de restaurar item por item alterado.

Manaus (AM), 26 de junho de 2023.

Salim Silva David

Gerente de Infraestrutura e Serviços de T.I.

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.

WWW.PRODAM.AM.GOV.BR
Instagram: @prodam_am
Facebook: ProdamAmazonas

Fone: (92) 2121-6500
Whatsapp: (92) 99115-9496
sacp@prodam.am.gov.br
Rua Jonathas Pedrosa, n°1937.
Praça 14 de Janeiro. Manaus -AM.
CEP 69020-110

PRODAM

PREGÃO ELETRÔNICO SRP 05/2023

Anexo 01-A – MODELO DE PROPOSTA DE PREÇOS

O preço deverá ser composto de acordo com a tabela abaixo:

| Item | ESPECIFICAÇÃO | Unidade | QTD. | Valor Mensal Unitário (R\$) | Valor Mensal Total (R\$) | Valor Total em 12 meses (R\$) |
|---------------------------|---|----------------|-------|-----------------------------|--------------------------|-------------------------------|
| 1 | <i>Kaspersky Endpoint Detection and Response Optimum – com validade de 36 meses</i> | <i>Licença</i> | 5.000 | | | |
| 2 | <i>Kaspersky Hybrid Cloud Security Enterprise Server – com validade de 36 meses</i> | <i>Licença</i> | 500 | | | |
| Valor Global (R\$) | | | | | | |

Os preços para sessão pública do Pregão deverá ser a soma de valores da última coluna, indicado como “**Valor Global**”.

Validade da Proposta: 90 (noventa) dias.

PREGÃO ELETRÔNICO SRP Nº 05/2023

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 Cívis, 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



AMAZONAS

GOVERNO DO ESTADO

Nível de Classificação
Público

Grupo de acesso
PÚBLICO

- 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:
- $$\frac{\text{ATIVO CIRCULANTE} + \text{REALIZÁVEL A LONGO PRAZO}}{\text{PASSIVO CIRCULANTE} + \text{PASSIVO NÃO CIRCULANTE}}$$
- 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 **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

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 e Municipal ou do Distrito Federal, conforme 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. Comprovação de aptidão da licitante para desempenho, através de apresentação de atestados ou certidões emitidas por entidades públicas e/ou privadas, indicando que a empresa já forneceu objeto semelhante ao desta licitação;
- 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 (dezesesseis) 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.



AMAZONAS

GOVERNO DO ESTADO

Nível de Classificação

Público

Grupo de acesso

PÚBLICO

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

WWW.PRODAM.AM.GOV.BR
Instagram: @prodam_am
Facebook: ProdamAmazonas

Fone: (92) 2121-6500
Whatsapp: (92) 99115-9496
sacp@prodam.am.gov.br
Rua Jonathas Pedrosa, n°1937.
Praça 14 de Janeiro. Manaus -AM.
CEP 69020-110

PRODAM

PREGÃO ELETRÔNICO SRP Nº 05/2023

ANEXO 3 – MINUTA DA ATA DE REGISTRO DE PREÇOS Nº 05/2023

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 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 XXXXXXXX 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 Reunião Extraordinária do Conselho de Administração datada de 05/05/2022 e Ata Registrada na Junta Comercial do Estado do Amazonas sob o n.º 1196758 em 10/05/2022, considerando julgamento da licitação na modalidade de Pregão, na forma Eletrônica, para REGISTRO DE PREÇOS n.º XX/20XX, publicada no Diário Oficial do Estado do Amazonas de XX/XX/XXXX, processo administrativo, **SIGED 01.05.016503.000971/2023-28**, 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 n.º 13.303, de 30.06.2016 e demais alterações, e o 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 licenças de antivírus Kaspersky para compor “prateleira” de produtos e serviços a serem comercializados pela PRODAM a seus clientes e consumidos pela própria PRODAM.
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: XXXXXXXXXXXXXXXXXXXX, CNPJ n.º xxxxxxxxxxx/xxxxx- xx, com sede na xxxxxxxxxxx, n.º xxx, bairro, CEP xxxxxxx, Cidade/ESTADO, telefone



AMAZONAS

GOVERNO DO ESTADO

Nível de Classificação

Público

Grupo de acesso

PÚBLICO

(XX) XXXXXXXX, E-mail: xxxxxxxxxxxxxxxxxxxx, representada por xxxxxxxxxxxx, Xx. XXXXXXXXXXXXXXXXXXXX, nacionalidade, profissão, estado civil, residente e domiciliado xxxxxxxxxxxx, n.º xxx, bairro, CEP xxxxxxxx, Cidade/ESTADO, RG n.º xxxxxxxx XXX/XXe CPF n.º XXXXXXXXXXXX;

2.2 Fornecedor: XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX, CNPJ n.º xxxxxxxx/xxxxx- xx, com sede na xxxxxxxxxxxx, n.º xxx, bairro, CEP xxxxxxxx, Cidade/ESTADO, telefone (XX) XXXXXXXX/ XXXXXXXX, E-mail: xxxxxxxxxxxxxxxxxxxxxxxxxxxx, representada por xxxxxxxxxxxx, Xx. XXXXXXXXXXXXXXXXXXXX, nacionalidade, profissão, estado civil, residente e domiciliado xxxxxxxxxxxx, n.º xxx, bairro, CEP xxxxxxxx, Cidade/ESTADO, RG n.º xxxxxxxx XXX/XXe CPF n.º XXXXXXXXXXXX;

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 no art. 24 do Decreto Estadual n.º 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 n.º 05/2023.**

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 n.º 05/2023.

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:** o prazo de entrega será conforme item 2.3 do termo de referência do Edital do Pregão Eletrônico SRP n.º 05/2023.



AMAZONAS

GOVERNO DO ESTADO

Nível de Classificação

Público

Grupo de acesso

PÚBLICO

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 **XXXXXXXXXXXXXXXXXXXXXX**

Lincoln Nunes da Silva

Diretor-Presidente

XXXXXXXXXXXXXXXXXXXXXX

Representante legal

REVISÃO E APROVAÇÃO:

Assessor Jurídico

WWW.PRODAM.AM.GOV.BR
Instagram: @prodam_am
Facebook: ProdAmAmazonas

Fone: (92) 2121-6500
Whatsapp: (92) 99115-9496
sacp@prodam.am.gov.br
Rua Jonathas Pedrosa, n°1937.
Praça 14 de Janeiro. Manaus -AM.
CEP 69020-110

PRODAM



AMAZONAS

GOVERNO DO ESTADO

Nível de Classificação
Público

Grupo de acesso
PÚBLICO

PREGÃO ELETRÔNICO SRP N.º 05/2023
ANEXO DA ATA DE REGISTRO DE PREÇOS N.º XX/20XX

GRUPO ÚNICO

| ITEM | DESCRIÇÃO | UNIDADE | QTD. | VALOR UNITÁRIO | VALOR TOTAL |
|------|--|---------|-------|----------------|-------------|
| 1 | Kaspersky Endpoint Detection and Response Optimum – com validade de 36 meses | Licença | 5.000 | | |
| 2 | Kaspersky Hybrid Cloud Security Enterprise Server – com validade de 36 meses | Licença | 500 | | |

Pela **PRODAM S.A.**

Pela **XXXXXXXXXXXXXXXXXXXXXX**

Lincoln Nunes da Silva

XXXXXXXXXXXXXXXXXXXXXX

Diretor-Presidente

Representante legal

VALOR TOTAL DA ATA: R\$ XXXXXXXXX (XXXXXXXXXXXXXXXXXX)



AMAZONAS

GOVERNO DO ESTADO

Nível de Classificação

Público

Grupo de acesso

PÚBLICO

PREGÃO ELETRÔNICO SRP Nº 05/2023

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: Esta declaração deverá ser emitida em papel timbrado da empresa proponente e carimbada com o número do CNPJ.



AMAZONAS

GOVERNO DO ESTADO

Nível de Classificação

Público

Grupo de acesso

PÚBLICO

PREGÃO ELETRÔNICO SRP Nº 05/2023

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 (dezesesseis) 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.



AMAZONAS

GOVERNO DO ESTADO

Nível de Classificação
Público

Grupo de acesso
PÚBLICO

PREGÃO ELETRÔNICO SRP Nº 05/2023
ANEXO 6 - TABELA DE PREÇO MÁXIMO

| Item | ESPECIFICAÇÃO | Referência | QTD. | Valor Unitário (R\$) | Valor Total (R\$) |
|------|---|----------------|-------|----------------------|-------------------|
| 1 | <i>Kaspersky Endpoint Detection and Response Optimum – com validade de 36 meses</i> | <i>Licença</i> | 5.000 | 264,88 | 1.324.400,00 |
| 2 | <i>Kaspersky Hybrid Cloud Security Enterprise Server – com validade de 36 meses</i> | <i>Licença</i> | 500 | 2852,50 | 1.426.250,00 |

Deverá ser respeitado o valor máximo de cada ITEM, sob pena de desclassificação.



AMAZONAS

GOVERNO DO ESTADO

Nível de Classificação
Público

Grupo de acesso
PÚBLICO

PREGÃO ELETRÔNICO SRP Nº 05/2023

ANEXO 7 – CHECKLIST– PROGRAMA DE INTEGRIDADE

| Item | Atendido? | | |
|---|-----------|-----|---------------|
| | Sim | Não | Não se Aplica |
| 1 - O grau de comprometimento da alta direção da pessoa jurídica, incluídos os Conselhos, quando aplicado, está evidenciado pelo apoio visível e inequívoco ao Programa? (participação em reuniões e avaliações periódicas, elaboração de dispositivos de controle, etc.) | | | |
| 2 – Os padrões de conduta, código de ética, políticas e procedimentos de integridade apresentados pela entidade são de conhecimento dos funcionários (cópia de documento entregue na contratação, publicação na empresa, etc.)? | | | |
| 3 – O nível de adesão dos padrões de conduta, código de ética e políticas de integridade estendidos, quando necessário, a terceiros, tais como, fornecedores, prestadores de serviço, agentes intermediários e associados, está sendo monitorado? | | | |
| 4 – A realização dos treinamentos periódicos sobre o Programa de Integridade está devidamente registrada? | | | |
| 5 – Os mecanismos de acompanhamento da análise periódica de riscos para realizar adaptações necessárias ao Programa de Integridade estão disponíveis e tem um cronograma estabelecido? | | | |
| 6 – Os controles internos que asseguram a pronta elaboração e confiabilidade de relatórios e demonstrações financeiras estão atualizados e em conformidade com os padrões das demonstrações contábeis? | | | |
| 7 – Os canais de denúncia de irregularidades, abertos e amplamente divulgados a funcionários e terceiros, e de mecanismos destinados à proteção de denunciadores de boa-fé são efetivamente monitorados? (relatórios periódicos, reuniões de avaliação, documentação relativa a tomada de providências, etc.) | | | |
| 8 – Existem medidas disciplinares em caso de violação do Programa de Integridade e sua efetividade (monitoramento das violações documentadas, relatórios de acompanhamento das medidas, registro e acompanhamento de medidas tomadas, etc.)? | | | |



AMAZONAS

GOVERNO DO ESTADO

Nível de Classificação

Público

Grupo de acesso

PÚBLICO

9 – Os procedimentos internos quanto ao Programa de Integridade, asseguram a pronta interrupção de irregularidades ou infrações detectadas e a tempestiva remediação dos danos gerados?

10 – As diligências apropriadas para contratação e, conforme o caso, supervisão de terceiros, tais como, fornecedores, prestadores de serviço, agentes intermediários e associados, são devidamente registradas e seu acompanhamento periódico é documentado?

Atesto para os devidos fins que a Contratada atende aos requisitos relacionados no Checklist referente a implantação do Programa de Integridade.

Contrato nº.: _____

Fiscal do Contrato: _____

Cargo: _____ CPF.: _____



AMAZONAS

GOVERNO DO ESTADO

Nível de Classificação
Público

Grupo de acesso
PÚBLICO

PREGÃO ELETRÔNICO SRP Nº 05/2023

ANEXO 8 – MINUTA DE CONTRATO

CONTRATO N.º XXX/20XX

TERMO DE CONTRATO PARA FORNECIMENTO DE LICENÇAS DE ANTIVÍRUS KASPERSKY PARA COMPOR “PRATELEIRA” DE PRODUTOS E SERVIÇOS A SEREM COMERCIALIZADOS PELA PRODAM A SEUS CLIENTES E CONSUMIDOS PELA PRÓPRIA PRODAM, CELEBRADO ENTRE A PRODAM – PROCESSAMENTO DE DADOS AMAZONAS S/A E A EMPRESA XXXXXXXXXXXXXXXXXXXX, 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 simplesmente **CONTRATANTE**, 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, sob o n.º 13300001038, e com Inscrição Estadual n.º 05.341.162-5 e CNPJ n.º 04.407.920/0001-80, neste ato representada por seu Diretor Presidente, Sr. **XXXXXXXXXXXXXXXXXXXX**, xxxxx, xxxxxx, xxxxxxx, portador da RG n.º xxxxx-x SSP/AM, e do CPF n.º xxxxxxxxxxxx, 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 Reunião Extraordinária do Conselho de Administração datada de 05/05/2022 e Ata Registrada na Junta Comercial do Estado do Amazonas sob o n.º 1196758 em 10/05/2022, e de outro lado, a **XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX**, doravante designada simplesmente **CONTRATADA**, com sede em XXXXXXXX, na XXXXXXXXXXXXX, n.º XXX, Bairro XXXXXXXXXXXXXXXXXXXX, CEP: XXXXXXX, XXXXXX/XX, inscrita no CNPJ n.º XX.XXX.XXX/XXXX-XX, inscrição municipal n.º xxxxxx, neste ato representada por XXXXXXXX, Sr. **XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX**, nacionalidade, estado civil, profissão, portador da Cédula de Identidade n.º XXXX XXXXX/XX e do CPF n.º XXX.XXX.XXX-XX, residente e domiciliado XXXXXXXXXXXXXXX, tendo em vista o que consta no Procedimento de Licitação, **Pregão Eletrônico SRP n.º 05/2023**, tudo em conformidade



AMAZONAS

GOVERNO DO ESTADO

Nível de Classificação
Público

Grupo de acesso
PÚBLICO

com a Lei n.º 13.303, de 30.06.2016 e demais alterações, e o RILC - Regulamento Interno de Licitações e Contratos da PRODAM, aplicando-se subsidiariamente as disposições estabelecidas no presente instrumento convocatório e seus Anexos, resolvem as partes celebrar o presente termo, 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 licenças de antivírus Kaspersky para compor “prateleira” de produtos e serviços a serem comercializados pela **CONTRATANTE** a seus clientes e consumidos pela própria **CONTRATANTE**.

CLÁUSULA SEGUNDA: DAS CARACTERÍSTICAS E ESPECIFICAÇÕES DO OBJETO

- 2.1 Tabela de itens para eventual contratação:

| ITEM | DESCRIÇÃO | UNIDADE | QUANTIDADE MÁXIMA |
|------|--|---------|-------------------|
| 1 | Kaspersky Endpoint Detection and Response Optimum – com validade de 36 meses | Licença | 5.000 |
| 2 | Kaspersky Hybrid Cloud Security Enterprise Server – com validade de 36 meses | Licença | 500 |

- 2.2 A solução deverá atender as especificações contidas no item 15 do Termo de Referência do Edital do Pregão Eletrônico SRP n.º 05/2023, parte integrante deste contrato.
- 2.3 O prazo de entrega das licenças será de até 15 dias corridos.

CLÁUSULA TERCEIRA: DAS CONDIÇÕES DE GARANTIA E SUPORTE

- 3.1 Todas as licenças devem oferecer validade, atualizações e suporte de software por 36 meses.

CLÁUSULA QUARTA: DO REGIME DE EXECUÇÃO DO CONTRATO

- 4.1 Regime de execução será por empreitada por preço unitário.
- 4.2 A contratação das licenças será por demanda e conveniência da **CONTRATANTE** através da emissão de Pedido de Compra – PC, vinculado ao respectivo Contrato.



AMAZONAS

GOVERNO DO ESTADO

Nível de Classificação

Público

Grupo de acesso

PÚBLICO

CLÁUSULA QUINTA: DOS PREÇOS E CONDIÇÕES DE PAGAMENTO

- 5.1 O Valor Global estimado do presente Contrato é de R\$ xxxxx (xxxxxxxxxxxxxxxxxxxx).
- 5.2 O pagamento ocorrerá de acordo com a apuração da quantidade de licenças solicitadas pelo Pedido de Compra – PC.
- 5.3 O pagamento será efetuado mediante apresentação da Nota Fiscal/Fatura e ocorrerá até o 15º (décimo quinto) dia útil do mês subsequente, com os descontos legais (retenções).
- 5.4 O valor a ser pago pelo consumo das licenças será calculado de acordo com a regra abaixo:
 - 5.4.1 Valor a pagar = Quantidade de licenças adquiridas * Valor unitário de cada licença.

CLÁUSULA SEXTA: DO REAJUSTAMENTO

- 6.1 A **CONTRATADA** poderá solicitar revisão dos preços dos itens de contrato em cada aniversário do contrato, 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).
- 6.2 A solicitação será avaliada pela **CONTRATANTE**.

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 n.º 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.

Nível de Classificação
Público

Grupo de acesso
PÚBLICO

- 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.

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**.



AMAZONAS

GOVERNO DO ESTADO

Nível de Classificação

Público

Grupo de acesso

PÚBLICO

CLÁUSULA DÉCIMA PRIMEIRA: DAS SANÇÕES ADMINISTRATIVAS

- 11.1 O serviço a ser prestado deverá seguir as especificações contidas neste Contrato. O descumprimento total ou parcial de qualquer obrigação estabelecida sujeitará a **CONTRATADA** às sanções legais aplicáveis, garantida a prévia e ampla defesa.
- 11.2 Além das penalidades legalmente previstas e sem prejuízo das mesmas, a **CONTRATADA** ficará sujeita às sanções a seguir relacionadas:
- 11.2.1 Advertência;
- 11.2.2 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;
- 11.2.3 Suspensão temporária de participação em licitação e impedimento de contratar com a **CONTRATANTE** pelo prazo de até 02 (dois) anos.
- 11.3 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**.
- 11.4 O valor da multa, apurado após regular procedimento administrativo, será descontado dos pagamentos eventualmente devidos pela **CONTRATANTE**, da Garantia ou cobrados judicialmente.

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 tiverem aplicado penalidades, a **CONTRATADA** poderá, sempre com efeito suspensivo:
- 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;
 - 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;
 - 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.



AMAZONAS

GOVERNO DO ESTADO

Nível de Classificação

Público

Grupo de acesso

PÚBLICO

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 **CONTRATANTE** 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 n.º 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.



AMAZONAS

GOVERNO DO ESTADO

Nível de Classificação

Público

Grupo de acesso

PÚBLICO

- 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:
- Assunção imediata do objeto deste contrato no estado em que se encontrar, por ato seu;
 - 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**;
 - 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 n.º 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 Termo.

| 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 Contrato, 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 Durante a vigência do contrato, a execução dos serviços será acompanhada e fiscalizada por colaborador designado.
- 19.2 A fiscalização do Contrato será exercida por colaborador formalmente designado por portaria interna da **CONTRATANTE**, para o acompanhamento da contratação e execução dos serviços, igualmente regulamentados por portaria interna.
- 19.3 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.
- 19.4 A **CONTRATADA** deverá facilitar, por todos os meios, a ampla ação da fiscalização da **CONTRATANTE**, assim como, providenciar, de imediato a regularização das observações e exigências apontadas pela fiscalização da **CONTRATANTE**.
- 19.5 A **CONTRATADA** deverá comunicar, imediatamente, a fiscalização da **CONTRATANTE**, qualquer anormalidade existente ou surgida que esteja impedindo o fiel cumprimento do objeto do Contrato.
- 19.6 A atividade de fiscalização será realizada para assegurar o efetivo cumprimento das obrigações contratuais assumidas e a qualidade dos serviços prestados à **CONTRATANTE**.
- 19.7 Para tanto, o fiscal a ser designado pela **CONTRATANTE** deverá:
 - 19.7.1 Acompanhar, fiscalizar e atestar a execução dos serviços contratados;
 - 19.7.2 Indicar as eventuais glosas das faturas;
 - 19.7.3 Informar à Administração da **CONTRATANTE** o eventual descumprimento dos compromissos pactuados, que poderá ensejar a aplicação de penalidades.
- 19.8 Informar à Administração da **CONTRATANTE** o eventual descumprimento dos compromissos pactuados, que poderá ensejar a aplicação de penalidades.
- 19.9 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.

Nível de Classificação
Público

Grupo de acesso
PÚBLICO

- 19.10 Nessa audiência serão definidos e formalizados os protocolos de comunicação entre a **CONTRATANTE** e **CONTRATADA**, para efeito da fiscalização do contrato.
- 19.11 Serão ainda ratificados os procedimentos decorrentes deste Contrato para:
- 19.11.1 Emissão dos Pedidos de Compras;
 - 19.11.2 Verificação do atendimento dos requisitos estabelecidos no Termo de Referência do Edital do Pregão Eletrônico SRP n.º 05/2023;
 - 19.11.3 Atestação das faturas;
 - 19.11.4 Descontos, multas e aplicação das demais sanções previstas;
 - 19.11.5 Renovação do contrato;
 - 19.11.6 Encerramento do contrato.

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 n.º 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 **CONTRATANTE** 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 n.º 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 n.º 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.



AMAZONAS

GOVERNO DO ESTADO

Nível de Classificação

Público

Grupo de acesso

PÚBLICO

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 N.º 05/2023

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



AMAZONAS

GOVERNO DO ESTADO

Nível de Classificação

Público

Grupo de acesso

PÚBLICO

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.



AMAZONAS

GOVERNO DO ESTADO

Nível de Classificação
Público

Grupo de acesso
PÚBLICO

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. 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



AMAZONAS

GOVERNO DO ESTADO

Nível de Classificação

Público

Grupo de acesso

PÚBLICO

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 _____.____.____-____