PROCESSO N.º 9.444/2025

PREGÃO ELETRÔNICO Nº 131/2025

Torna-se público que a Prefeitura Municipal de Americana, realizará licitação, conforme modalidade, forma, critério de julgamento e modo de disputa indicados no quadro abaixo, nos termos da Lei nº 14.133/2021, do Decreto Municipal nº 13.826/2025 https://www.americana.sp.gov.br/legislacao/decreto_13826_2025.html e demais legislação aplicável e, ainda, de acordo com as condições estabelecidas neste Edital.

Modalidade e Forma	Pregão Eletrônico
Apresentação de Proposta	**Até 19/11/2025 às 07:30hs** (horário de Brasília)
Abertura da licitação	**19/11/2025 às 08:30hs** (horário de Brasília)
Critério de Julgamento	Menor Preço Global
Modo de Disputa	Aberto
Intervalo mínimo de diferença de valores ou percentuais entre os lances	R$ 100,00
Benefícios ME/EPP	Sim. Vide condições do Edital
Permitida a participação de consórcio	Não, conforme justificativa constante do Termo de Referência
Garantia de proposta (art. 58 da Lei 14.133/2021)	Não
Valor Estimado da Contratação	R$ 201.842,22 (duzentos e um mil, oitocentos e quarenta e dois reais e vinte e dois centavos). A planilha orçamentária com o valor unitário dos itens encontra-se disponível para consulta no processo.
Sistema Eletrônico	*Plataforma BBMNET - novobbmnet.com.br*
Locais em que serão divulgadas informações sobre o certame	*Diário Oficial do Município* *Jornal de Grande Circulação (Folha de São Paulo)* *www.americana.sp.gov.br* *www.novobbmnet.com.br* *PNCP – Portal Nacional de Contratações Públicas*
Pedidos de esclarecimentos e impugnações	Sistema Eletrônico da BBMNET, através do e-mail da pregoeira tassia.suprimentos@americana.sp.gov.br ou na Prefeitura Municipal de Americana, Protocolo Geral, à Av. Brasil, n.º 85 – Térreo – Centro – Americana (SP).

1. DO OBJETO

1.1. O objeto da presente licitação é a **CONTRATAÇÃO DE SERVIÇOS DE LICENÇA DE USO DE 1.050 LICENÇAS DE ENDPOINT VISION ONE 03 LICENÇAS DE PROTEÇÃO CLOUD VISION ONE – TREND MICRO, DESTINADAS À PROTEÇÃO DAS ESTAÇÕES DE TRABALHO E SERVIDORES EM NUVEM DE ESTAÇÕES DE TRABALHO, SERVIDORES E SERVIÇOS EM NUVEM, A SEREM UTILIZADAS EM TODA A ESTRUTURA DA ADMINISTRAÇÃO MUNICIPAL,** conforme condições, quantidades e exigências estabelecidas no Termo de Referência, Anexo III deste edital.

1.2. O critério de julgamento será o indicado no quadro acima e quando da licitação dividida em lotes, o licitante poderá participar em quantos lotes forem de seu interesse, devendo oferecer proposta para todos os itens que compõem o lote escolhido.

2. DA PARTICIPAÇÃO NA LICITAÇÃO

2.1. Poderão participar deste Pregão os interessados do ramo de atividade pertinente ao objeto da contratação, que preencham as condições estabelecidas neste edital e que estiverem previamente credenciados perante o provedor do sistema eletrônico da BBMNET, www.novobbmnet.com.br.

2.2. A participação do licitante no pregão eletrônico se dará exclusivamente por meio do sistema eletrônico da BBMNET, www.novobbmnet.com.br, através de manifestação de operador formalmente designado.

2.3. O acesso do operador ao pregão, para efeito de encaminhamento de proposta de preço e lances sucessivos de preços, em nome do licitante, somente se dará mediante prévia definição de senha privativa.

2.4. É de exclusiva responsabilidade do usuário o sigilo da senha, bem como seu uso em qualquer transação efetuada diretamente ou por seu representante, não cabendo a BBMNET ou ao órgão promotor da licitação a responsabilidade por eventuais danos decorrentes de uso indevido da senha, ainda que por terceiros.

2.5. O licitante se compromete a:

2.5.1. responsabilizar-se, formalmente, pelas transações efetuadas em seu nome, assumindo como firmes e verdadeiras suas propostas e lances, inclusive, os atos praticados diretamente ou por seu representante, não cabendo ao provedor do sistema ou ao órgão promotor da licitação, responsabilidade por eventuais danos decorrentes do uso indevido da senha, ainda que por terceiros;

2.5.2. acompanhar as operações do sistema eletrônico durante o processo licitatório, responsabilizando-se pelo ônus decorrente da perda de negócios, diante da inobservância de quaisquer mensagens emitidas pelo órgão promotor da licitação ou de sua desconexão;

2.5.3. comunicar ao provedor do sistema, qualquer acontecimento que possa comprometer o sigilo ou a segurança, para imediato bloqueio de acesso;

2.6. No caso de dúvida quanto à utilização da ferramenta da “BBMNET”, utilizar o suporte técnico através do telefone (11) 3181-8214 ou através do e-mail elicitacao@bbmnet.com.br .

2.7. É de responsabilidade do cadastrado conferir a exatidão dos seus dados cadastrais no Sistema relacionados no item anterior 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 aqueles se tornem desatualizados.

2.8. A não observância do disposto no item anterior poderá ensejar desclassificação no momento da habilitação.

2.9. Será concedido tratamento favorecido para as microempresas e empresas de pequeno porte, para as sociedades cooperativas mencionadas no art. 16 da Lei nº 14.133/2021 e para o microempreendedor individual - MEI, nos limites previstos da Lei Complementar nº 123/2006 e conforme disposto nos §§ 1º ao 3º do art. 4º da Lei nº 14.133/2021.

2.10. Além das vedações estabelecidas pelo art. 14 da Lei nº 14.133/2021, não será permitida a participação do licitante:

2.10.1. que não atenda às condições deste Edital e seu(s) anexo(s);

2.10.2. agente público do órgão licitante nos termos do §1º do art. 9º da Lei 14.133/2021;

2.10.3. entidades do terceiro setor assim classificadas como Organização da Sociedade Civil - OSC, atuando nessa condição;

2.10.4. reunido em consórcio, salvo se autorizado no quadro constante do preâmbulo deste edital.

3. DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

3.1. Os licitantes encaminharão, exclusivamente por meio do sistema eletrônico, a proposta com o preço ou o percentual de desconto, conforme o critério de julgamento adotado neste Edital, até a data e o horário estabelecidos para abertura da sessão pública.

3.2. No cadastramento da proposta inicial o licitante declarará, em campo próprio do sistema, caso a funcionalidade esteja disponível, que:

3.2.1. está ciente e concorda com as condições contidas no edital e seus anexos, bem como de que a proposta apresentada compreende a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de sua entrega em definitivo e que cumpre plenamente os requisitos de habilitação definidos no instrumento convocatório;

3.2.2. não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do art. 7º, XXXIII, da Constituição Federal;

3.2.3. não possui empregados executando trabalho degradante ou forçado, observando o disposto nos incisos III e IV do art. 1º e no inciso III do art. 5º da Constituição Federal;

3.2.4. cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas.

Obs.: As declarações que o sistema não facultar em campo próprio devem ser apresentadas pelo licitante detentor da melhor proposta juntamente com seus documentos de habilitação.

3.3. O licitante organizado em cooperativa deverá declarar, ainda, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no art. 16 da Lei nº 14.133/2021.

3.4. O fornecedor enquadrado como microempresa ou empresa de pequeno porte deverá declarar, ainda, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no art. 3º da Lei Complementar nº 123/2006, estando apto a usufruir do tratamento favorecido estabelecido em seus arts. 42 a 49, observado o disposto nos §§ 1º ao 3º do art. 4º da Lei nº 14.133/2021.

3.4.1. No caso de item exclusivo para participação de microempresas e empresas de pequeno porte, a assinalação do campo “não” impedirá o prosseguimento no certame, para aquele item;

3.4.2. Nos itens em que a participação não for exclusiva para microempresas e empresas de pequeno porte, a assinalação do campo “não” apenas produzirá o efeito de o licitante não ter direito

ao tratamento favorecido previsto na Lei Complementar nº 123/2026, mesmo que microempresa ou empresa de pequeno porte.

3.4.3. Caso o valor estimado da presente licitação seja superior à receita bruta máxima admitida para fins de enquadramento como empresa de pequeno porte, conforme informação constante no preâmbulo do edital, não será aplicado as disposições constantes dos arts. 42 a 49 da LC 123/2006, nos termos do quanto disposto no §1º do art. 4º da Lei nº 14.133/2021.

3.5. A falsidade da declaração de que trata os itens 3.2 a 0 sujeitará o licitante às sanções previstas na Lei nº 14.133/2021 e neste Edital.

3.6. Os licitantes poderão retirar ou substituir a(s) proposta(s) inserida(s) no sistema, até a abertura da sessão pública.

3.7. Não haverá ordem de classificação na etapa de apresentação da proposta, o que ocorrerá somente após os procedimentos de abertura da sessão pública e da fase de envio de lances.

3.8. Serão disponibilizados para acesso público os documentos que compõem a proposta dos licitantes convocados para apresentação de propostas, após a fase de envio de lances.

3.9. Se o sistema assim permitir, o licitante poderá parametrizar o seu valor final mínimo ou o seu percentual de desconto máximo quando do cadastramento da proposta e obedecerá às seguintes regras:

3.9.1. a aplicação do intervalo mínimo de diferença de valores ou de percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação ao lance que cobrir a melhor oferta; e

3.9.2. os lances serão de envio automático pelo sistema, respeitado o valor final mínimo, caso estabelecido, e o intervalo de que trata o subitem acima.

3.10. O valor final mínimo ou o percentual de desconto final máximo parametrizado no sistema poderá ser alterado pelo fornecedor durante a fase de disputa, sendo vedado valor superior a lance já registrado pelo fornecedor no sistema, quando adotado o critério de julgamento por menor preço e percentual de desconto inferior a lance já registrado pelo fornecedor no sistema, quando adotado o critério de julgamento por maior desconto.

3.10.1. O valor final mínimo ou o percentual de desconto final máximo parametrizado na forma do item 03.9 possuirá caráter sigiloso para os demais fornecedores e para o órgão promotor da licitação, podendo ser disponibilizado estrita e permanentemente aos órgãos de controle externo e interno.

4. DO PREENCHIMENTO DA PROPOSTA

4.1. O licitante deverá enviar sua proposta mediante o preenchimento, no sistema eletrônico, dos seguintes campos, conforme o caso:

4.1.1. valor unitário e total do lote;

4.1.2. quantidade;

4.1.3. marca, fabricante.

4.1.4. *Poderá ser juntado ainda pelo licitante catálogos, prospectos, manuais, etc, que comprovem que o produto ofertado atende as especificações do edital, sendo vedado, contudo a apresentação de documentos que identifique o licitante, sob pena de desclassificação da proposta.*

4.2. Todas as especificações do objeto contidas na proposta vinculam o licitante.

4.2.1. Não será admitida a cotação de quantitativo inferior ao previsto para a contratação, salvo se devidamente expresso no Termo de Referência.

4.3. Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente na execução do objeto, de acordo com a Súmula 10[1] do TCE/SP, sendo que o proponente será responsável por quaisquer ônus decorrente: marcas, registros e patentes ao objeto cotado.

4.4. Os preços ofertados, tanto na proposta inicial, quanto na etapa de lances, serão de exclusiva responsabilidade do licitante, não lhe assistindo o direito de pleitear qualquer alteração, sob alegação de erro, omissão ou qualquer outro pretexto.

4.5. Se o regime tributário da empresa implicar o recolhimento de tributos em percentuais variáveis, a cotação adequada será a que corresponde à média dos efetivos recolhimentos da empresa nos últimos doze meses.

4.6. Independentemente do percentual de tributo inserido na planilha, no pagamento serão retidos na fonte os percentuais estabelecidos na legislação vigente.

4.7. Na presente licitação, a Microempresa e a Empresa de Pequeno Porte poderão se beneficiar do regime de tributação pelo Simples Nacional, desde que observado o disposto na legislação vigente (art. 17 e art. 18 da Lei Complementar nº 123/2006).

4.8. A apresentação das propostas implica obrigatoriedade do cumprimento das disposições nelas contidas, em conformidade com o que dispõe o Termo de Referência, assumindo o proponente o compromisso de executar o objeto licitado nos seus termos, bem como de fornecer os materiais, equipamentos, ferramentas e utensílios necessários, em quantidades e qualidades adequadas à perfeita execução contratual, promovendo, quando requerido, sua substituição.

4.9. O prazo de validade da proposta será de 90 (noventa) dias, contar da data de sua apresentação.

5. DA ABERTURA DA SESSÃO, CLASSIFICAÇÃO DAS PROPOSTAS E FORMULAÇÃO DE LANCES

5.1. A abertura da presente licitação dar-se-á automaticamente ou por permissão do pregoeiro em sessão pública, por meio de sistema eletrônico, na data, horário e local indicados no preâmbulo deste edital.

5.2. Os licitantes poderão retirar ou substituir a proposta, até o horário estabelecido no campo apresentação de proposta do quadro constante no preâmbulo do Edital.

5.3. O sistema disponibilizará campo próprio para troca de mensagens entre o pregoeiro e os licitantes.

5.4. Iniciada a etapa competitiva, os licitantes deverão encaminhar lances exclusivamente por meio de sistema eletrônico, sendo imediatamente informados do seu recebimento e do valor consignado no registro.

5.5. O lance deverá ser ofertado conforme critério de julgamento indicado no quadro constante no preâmbulo deste edital.

5.6. Os licitantes poderão oferecer lances sucessivos, observando o horário fixado para abertura da sessão e as regras estabelecidas no edital.

5.7. O licitante somente poderá oferecer lance de valor inferior ou percentual de desconto superior, conforme o caso, ao último por ele ofertado e registrado pelo sistema.

[1] Súmula nº 10: O preço final do produto ofertado pelos proponentes deve incluir os tributos e demais encargos a serem suportados pelo ofertante

5.8. O licitante poderá solicitar ao pregoeiro, via chat, a exclusão de seu último lance ofertado, no intervalo de quinze segundos após o registro no sistema, na hipótese de lance inconsistente ou inexeqüível.

5.9. O procedimento seguirá de acordo com o modo de disputa adotado e indicado no quadro do preâmbulo deste edital.

5.10. Caso seja adotado para o envio de lances no pregão eletrônico o modo de disputa **"aberto"**, os licitantes apresentarão lances públicos e sucessivos, com prorrogações.

5.10.1. A etapa de lances da sessão pública terá duração de 10 (dez) minutos e, após isso, será prorrogada automaticamente pelo sistema quando houver lance ofertado nos últimos 02 (dois) minutos do período de duração da sessão pública.

5.10.2. A prorrogação automática da etapa de lances, de que trata o subitem anterior, será de 02 (dois) minutos e ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive no caso de lances intermediários.

5.10.3. Não havendo novos lances na forma estabelecida nos itens anteriores, a sessão pública encerrar-se-á automaticamente, e o sistema ordenará e divulgará os lances conforme a ordem final de classificação.

5.11. Caso seja adotado para o envio de lances no pregão eletrônico o modo de disputa **"aberto e fechado"**, os licitantes apresentarão lances públicos e sucessivos, com lance final e fechado.

5.11.1. A etapa de lances da sessão pública terá duração inicial de 15 (quinze) minutos. Após esse prazo, o sistema encaminhará aviso de fechamento iminente dos lances, após o que transcorrerá o período de até 10 (dez) minutos, aleatoriamente determinado, findo o qual será automaticamente encerrada a recepção de lances.

5.11.2. Encerrado o prazo previsto no subitem anterior, o sistema abrirá oportunidade para que o autor da oferta de valor mais baixo e os das ofertas com preços até 10% (dez por cento) superiores àquela possam ofertar um lance final e fechado em até 05 (cinco) minutos, o qual será sigiloso até o encerramento deste prazo.

5.11.3. No procedimento de que trata o subitem supra, o licitante poderá optar por manter o seu último lance da etapa aberta, ou por ofertar melhor lance.

5.11.4. Não havendo pelo menos 03 (três) ofertas nas condições definidas neste item, poderão os autores dos melhores lances subsequentes, na ordem de classificação, até o máximo de três, oferecer um lance final e fechado em até 05 (cinco) minutos, o qual será sigiloso até o encerramento deste prazo.

5.11.5. Após o término dos prazos estabelecidos nos itens anteriores, o sistema ordenará e divulgará os lances segundo a ordem crescente de valores.

5.12. Caso seja adotado para o envio de lances no pregão eletrônico o modo de disputa **"fechado e aberto"**, poderão participar da etapa aberta somente os licitantes que apresentarem a proposta de menor preço ou maior desconto e os das propostas até 10% (dez por cento) superiores/inferiores àquela, em que os licitantes apresentarão lances públicos e sucessivos, até o encerramento da sessão e eventuais prorrogações.

5.12.1. Não havendo pelo menos 3 (três) propostas nas condições definidas no item 5.12, poderão os licitantes que apresentaram as 3 (três) melhores propostas, consideradas as empatadas, oferecer novos lances sucessivos.

5.12.2. A etapa de lances da sessão pública terá duração de 10 (dez) minutos e, após isso, será prorrogada automaticamente pelo sistema quando houver lance ofertado nos últimos 02 (dois) minutos do período de duração da sessão pública.

5.12.3. A prorrogação automática da etapa de lances, de que trata o subitem anterior, será de 02 (dois) minutos e ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive no caso de lances intermediários.

5.12.4. Não havendo novos lances na forma estabelecida nos itens anteriores, a sessão pública encerrar-se-á automaticamente, e o sistema ordenará e divulgará os lances conforme a ordem final de classificação.

5.12.5. Após o término dos prazos estabelecidos nos subitens anteriores, o sistema ordenará e divulgará os lances segundo a ordem crescente de valores ou decrescente de desconto, conforme o caso.

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

5.14. Durante o transcurso da sessão pública, os licitantes serão informados, em tempo real, do valor do menor lance ou maior desconto registrado, vedada a identificação do licitante.

5.15. 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.

5.16. Quando a desconexão do sistema eletrônico para o pregoeiro persistir por tempo superior a 10 (dez) minutos, a sessão pública será suspensa e reiniciada somente após decorridas 24 (vinte e quatro) horas da comunicação do fato pelo pregoeiro aos participantes, no sítio eletrônico do órgão promotor da licitação e do sistema do pregão.

5.17. Caso o licitante não apresente lances, concorrerá com o valor de sua proposta.

5.18. Em relação a itens não exclusivos para participação de microempresas e empresas de pequeno porte, uma vez encerrada a etapa de lances, será identificado pelo sistema as microempresas e empresas de pequeno porte participantes, procedendo à comparação com os valores da primeira colocada, se esta for empresa de maior porte, assim como das demais classificadas, para o fim de aplicar-se o disposto nos arts. 44 e 45 da Lei Complementar nº 123/2006.

5.18.1. Nessas condições, as propostas de microempresas e empresas de pequeno porte que se encontrarem na faixa de até 5% (cinco por cento) acima da melhor proposta ou melhor lance serão consideradas empatadas com a primeira colocada.

5.18.2. A melhor classificada nos termos do subitem anterior terá o direito de encaminhar uma última oferta para desempate, obrigatoriamente em valor inferior ao da primeira colocada, no prazo de 5 (cinco) minutos controlados pelo sistema, contados após a comunicação automática para tanto.

5.18.3. Caso a microempresa ou a empresa de pequeno porte melhor classificada desista ou não se manifeste no prazo estabelecido, serão convocadas as demais licitantes microempresa e empresa de pequeno porte que se encontrem naquele intervalo de 5% (cinco por cento), na ordem de classificação, para o exercício do mesmo direito, no prazo estabelecido no subitem anterior.

5.18.4. No caso de equivalência dos valores apresentados pelas microempresas e empresas de pequeno porte que se encontrem nos intervalos estabelecidos nos subitens anteriores, será realizado sorteio entre elas para que se identifique aquela que primeiro poderá apresentar melhor oferta.

5.18.5. Os procedimentos indicados nos itens 5.18 a 5.18.4 não serão levados em consideração quando o valor estimado da licitação superar o limite de enquadramento para empresa de pequeno porte, nos termos do §1º do art. 4º da Lei nº 14.1333/2021 e item 3.4.3 deste Edital.

5.19. Só poderá haver empate entre propostas iguais (não seguidas de lances), ou entre lances finais da fase fechada do modo de disputa aberto e fechado.

5.19.1. Havendo eventual empate entre propostas ou lances, o critério de desempate será aquele previsto no art. 60 da Lei nº 14.133/2021.

5.19.2. Persistindo o empate, será aplicado o disposto no §1º do art. 60 da Lei nº 14.133/2021.

5.20. Encerrada a etapa de envio de lances da sessão pública, na hipótese da proposta do primeiro colocado permanecer acima do preço máximo ou inferior ao desconto definido para a contratação, o pregoeiro poderá negociar condições mais vantajosas, após definido o resultado do julgamento.

5.20.1. No caso de licitação por lote, a contratação posterior de item específico que compõe o lote, serão observados os preços unitários máximos como critério de aceitabilidade.

5.20.2. Não será admitida a previsão de preços diferentes em razão de local de entrega ou de acondicionamento, tamanho de lote ou qualquer outro motivo, salvo no caso de situação excepcional a ser indicada no Termo de Referência.

5.20.3. A negociação poderá ser feita com os demais licitantes, segundo a ordem de classificação inicialmente estabelecida, quando o primeiro colocado, mesmo após a negociação, for desclassificado em razão de sua proposta permanecer acima do preço máximo definido pela Administração.

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

5.20.5. O resultado da negociação será divulgado a todos os licitantes e anexado aos autos do processo licitatório.

5.21. O pregoeiro solicitará ao licitante mais bem classificado que, no prazo de 2 (duas) horas, envie a proposta adequada ao último lance ofertado ou após a negociação realizada, acompanhada, se for o caso, dos documentos complementares, quando necessários à confirmação daqueles exigidos neste edital e já apresentados, prazo esse que é o mesmo para apresentação dos documentos de habilitação conforme disposto no item 7.5.

5.21.1. Poderá ser exigida ainda a decomposição dos custos unitários com os respectivos valores adequados ao valor final da sua proposta, sob pena de não aceitação da proposta.

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

5.22. Após o envio da proposta readequada, amostras (quando for o caso) e dos documentos de habilitação, o pregoeiro iniciará a fase de aceitação e julgamento da proposta.

6. DA FASE DE JULGAMENTO

6.1. Após o envio da proposta readequada e dos documentos de habilitação, o pregoeiro verificará se o licitante provisoriamente classificado em primeiro lugar atende às condições de participação no certame, conforme previsto no art. 14 da Lei nº 14.133/2021, legislação correlata e no item 0 do edital, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

6.1.1. Sistema Apenados mantido pelo Tribunal de Contas do Estado de São Paulo (https://www4.tce.sp.gov.br/apenados/publico/#/);

6.1.2. Cadastro Nacional de Empresas Inidôneas e Suspensas - CEIS, e Cadastro Nacional de Empresas Punidas - CNEP, disponíveis em https://certidoes.cgu.gov.br/.

6.2. Constatada a existência de sanção, o licitante será reputado inabilitado, por falta de condição de participação.

6.3. Caso o licitante provisoriamente classificado em primeiro lugar tenha se utilizado de algum tratamento favorecido às ME/EPPs, o pregoeiro verificará se faz jus ao benefício, em conformidade com o disposto neste edital.

6.4. Verificadas as condições de participação e de utilização do tratamento favorecido, o pregoeiro examinará a proposta classificada em primeiro lugar quanto à adequação ao objeto e à compatibilidade do preço em relação ao máximo estipulado para contratação neste edital e em seus anexos.

6.5. Será desclassificada a proposta vencedora que:

6.5.1. contiver vícios insanáveis;

6.5.2. não obedecer às especificações técnicas contidas no Termo de Referência;

apresentar preços inexequíveis ou permanecerem acima do preço máximo definido para a contratação;

6.5.3. não tiverem sua exequibilidade demonstrada, quando exigido pela Administração;

6.5.4. apresentar desconformidade com quaisquer outras exigências deste edital ou seus anexos, desde que insanável.

6.6. No caso de bens e serviços em geral, é indício de inexequibilidade das propostas valores inferiores a 50% (cinquenta por cento) do valor orçado pela Administração. A inexequibilidade, neste caso, só será considerada após diligência do pregoeiro, que comprove que o custo do licitante ultrapassa o valor da proposta e que inexistirem custos de oportunidade capazes de justificar o vulto da oferta.

6.7. No caso de serviços de engenharia, poderão ser consideradas inexequíveis as propostas cujos valores forem inferiores a 75% (setenta e cinco por cento) do valor orçado pela Administração, independentemente do regime de execução, devendo, contudo, a exequibilidade ser comprovada pela licitante quando da apresentação de sua proposta readequada.

6.8. Se houver indícios de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, poderão ser efetuadas diligências, para que a empresa comprove a exequibilidade da proposta.

6.9. Erros no preenchimento da planilha não constituem motivo para a desclassificação da proposta. A planilha poderá ser ajustada pelo fornecedor, no prazo indicado pelo sistema, desde que não haja majoração do preço e que se comprove que este é o bastante para arcar com todos os custos da contratação;

6.9.1. O ajuste de que trata este dispositivo se limita a sanar erros ou falhas que não alterem a substância das propostas.

6.10. Para fins de análise da proposta quanto ao cumprimento das especificações do objeto, poderá ser colhida a manifestação escrita do setor requisitante do serviço ou da área especializada no objeto.

6.11. Caso o Termo de Referência exija a apresentação de amostra, o licitante classificado em primeiro lugar deverá apresentá-la, conforme disciplinado no Termo de Referência, sob pena de não aceitação da proposta.

6.11.1. Os resultados das avaliações serão divulgados por meio de mensagem no sistema.

6.11.2. No caso de não haver entrega da amostra ou ocorrer atraso na entrega, sem justificativa aceita pelo Pregoeiro, ou havendo entrega de amostra fora das especificações previstas neste Edital, a proposta do licitante será recusada.

6.11.3. Se a(s) amostra(s) apresentada(s) pelo primeiro classificado não for(em) aceita(s), o Pregoeiro analisará a aceitabilidade da proposta ou lance ofertado pelo segundo classificado. Seguir-se-á com a verificação da(s) amostra(s) e, assim, sucessivamente, até a verificação de uma que atenda às especificações constantes no Termo de Referência.

7. DA FASE DE HABILITAÇÃO

7.1. Para fins de habilitação, nos termos dos arts. 62 a 70 da Lei 14.133/2021, serão exigidos os documentos previstos no Anexo I deste edital.

7.2. Na hipótese de não constar prazo de validade nas certidões apresentadas, serão aceitas como válidas as expedidas até 180 (cento e oitenta) dias imediatamente anteriores à data de apresentação das propostas.

7.3. Se o licitante for a matriz, todos os documentos deverão estar em nome da matriz, e se 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;

7.3.1. Caso o licitante pretenda que um de seus estabelecimentos, que não o participante desta licitação, execute o futuro contrato, deverá apresentar toda documentação de habilitação de ambos os estabelecimentos.

7.4. A verificação pelo pregoeiro, em sítios eletrônicos oficiais de órgãos e entidades emissores de certidões constitui meio legal de prova, para fins de habilitação.

7.5. Os documentos exigidos para habilitação deverão ser enviados por meio do sistema, em formato digital, no prazo de **2 (duas) horas**, prorrogável por igual período, juntamente com a proposta readequada conforme disposto no item 5.21.

7.6. Após a entrega dos documentos para habilitação, não será permitida a substituição ou a apresentação de novos documentos, salvo em sede de diligência, nos termos do art. 64 da Lei 14.133/2021 para:

7.6.1. complementação de informações acerca dos documentos já apresentados pelos licitantes e desde que necessária para apurar fatos existentes à época da abertura do certame; e

7.6.2. atualização de documentos cuja validade tenha expirado após a data de recebimento das propostas.

7.7. Na análise dos documentos de habilitação, o pregoeiro poderá sanar erros ou falhas, que não alterem a substância dos documentos e sua validade jurídica, mediante decisão fundamentada, registrada em ata e acessível a todos, atribuindo-lhes eficácia para fins de habilitação e classificação.

7.7.1. Verificada falha por parte do licitante acerca da juntada **de documento de qualificação fiscal, social e trabalhista** que ateste condição preexistente, fica autorizado o agente de contratação, pregoeiro ou comissão de contratação, conforme o caso, diligências necessárias a fim de complementar tais documentos, não sendo tal providência considerada inclusão posterior de documentos.

7.8. Na hipótese de o licitante não atender às exigências para habilitação, ele será inabilitado e o pregoeiro examinará a proposta subsequente e assim sucessivamente, na ordem de classificação, até a apuração de uma proposta que atenda ao presente edital, observado o prazo disposto no subitem 7.5.

7.9. A comprovação de regularidade fiscal e trabalhista das microempresas e empresas de pequeno porte somente será exigida para efeito de assinatura do contrato, porém, será obrigatória durante a fase de habilitação a apresentação dos documentos indicados no Anexo I, ainda que veiculem restrições impeditivas à referida comprovação.

7.9.1. Havendo alguma restrição na comprovação da regularidade fiscal e trabalhista das microempresas e empresas de pequeno porte, será assegurado o prazo de 5 (cinco) dias úteis, a contar da adjudicação e homologação do certame, prorrogáveis por igual período, a critério da Administração, para a regularização da documentação com emissão de certidões negativas ou positivas com efeito de negativas.

7.9.2. A não regularização da documentação no prazo previsto no item anterior implicará na decadência do direito à contratação, sem prejuízo das sanções legais, procedendo-se à convocação dos licitantes para, em sessão pública, retomar os atos referentes ao procedimento licitatório.

7.9.3. O benefício de que trata este item não serão aplicados quando o valor estimado da licitação superar o limite de enquadramento para empresa de pequeno porte, nos termos do §1º do art. 4º da Lei nº 14.1333/2021 e item 3.4.3 deste Edital.

7.10. Os documentos assinados digitalmente a partir de sistema informatizado prevendo acesso por meio de chave de identificação e senha do interessado ou com assinatura digital no padrão da infraestrutura de chaves públicas brasileira - ICP-Brasil possuem presunção legal de veracidade com os mesmos efeitos da assinatura manuscrita reconhecida em cartório, podendo a qualquer tempo ser solicitado ao licitante os respectivos arquivos para validação, se for o caso.

7.11. Constatado o cumprimento dos requisitos e condições estabelecidos no edital, o licitante será habilitado e declarado vencedor do certame.

7.12. Somente serão disponibilizados para acesso público os documentos de habilitação do licitante cuja proposta atenda ao edital de licitação, após concluídos os procedimentos de que trata o subitem anterior.

8. DA ADJUDICAÇÃO, DA HOMOLOGAÇÃO E FORMALIZAÇÃO DO CONTRATO

8.1. Decididos os recursos e constatada a regularidade dos atos procedimentais, a autoridade competente homologará e adjudicará o objeto ao vencedor, podendo revogar a licitação nos termos do artigo 71, IV da Lei n º 14.133/2021 e suas alterações posteriores.

8.1.1. O certame apenas será homologado/adjudicado para as pessoas jurídicas que atuarem no ramo de atividade compatível com o objeto da licitação.

8.2. Antes de formalizar ou prorrogar o prazo de vigência do contrato, a Administração deverá verificar a regularidade fiscal do contratado, consultar o Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e o Cadastro Nacional de Empresas Punidas (Cnep), emitir as certidões negativas de inidoneidade, de impedimento e de débitos trabalhistas e juntá-las ao respectivo processo.

8.3. Quando o proponente vencedor, convocado dentro do prazo de validade da sua proposta, não assinar o Contrato no prazo de 5 (cinco) dias úteis, contados da notificação, será convocado outro licitante, observada a ordem de classificação, e assim sucessivamente, sem prejuízo da aplicação das sanções cabíveis.

8.4. Juntamente com o instrumento contratual, a empresa deverá assinar o Termo de Ciência e de Notificação, Declaração de Documentos à Disposição do TCE-SP e apresentar o comprovante de cadastro no CadTCESP.

8.5. A recusa injustificada em assinar o contrato, aceitar ou retirar o instrumento equivalente, dentro do prazo estabelecido pela Administração, caracteriza o descumprimento total da obrigação assumida, sujeitando-o às penalidades legalmente estabelecidas, sendo que este disposto se aplica inclusive aos licitantes remanescentes, que não aceitarem a convocação, sem justificativa ou com justificativa recusada pela administração pública.

9. DOS RECURSOS

9.1. O prazo recursal é de 3 (três) dias úteis contados da data de intimação do pregoeiro ou de lavratura da ata e observará o disposto no art. 165 da Lei 14.133/2021.

9.2. Quando o recurso apresentado impugnar o julgamento das propostas ou o ato de habilitação ou inabilitação do licitante:

9.2.1. a intenção de recorrer deverá ser manifestada imediatamente, no prazo de 10 (dez) minutos, sob pena de preclusão;

9.2.2. o prazo de 3 (três) dias úteis para apresentação das razões recursais será iniciado na data de intimação ou de lavratura da ata de habilitação ou inabilitação que ocorrerá exclusivamente pelo sistema;

9.2.3. o prazo para apresentação de contrarrazões ao recurso pelos demais licitantes será de 3 (três) dias úteis, contados da data da divulgação da interposição do recurso a ser realizada pelo sistema, assegurada a vista imediata dos elementos indispensáveis à defesa de seus interesses.

9.3. Os recursos deverão ser encaminhados em campo próprio do sistema, através do e-mail da pregoeira tassia.suprimentos@americana.sp.gov.br ou na Prefeitura Municipal de Americana, Protocolo Geral, à Av. Brasil, n.º 85 – Térreo – Centro – Americana (SP).

9.4. O recurso será dirigido ao pregoeiro ou à autoridade que proferiu a decisão recorrida, que poderão reconsiderar sua decisão no prazo de 3 (três) dias úteis, ou, nesse mesmo prazo, encaminhar recurso para a autoridade superior, a qual deverá proferir sua decisão no prazo de 10 (dez) dias úteis, contado do recebimento dos autos.

9.5. Os recursos interpostos fora do prazo não serão conhecidos.

9.6. O recurso e o pedido de reconsideração terão efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente.

9.7. O acolhimento do recurso invalida tão somente os atos insuscetíveis de aproveitamento.

10. DAS INFRAÇÕES ADMINISTRATIVAS E SANÇÕES

10.1. Comete infração administrativa, nos termos da lei, o licitante que, com dolo ou culpa:

10.1.1. deixar de entregar a documentação exigida para o certame ou não entregar qualquer documento que tenha sido solicitado pelo/a pregoeiro/a durante o certame;

10.1.2. salvo em decorrência de fato superveniente devidamente justificado, não mantiver a proposta em especial quando:

10.1.2.1. não enviar a proposta adequada ao último lance ofertado ou após a negociação;

10.1.2.2. recusar-se a enviar o detalhamento da proposta quando exigível;

10.1.2.3. pedir para ser desclassificado quando encerrada a etapa competitiva;

10.1.2.4. deixar de apresentar amostra, se for o caso;

10.1.2.5. apresentar proposta ou amostra em desacordo com as especificações do edital;

10.1.3. não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta, inclusive quanto a documentação visando a comprovação de regularidade fiscal e trabalhista das micro e pequenas empresas;

10.1.3.1. recusar-se, sem justificativa, a assinar o contrato ou a ata de registro de preço, ou a aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração;

10.1.4. apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação;

10.1.5. fraudar a licitação;

10.1.6. comportar-se de modo inidôneo ou cometer fraude de qualquer natureza, em especial quando:

10.1.6.1. agir em conluio ou em desconformidade com a lei;

10.1.6.2. induzir deliberadamente a erro no julgamento;

10.1.6.3. apresentar amostra falsificada ou deteriorada;

101.7. praticar atos ilícitos com vistas a frustrar os objetivos da licitação;

10.1.8. praticar ato lesivo previsto no art. 5º da Lei nº 12.846/2013;

10.1.9. dar causa à inexecução parcial do contrato/ata;

10.1.10. dar causa à inexecução parcial do contrato/ata que cause grave dano à administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;

10.1.11. dar causa à inexecução total do contrato/ata.

10.2. Com fulcro na Lei nº 14.133/2021, a Administração poderá, garantida a prévia defesa, aplicar aos licitantes e/ou adjudicatários as seguintes sanções, sem prejuízo das responsabilidades civil e criminal:

102.2.1. advertência;

10.2.2. multa;

10.2.3. impedimento de licitar e contratar e

10.2.4. declaração de inidoneidade para licitar ou contratar.

10.3. A multa será recolhida nos percentuais abaixo indicados, incidentes sobre o valor da proposta inicial do licitante que deu causa a infração, recolhida no prazo máximo de 30 (trinta) dias úteis, a contar da comunicação oficial.

10.3.1. para as infrações previstas nos itens 10.1.10 e 10.1.2, a multa será de a multa será de 10%;

10.3.2. para as infrações previstas nos itens 10.1.3, 10.1.9, 10.1.10 e 10.1.11 a multa será de 20%;

10.3.3. para as infrações previstas nos itens 10.1.4, 10.1.5, 10.1.6, 10.1.7 e 10.1.8 a multa será de 30%.

10.4. As sanções de advertência, impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar poderão ser aplicadas, cumulativamente ou não, à penalidade de multa.

10.5. Na aplicação da sanção de multa e advertência será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação.

10.6. A recusa injustificada do adjudicatário em assinar o contrato ou a ata de registro de preço, ou em aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração, descrita no item 10.1.3, caracterizará o descumprimento total da obrigação assumida e o sujeitará às penalidades e à imediata perda da garantia de proposta em favor do órgão promotor da licitação, se for o caso.

10.7. A apuração de responsabilidade relacionadas às sanções de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar demandará a instauração de processo de responsabilização nos termos do art. 158 da Lei nº 14.133/2021.

10.8. Caberá recurso no prazo de 15 (quinze) dias úteis da aplicação das sanções de advertência, multa e impedimento de licitar e contratar, contado da data da intimação, o qual será dirigido à autoridade que tiver proferido a decisão recorrida, que, se não a reconsiderar no prazo de 5 (cinco) dias úteis, encaminhará o recurso com sua motivação à autoridade superior, que deverá proferir sua decisão no prazo máximo de 20 (vinte) dias úteis, contado do recebimento dos autos.

10.9. Caberá a apresentação de pedido de reconsideração da aplicação da sanção de declaração de inidoneidade para licitar ou contratar no prazo de 15 (quinze) dias úteis, contado da data da intimação, e decidido no prazo máximo de 20 (vinte) dias úteis, contado do seu recebimento.

10.10. O recurso e o pedido de reconsideração terão efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente.

10.11. A aplicação das sanções previstas neste edital não exclui, em hipótese alguma, a obrigação de reparação integral dos danos causados ao município.

11. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

11.1. Qualquer pessoa é parte legítima para impugnar este Edital por irregularidade na aplicação da Lei nº 14.133/2021, devendo apresentar o pedido até 3 (três) dias úteis antes da data da abertura do certame.

11.2. A impugnação e o pedido de esclarecimento poderão ser realizados por forma eletrônica através do próprio sistema eletrônico do pregão, pelo e-mail indicado no quadro constante no preâmbulo deste edital ou na Prefeitura Municipal de Americana, Protocolo Geral, à Av. Brasil, n.º 85 – Térreo – Centro – Americana (SP).

11.3. A resposta à impugnação ou ao pedido de esclarecimento será divulgado no sítio eletrônico oficial do órgão promotor da licitação e no sistema eletrônico do pregão, no prazo de até 3 (três) dias úteis, limitado ao último dia útil anterior à data da abertura do certame.

11.4. As impugnações e pedidos de esclarecimentos não suspendem os prazos previstos no certame.

11.5. Acolhida a impugnação, será definida e publicada nova data para a realização do certame.

12. DOS RECURSOS ORÇAMENTÁRIOS

12.1. As despesas decorrentes desta licitação onerarão as dotações orçamentárias do corrente exercício:

- 02.23.01.33.90.40 – Ficha 1627 – Secretaria de Comunicação e Tecnologia da Informação;

- 02.14.06.3390.40 - Fichas 1406, 1409 e 1420 – Secretaria de Saúde.

13. DAS DISPOSIÇÕES GERAIS

13.1. Será divulgada ata da sessão pública no sistema eletrônico.

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

13.3. Todas as referências de tempo no Edital, no aviso e durante a sessão pública observarão o horário de Brasília - DF.

13.4. A homologação do resultado desta licitação não implicará direito à contratação.

13.5. As normas disciplinadoras da licitação serão sempre interpretadas em favor da ampliação da disputa entre os interessados, desde que não comprometam o interesse da Administração, o princípio da isonomia, a finalidade e a segurança da contratação.

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

13.7. Na contagem dos prazos estabelecidos neste edital e seus Anexos, excluir-se-á o dia do início e incluir-se-á o do vencimento. Só se iniciam e vencem os prazos em dias de expediente na Administração.

13.8. O desatendimento de exigências formais não essenciais não importará o afastamento do licitante, desde que seja possível o aproveitamento do ato, observados os princípios da isonomia e do interesse público.

13.9. Em caso de divergência entre disposições deste Edital e de seus anexos ou demais peças que compõem o processo, prevalecerá as deste Edital.

13.10. O Edital e seus anexos estão disponíveis, na íntegra, no Portal Nacional de Contratações Públicas (PNCP), no sítio oficial www.americana.sp.gov.br e na plataforma eletrônico do pregão.

13.11. Integram este Edital, para todos os fins e efeitos, os seguintes anexos:

ANEXO I – Documentos de Habilitação

ANEXO I A - Declarações

ANEXO II - Minuta do Contrato

ANEXO III - Termo de Referência

ANEXO III – A – Relação de Endereços e Velocidades

ANEXO IV – Modelo de Proposta

Americana, 04 de novembro de 2025.

_____

José Eduardo da Cruz Rodrigues Flores

Secretário Adjunto de Administração

PROCESSO N.º 9.444/2025

PREGÃO ELETRÔNICO Nº 131/2025

ANEXO I – DOCUMENTOS DE HABILITAÇÃO

1. HABILITAÇÃO JURÍDICA (art. 66 da Lei 14.133/2021)

a) Registro empresarial na Junta Comercial, no caso de empresário individual (ou cédula de identidade em se tratando de pessoa física não empresária);

b) Ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado na Junta Comercial, tratando-se de sociedade empresária;

c) Documentos de eleição ou designação dos atuais administradores, tratando-se de sociedade empresária;

d) Ato constitutivo devidamente registrado no Registro Civil de Pessoas Jurídicas tratando-se de sociedade não empresária, acompanhado de prova da diretoria em exercício;

e) Decreto de autorização, tratando-se de sociedade estrangeira no país, e ato de registro ou autorização para funcionamento, expedidos por órgão competente, quando a atividade assim o exigir;

f) Comprovante de Inscrição do Microempreendedor Individual – MEI

1.1. Os documentos acima deverão ser apresentados com todas as suas alterações, excluindo-se os casos de documentos expressamente consolidados.

2. HABILITAÇÃO FISCAL E TRABALHISTA (art. 68 da Lei 14.133/2021)

a) Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas do Ministério da Fazenda (CNPJ) ou no Cadastro de Pessoas Físicas (CPF);

b) Prova de inscrição no Cadastro de Contribuintes Estadual e/ou Municipal, relativa à sede ou ao domicílio do licitante, pertinente ao seu ramo de atividade e compatível com o objeto do certame;

c) Certidão Conjunta Negativa de Débitos ou Positiva com efeito de Negativa, relativa a Tributos Federais (inclusive às contribuições sociais) e à Dívida Ativa da União;

d) Certidão de regularidade de débito com a Fazenda Estadual, referente ao ICMS, se incidente sobre o objeto desta licitação;

e) Certidão de regularidade de débito com a Fazenda Municipal, da sede ou do domicílio do licitante, relativa aos tributos mobiliários e incidentes sobre o objeto desta licitação;

f) Certidão de regularidade de débito para com o Fundo de Garantia por Tempo de Serviço (FGTS) e

g) Certidão Negativa de Débitos Trabalhistas - CNDT ou Positiva de Débitos Trabalhistas com Efeito de Negativa.

3. HABILITAÇÃO TÉCNICA (art. 67 da Lei 14.133/2021)

a) Comprovação da capacitação técnico-operacional, emitido(s) por pessoa jurídica de direito público ou privado, que comprove(m) o fornecimento da solução de antivírus corporativo, em quantidade e complexidade compatíveis com o objeto desta contratação.

4. HABILITAÇÃO ECONÔMICO-FINANCEIRA (art. 69 da Lei 14.133/2021)

a) Certidão negativa de falência expedida pelo distribuidor da sede da pessoa jurídica;

b) Comprovação de capital social ou patrimônio líquido registrado e integralizado igual ou superior a 10% do valor do serviço**,** até a data designada para abertura das propostas, admitida a atualização até essa data, através de índices oficiais, podendo ser comprovado sob a forma de qualquer das modalidades, a saber:

b.1) Último Instrumento de Alteração Contratual, devidamente registrado;
b.2) Balanço apresentado na forma da lei;
b.3) Certidão de Breve relato expedida pela Junta Comercial;

5. OUTRAS COMPROVAÇÕES

Declaração subscrita pelo representante legal do licitante, conforme modelo Anexo I – A, elaborada em papel timbrado, atestando que:

a) atende aos requisitos de habilitação definidos no instrumento convocatório, e que responderá pela veracidade das informações prestadas, na forma da lei (art. 63, I da Lei nº 14.133/2021);

b) cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas (art. 63, IV da Lei nº 14.133/2021);

c) suas propostas econômicas compreendem a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de entrega das propostas (art. 63, §1º da Lei nº 14.133/2021);

d) não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do art. 7º, XXXIII, da Constituição Federal (art. 68, VI da Lei nº 14.133/2021);

e) não possui empregados executando trabalho degradante ou forçado, observando o disposto nos incisos III e IV do art. 1º e no inciso III do art. 5º da Constituição Federal;

f) está ciente da obrigação de manter o endereço da empresa atualizado junto ao órgão promotor da licitação, e de que as notificações e comunicações formais decorrentes da execução do contrato serão efetuadas no endereço que constar em seu preâmbulo. Caso a empresa não seja encontrada, será notificada pelo Diário Oficial do Município acessível em www.americana.sp.gov.br

g) no caso de microempresas ou empresas de pequeno porte: a empresa não possui qualquer dos impedimentos previstos nos §§ 4º e seguintes todos do artigo 3º da Lei Complementar nº 123, de 14 de dezembro de 2006, e alterações, assim como §§ 1º a 4º do art. 4º da Lei 14.133/2021, cujos termos declara conhecer na íntegra;

h) não se enquadra em nenhuma das restrições de participação, conforme art. 14 da Lei nº 14.133/2021 e item 2.10 do edital;

i) está ciente sobre a observação das disposições da Lei Federal nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), e alterações, quando do tratamento de dados pessoais e dados pessoais sensíveis a que tenha acesso, para o propósito de execução e acompanhamento do Contrato, não podendo divulgar, revelar, produzir, utilizar ou deles dar conhecimento a terceiros estranhos a esta contratação, a não ser por força de obrigação legal ou regulatória.

ANEXO I – A

MODELO DE DECLARAÇÃO

Ref.: **PROCESSO N.º 9.444/2025**

PREGÃO ELETRÔNICO Nº 131/2025

, inscrita no CNPJ sob o nº , sediada na , por meio de seu representante legal abaixo identificado, DECLARA, sob as penas da Lei, que atende aos requisitos de habilitação definidos no instrumento convocatório, e que responderá pela veracidade das informações prestadas, na forma da lei (art. 63, I da Lei nº 14.133/2021) e declara ainda que:

a) atende aos requisitos de habilitação definidos no instrumento convocatório, e que responderá pela veracidade das informações prestadas, na forma da lei (art. 63, I da Lei nº 14.133/2021);

b) cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas (art. 63, IV da Lei nº 14.133/2021);

c) suas propostas econômicas compreendem a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de entrega das propostas (art. 63, §1º da Lei nº 14.133/2021);

d) não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do art. 7º, XXXIII, da Constituição Federal (art. 68, VI da Lei nº 14.133/2021);

e) não possui empregados executando trabalho degradante ou forçado, observando o disposto nos incisos III e IV do art. 1º e no inciso III do art. 5º da Constituição Federal;

f) está ciente da obrigação de manter o endereço da empresa atualizado junto ao órgão promotor da licitação, e de que as notificações e comunicações formais decorrentes da execução do contrato serão efetuadas no endereço que constar em seu preâmbulo. Caso a empresa não seja encontrada, será notificada pelo Diário Oficial do Município acessível em www.americana.sp.gov.br

g) no caso de microempresas ou empresas de pequeno porte: a empresa não possui qualquer dos impedimentos previstos nos §§ 4º e seguintes todos do artigo 3º da Lei Complementar nº 123, de 14 de dezembro de 2006, e alterações, assim como §§ 1º a 4º do art. 4º da Lei 14.133/2021, cujos termos declara conhecer na íntegra;

h) não se enquadra em nenhuma das restrições de participação, conforme art. 14 da Lei nº 14.133/2021 e item 2.10 do edital;

i) está ciente sobre a observação das disposições da Lei Federal nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), e alterações, quando do tratamento de dados pessoais e dados pessoais sensíveis a que tenha acesso, para o propósito de execução e acompanhamento do Contrato, não podendo divulgar, revelar, produzir, utilizar ou deles dar conhecimento a terceiros estranhos a esta contratação, a não ser por força de obrigação legal ou regulatória.

, de de .

_____

(Identificação e assinatura do representante legal da proponente)

PROCESSO N.º 9.444/2025

PREGÃO ELETRÔNICO Nº 131/2025

ANEXO II - MINUTA DO CONTRATO

O **MUNICÍPIO DE AMERICANA**, com sede na Av. Brasil, 85, Centro, Americana/SP, inscrita no CNPJ sob o nº 45.781.176/0001-66, doravante denominado CONTRATANTE, neste ato representada pelo Sr. Xxxxx, Secretário Municipal de xxxxxx, conforme poderes delegados no Decreto Municipal nº 12.918/2022, e a inscrita no CNPJ sob o nº , com sede , município de , doravante designada CONTRATADA, neste ato representada por *(nome e função no contratado)*, conforme atos constitutivos da empresa OU procuração apresentada nos autos, tendo em vista o que consta no Processo **nº 9.444/2025** e em observância às disposições da Lei nº 14.133/2021 e Decreto Municipal nº 13.826/2025, resolvem celebrar o presente Termo de Contrato, decorrente do Pregão Eletrônico nº **131/2025**, mediante as cláusulas e condições a seguir enunciadas.

CLÁUSULA PRIMEIRA – OBJETO (art. 92, I e II)

1.1. O objeto do presente instrumento é a **SERVIÇOS DE LICENÇA DE USO DE 1.050 LICENÇAS DE ENDPOINT VISION ONE 03 LICENÇAS DE PROTEÇÃO CLOUD VISION ONE – TREND MICRO, DESTINADAS À PROTEÇÃO DAS ESTAÇÕES DE TRABALHO E SERVIDORES EM NUVEM DE ESTAÇÕES DE TRABALHO, SERVIDORES E SERVIÇOS EM NUVEM, A SEREM UTILIZADAS EM TODA A ESTRUTURA DA ADMINISTRAÇÃO MUNICIPAL,** nas condições estabelecidas no Termo de Referência.

1.2. Objeto da contratação:

ITEM	Unid.	DESCRIÇÃO	Quant.	VALOR UNITÁRIO R$	VALOR TOTAL R$
1	serv.	RENOVAÇÃO LICENÇA DE USO DE PROGRAMAS DE COMPUT.TREND VISION ONE – ENDPOINT SECURITY (CORE) ESTAÇÕES DE TRABALHO. **RENEW - Part Number – VORA0026**	**650**		
2	serv.	RENOVAÇÃO LICENÇA DE USO DE PROGRAMAS DE COMPUT. TREND VISION ONE – ENDPOINT SECURITY (PRO-CLOUD) SERVIDORES. **RENEW - Part Number – VORA0041**	**3**		
3	serv.	AQUISIÇÃO LICENÇA DE USO DE PROGRAMAS DE COMPUT. - TREND VISION ONE - ENDPOINT SECURITY (CORE) ESTAÇÕES DE TRABALHO. **NEW - Part Number – VONA0028**	**400**		
		VALOR GLOBAL R$			

1.3. São anexos a este instrumento e vinculam esta contratação, independentemente de transcrição: O Termo de Referência que embasou a contratação, a Proposta do Contratado; e Eventuais anexos dos documentos supracitados.

CLÁUSULA SEGUNDA – VIGÊNCIA E PRORROGAÇÃO.

2.1. O prazo de vigência da contratação é de 02 (dois) anos contados do(a) assinatura, prorrogável nos termos do artigo 107, da Lei Federal n° 14.133/2021.

2.1.1. A prorrogação de que trata este item é condicionada ao ateste, pela autoridade competente, de que as condições e os preços permanecem vantajosos para a Administração, permitida a negociação com o contratado.

CLÁUSULA TERCEIRA – MODELOS DE EXECUÇÃO E GESTÃO CONTRATUAIS (art. 92, IV, VII e XVIII)

3.1. O regime de execução contratual, o modelo de gestão, assim como os prazos e condições de conclusão, entrega, observação e recebimento definitivo constam no Termo de Referência, anexo a este Contrato e Decreto Municipal nº 13.826/2025.

CLÁUSULA QUARTA - SUBCONTRATAÇÃO

4.1. É permitida a subcontratação parcial do objeto, até o limite de 30% (trinta por cento) do valor total do contrato e depende de autorização prévia da Contratante, a quem incumbe avaliar se a subcontratada cumpre os requisitos de qualificação técnica necessários para a execução do objeto.

4.1.1. É vedada a subcontratação completa ou da parcela principal da obrigação:

4.1.2. Em qualquer hipótese de subcontratação, permanece a responsabilidade integral da Contratada pela perfeita execução contratual, cabendo-lhe realizar a supervisão e coordenação das atividades da subcontratada, bem como responder perante a Contratante pelo rigoroso cumprimento das obrigações contratuais correspondentes ao objeto da subcontratação.

4.2. É vedada a subcontratação de pessoa física ou jurídica, se aquela ou os dirigentes desta mantiverem vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que desempenhe função na contratação ou atue na fiscalização ou na gestão do contrato, ou se deles forem cônjuge, companheiro ou parente em linha reta, colateral, ou por afinidade, até o terceiro grau.

CLÁUSULA QUINTA – PAGAMENTO (art. 92, V e VI)

5.1. PREÇO

5.1.1. Face ao disposto na cláusula primeira, e de acordo com a proposta apresentada, a **“CONTRATANTE"** ajusta com a **"CONTRATADA"** os serviços objeto da licitação pelo valor unitário descrito na tabela acima, perfazendo o valor global de R$ ( ).

5.1.2. No valor acima estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução do objeto, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação.

5.2. FORMA DE PAGAMENTO

5.2.1. O pagamento será realizado através de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo contratado.

5.3. PRAZO DE PAGAMENTO

5.3.1. O pagamento será efetuado no prazo máximo de até 30 (trinta) dias, contados do recebimento da Nota Fiscal/Fatura.

5.3.2. Considera-se ocorrido o recebimento da nota fiscal ou fatura quando o órgão contratante atestar a execução do objeto do contrato.

5.3.3. No caso de atraso pelo Contratante, os valores devidos ao contratado serão atualizados monetariamente entre o termo final do prazo de pagamento até a data de sua efetiva realização, mediante aplicação do índice IPCA de correção monetária.

5.4. CONDIÇÕES DE PAGAMENTO

5.4.1. A emissão da Nota Fiscal/Fatura será precedida do recebimento definitivo do objeto da contratação, conforme disposto neste instrumento e/ou no Termo de Referência. Quando houver glosa parcial do objeto, o contratante deverá comunicar a empresa para que emita a nota fiscal ou fatura com o valor exato dimensionado.

5.4.2. Havendo erro na apresentação da Nota Fiscal/Fatura, ou circunstância que impeça a liquidação da despesa, o pagamento ficará sobrestado até que o contratado providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para o contratante;

5.4.3. A Nota Fiscal ou Fatura deverá ser obrigatoriamente acompanhada da comprovação da regularidade fiscal, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 68 da Lei nº 14.133/2021.

5.4.3.1. Previamente a cada pagamento, a Administração deverá realizar consulta para verificar a manutenção das condições de habilitação exigidas na contratação;

5.4.3.2. Constatando-se a situação de irregularidade do contratado, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério do contratante.

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

5.4.3.4. Persistindo a irregularidade, o contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada ao contratado a ampla defesa.

5.4.3.5. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso o contratado não regularize sua situação.

5.4.3.6. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável. Independentemente do percentual de tributo inserido na planilha, no pagamento serão retidos na fonte os percentuais estabelecidos na legislação vigente.

5.4.3.7. O contratado regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

CLÁUSULA SEXTA - REAJUSTE (art. 92, V)

6.1. Os preços inicialmente contratados são fixos e irreajustáveis no prazo de um ano contado da data do orçamento estimado, em **29/09/2025**.

6.2. Após o interregno de um ano, e independentemente de pedido do Contratado, os preços iniciais serão reajustados, mediante a aplicação, pelo Contratante, do índice IPCA, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade

6.3. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

6.4. No caso de atraso ou não divulgação do(s) índice (s) de reajustamento, o Contratante pagará ao Contratado a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja(m) divulgado(s) o(s) índice(s) definitivo(s).

6.5. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.

6.6. O reajuste será realizado por apostilamento.

CLÁUSULA SÉTIMA - OBRIGAÇÕES DO CONTRATANTE (art. 92, X, XI e XIV)

7.1. São obrigações do Contratante:

7.1.1. Exigir o cumprimento de todas as obrigações assumidas pelo Contratado, de acordo com o contrato e seus anexos;

7.1.2. Receber o objeto no prazo e condições estabelecidas no Termo de Referência e Decreto Municipal nº 13.826/2025;

7.1.3. Notificar o Contratado, por escrito, sobre vícios, defeitos ou incorreções verificadas no objeto fornecido, para que seja por ele substituído, reparado ou corrigido, no total ou em parte, às suas expensas;

7.1.4. Acompanhar e fiscalizar a execução do contrato e o cumprimento das obrigações pelo Contratado;

7.1.5. Efetuar o pagamento ao Contratado do valor correspondente ao fornecimento do objeto ou prestação dos serviços, no prazo, forma e condições estabelecidos no presente Contrato;

7.1.6. Aplicar ao Contratado sanções motivadas pela inexecução total ou parcial do Contrato;

7.1.7. Cientificar a procuradoria do município para adoção das medidas cabíveis quando do descumprimento de obrigações pelo Contratado;

7.1.8. Explicitamente emitir decisão sobre todas as solicitações e reclamações relacionadas à execução do presente Contrato, ressalvados os requerimentos manifestamente impertinentes, meramente protelatórios ou de nenhum interesse para a boa execução do ajuste.

7.1.9. Concluída a instrução do requerimento, a Administração terá o prazo de 30 (trinta) dias para decidir, admitida a prorrogação motivada por igual período.

7.1.10. Notificar os emitentes das garantias quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais, se for o caso.

7.1.11. Comunicar o Contratado na hipótese de posterior alteração do projeto pelo Contratante, no caso do art. 93, §2º, da Lei nº 14.133/21, se for o caso.

7.2. A Administração não responderá por quaisquer compromissos assumidos pelo Contratado com terceiros, ainda que vinculados à execução do contrato, bem como por qualquer dano causado a terceiros em decorrência de ato do Contratado, de seus empregados, prepostos ou subordinados.

CLÁUSULA OITAVA - OBRIGAÇÕES DO CONTRATADO (art. 92, XIV, XVI e XVII)

8.1. O Contratado deve cumprir todas as obrigações constantes deste Contrato, em seus anexos, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto, observando, ainda, as obrigações a seguir dispostas:

8.1.1. Manter preposto aceito pela Administração no local da obra ou do serviço para representá-lo na execução do contrato. A indicação ou a manutenção do preposto da empresa poderá ser recusada desde que devidamente justificada, devendo a empresa designar outro para o exercício da atividade.

8.1.2. Atender às determinações regulares emitidas pelo fiscal do contrato ou autoridade superior (art. 137, II);

8.1.3. Alocar os empregados necessários, com habilitação e conhecimento adequados, ao perfeito cumprimento das cláusulas deste contrato, fornecendo os materiais, equipamentos, ferramentas e utensílios demandados, cuja quantidade, qualidade e tecnologia deverão atender às recomendações de boa técnica e a legislação de regência;

8.1.4. Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os serviços nos quais se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;

8.1.5. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, bem como por todo e qualquer dano causado à Administração ou terceiros, não reduzindo essa responsabilidade a fiscalização ou o acompanhamento da execução contratual pelo Contratante, que ficará autorizado a descontar dos pagamentos devidos ou da garantia, caso exigida no edital, o valor correspondente aos danos sofridos;

8.1.6. Não contratar, durante a vigência do contrato, cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, de dirigente do contratante ou do Fiscal ou Gestor do contrato, nos termos do artigo 48, parágrafo único, da Lei nº 14.133, de 2021;

8.1.7. Quando não for possível a verificação da regularidade fiscal, a empresa contratada deverá entregar ao setor responsável pela fiscalização do contrato, até o dia trinta do mês seguinte ao da prestação dos serviços, os seguintes documentos:

a) prova de regularidade perante a Fazenda Municipal (mobiliários), especialmente quando o proponente possuir domicílio ou sede no município;

b) prova de regularidade relativa à Seguridade Social e ao FGTS, que demonstre cumprimento dos encargos sociais instituídos por lei;

c) prova de regularidade perante a Justiça do Trabalho.

8.1.8. Responsabilizar-se pelo cumprimento das obrigações previstas em Acordo, Convenção, Dissídio Coletivo de Trabalho ou equivalentes das categorias abrangidas pelo contrato, por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas em legislação específica, cuja inadimplência não transfere a responsabilidade ao Contratante;

8.1.9. Comunicar ao Fiscal do contrato, no prazo de 24 (vinte e quatro) horas, qualquer ocorrência anormal ou acidente que se verifique no local dos serviços;

8.1.10. Prestar todo esclarecimento ou informação solicitada pelo Contratante ou por seus prepostos, garantindo-lhes o acesso, a qualquer tempo, ao local dos trabalhos, bem como aos documentos relativos à execução do empreendimento;

8.1.11. Paralisar, por determinação do Contratante, qualquer atividade que não esteja sendo executada de acordo com a boa técnica ou que ponha em risco a segurança de pessoas ou bens de terceiros;

8.1.12. Promover a guarda, manutenção e vigilância de materiais, ferramentas, e tudo o que for necessário à execução do objeto, durante a vigência do contrato;

8.1.13. Conduzir os trabalhos com estrita observância às normas da legislação pertinente, cumprindo as determinações dos Poderes Públicos, mantendo sempre limpo o local dos serviços e nas melhores condições de segurança, higiene e disciplina;

8.1.14. Submeter previamente, por escrito, ao Contratante, para análise e aprovação, quaisquer mudanças nos métodos executivos que fujam às especificações do memorial descritivo ou instrumento congênere;

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

8.1.16. Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições exigidas para habilitação na licitação, ou para qualificação, na contratação direta;

8.1.17. Cumprir, durante todo o período de execução do contrato, a reserva de cargos prevista em lei para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz, bem como as reservas de cargos previstas na legislação (art. 116);

8.1.18. Comprovar a reserva de cargos a que se refere a cláusula acima, no prazo fixado pelo fiscal do contrato, com a indicação dos empregados que preencheram as referidas vagas (art. 116, parágrafo único);

8.1.19. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato;

8.1.20. Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto da contratação, exceto quando ocorrer algum dos eventos arrolados no art. 124, II, d, da Lei nº 14.133, de 2021;

8.1.21. Cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança do Contratante.

CLÁUSULA NONA- OBRIGAÇÕES PERTINENTES À LGPD –

As partes deverão cumprir a Lei nº 13.709/2018 (LGPD), quanto a todos os dados pessoais a que tenham acesso em razão do certame ou do contrato administrativo que eventualmente venha a ser firmado, a partir da apresentação da proposta no procedimento de contratação, independentemente de declaração ou de aceitação expressa. Os dados obtidos somente poderão ser utilizados para as finalidades que justificaram seu acesso e de acordo com a boa-fé e com os princípios do art. 6º da LGPD.

CLÁUSULA DÉCIMA – GARANTIA DE EXECUÇÃO (art. 92, XII e XIII)

10.1. Não haverá exigência de garantia contratual da execução.

CLÁUSULA DÉCIMA PRIMEIRA – INFRAÇÕES E SANÇÕES ADMINISTRATIVAS (art. 92, XIV)

11.1. Comete infração administrativa, o Contratado que praticar qualquer uma das condutas elencadas no art. 155 da Lei nº 14.133/2021.

11.2. Serão aplicadas ao responsável pelas infrações administrativas acima descritas as seguintes sanções:

11.2.1. Advertência, quando o Contratado der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave (art. 156, §2º, da Lei);

11.2.2. Impedimento de licitar e contratar, quando praticadas as condutas descritas nos incisos II, III, IV, V, VI e VII do artigo 155 da Le 14.133/21, sempre que não se justificar a imposição de penalidade mais grave (art. 156, §4º, da Lei);

11.2.3. Declaração de inidoneidade para licitar e contratar, quando praticadas as condutas descritas nos incisos VIII, IX, X, XI e XII do artigo 155 da Le 14.133/21, bem como incisos II, III, IV, V, VI e VII do artigo 155 da Lei 14.133/21, que justifiquem a imposição de penalidade mais grave (art. 156, §5º, da Lei)

11.2.4. Multa:

a) moratória de 1 % (um por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 15 (quinze) dias. O atraso superior a 15 dias autoriza a Administração a promover a rescisão do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõe o inciso I do art. 137 da Lei n. 14.133/2021.

b) compensatória de 20% (vinte por cento) sobre o valor total do contrato, no caso de inexecução total do objeto;

11.2.5. A aplicação das sanções previstas neste Contrato não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado à Contratante (art. 156, §9º).

11.2.6. Todas as sanções previstas neste Contrato poderão ser aplicadas cumulativamente com a multa (art. 156, §7º).

11.2.7. Antes da aplicação da multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação (art. 157)

11.2.8. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pelo Contratante ao Contratado, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente (art. 156, §8º).

11.2.9. Previamente ao encaminhamento à cobrança judicial, a multa poderá ser recolhida administrativamente no prazo máximo de 30 (trinta) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

11.3. A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa ao Contratado, observando-se o procedimento previsto no caput e parágrafos do art. 158 da Lei nº 14.133, de 2021, para as penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar.

11.4. Os atos previstos como infrações administrativas na Lei nº 14.133, de 2021, ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei nº 12.846, de 2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e autoridade competente definidos na referida Lei (art. 159)

11.5. As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do art. 163 da Lei nº 14.133/21.

CLÁUSULA DÉCIMA SEGUNDA – DA EXTINÇÃO CONTRATUAL (art. 92, XIX)

12.1. O contrato se extingue quando cumpridas as obrigações de ambas as partes, ainda que isso ocorra antes do prazo estipulado para tanto.

12.2. Se as obrigações não forem cumpridas no prazo estipulado, a vigência ficará prorrogada até a conclusão do objeto, caso em que deverá a Administração providenciar a readequação do cronograma físico-financeiro.

12.2.1. Quando a não conclusão do contrato referida no item anterior decorrer de culpa do contratado:

12.2.1.1 ficará ele constituído em mora, sendo-lhe aplicáveis as respectivas sanções administrativas; e

12.2.1.2. poderá a Administração optar pela extinção do contrato e, nesse caso, adotará as medidas admitidas em lei para a continuidade da execução contratual.

12.2. O contrato pode ser extinto antes de cumpridas as obrigações nele estipuladas, ou antes do prazo nele fixado, por algum dos motivos previstos no artigo 137 da NLLC, bem como amigavelmente, assegurados o contraditório e a ampla defesa.

12.2.1. Nesta hipótese, aplicam-se também os artigos 138 e 139 da mesma Lei.

12.2.2. A alteração social ou modificação da finalidade ou da estrutura da empresa não ensejará rescisão se não restringir sua capacidade de concluir o contrato.

12.2.3. Se a operação implicar mudança da pessoa jurídica contratada, deverá ser formalizado termo aditivo para alteração subjetiva.

12.3. O termo de rescisão, sempre que possível, será precedido de balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos; relação dos pagamentos já efetuados e ainda devidos e indenizações e multas.

CLÁUSULA DÉCIMA TERCEIRA – DOTAÇÃO ORÇAMENTÁRIA (art. 92, VIII)

13.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados nas dotações orçamentárias:

- 02.23.01.33.90.40 – Ficha 1627 – Secretaria de Comunicação e Tecnologia da Informação;

- 02.14.06.3390.40 - Fichas 1406, 1409 e 1420 – Secretaria de Saúde.

CLÁUSULA DÉCIMA QUARTA – DOS CASOS OMISSOS (art. 92, III)

14.1. Os casos omissos serão decididos pelo CONTRATANTE, segundo as disposições contidas na Lei nº 14.133, de 2021 e demais normas federais aplicáveis e, subsidiariamente, segundo as disposições contidas na Lei nº 8.078, de 1990 – Código de Defesa do Consumidor – e normas e princípios gerais dos contratos.

CLÁUSULA DÉCIMA QUINTA – ALTERAÇÕES

15.1. Eventuais alterações contratuais reger-se-ão pela disciplina dos arts. 124 e seguintes da Lei nº 14.133, de 2021.

15.2. O CONTRATADO é obrigada a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato. As supressões resultantes de acordo celebrado entre as partes contratantes poderão exceder o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do termo de contrato.

15.3. Registros que não caracterizam alteração do contrato podem ser realizados por simples apostila, dispensada a celebração de termo aditivo, na forma do art. 136 da Lei nº 14.133, de 2021.

CLÁUSULA DÉCIMA SEXTA – PUBLICAÇÃO

16.1. Incumbirá à CONTRATANTE providenciar a publicação deste instrumento nos termos e condições previstas na Lei nº 14.133/21.

CLÁUSULA DÉCIMA SÉTIMA – FORO (art. 92, §1º)

17.1. É eleito o Foro da Comarca de Americana para dirimir os litígios que decorrerem da execução deste Termo de Contrato que não possam ser compostos pela conciliação, conforme art. 92, §1º da Lei nº 14.133/21.

Americana, de de 2025.

Identificação e assinaturas:

Representante legal do CONTRATANTE

Representante legal do CONTRATADO

TESTEMUNHAS:

1-

2-

ANEXO III – TERMO DE REFERÊNCIA

1- OBJETO

Contratação de serviços de licença de uso de **1.050 licenças de Endpoint Vision One 03 licenças de proteção Cloud Vision One – Trend Micro**, destinadas à proteção das estações de trabalho e servidores em nuvem de estações de trabalho, servidores e serviços em nuvem, a serem utilizadas em toda a estrutura da Administração Municipal.

1.1 Classificação do serviço.

Considerando as definições constantes no Art. 6º da Lei 14.133/2021, o objeto pretendido enquadra-se como serviço comum e fornecimento contínuo, conforme os incisos XIII e XV.

2 – JUSTIFICATIVA DA NECESSIDADE DE CONTRATAÇÃO

A transformação digital da gestão pública exige uma infraestrutura de conectividade eficiente. A ausência ou a precariedade do acesso à internet limita a execução de políticas públicas e a prestação de serviços ao cidadão.

Com a crescente digitalização de processos, utilização de sistemas integrados e a ampliação de serviços online voltados à população (educação híbrida, saúde digital, protocolos eletrônicos, atendimento remoto, entre outros), a conectividade torna-se estratégica e essencial.

A conectividade é essencial para o funcionamento de sistemas administrativos, educacionais, de saúde, assistência social, segurança e demais áreas da gestão municipal. A ausência ou precariedade de acesso à internet impacta diretamente na qualidade e agilidade do atendimento ao cidadão.

Além disso, diversos projetos de inclusão digital, telemedicina, educação híbrida, atendimento digital ao cidadão e integração de sistemas governamentais exigem conectividade estável e de alta performance. A contratação dos serviços permitirá:

- Melhorar o acesso da população aos serviços públicos;
- Integrar sistemas de informação;
- Viabilizar o funcionamento de equipamentos públicos (escolas, unidades de saúde, CRAS, entre outros);
- Otimizar processos internos da administração municipal;
- Reduzir custos operacionais a médio e longo prazo por meio da digitalização.

3 – ESPECIFICAÇÃO DO OBJETO

SOLUÇÃO DE SEGURANÇA PARA SISTEMAS CRÍTICOS ESTAÇÃO DE TRABALHO E SERVIDORES

3.1 – Composição da Solução

ITEM	Quant.	DESCRIÇÃO
1	650	RENOVAÇÃO LICENÇA DE USO DE PROGRAMAS DE COMPUT.TREND VISION ONE – ENDPOINT SECURITY (CORE) ESTAÇÕES DE TRABALHO. RENEW - Part Number – VORA0026
2	3	RENOVAÇÃO LICENÇA DE USO DE PROGRAMAS DE COMPUT. TREND VISION ONE – ENDPOINT SECURITY (PRO-CLOUD) SERVIDORES. RENEW - Part Number – VORA0041
3	400	AQUISIÇÃO LICENÇA DE USO DE PROGRAMAS DE COMPUT. - TREND VISION ONE - ENDPOINT SECURITY (CORE) ESTAÇÕES DE TRABALHO. NEW - Part Number – VONA0028

Item 1 – SOLUÇÃO DE SEGURANÇA PARA ESTAÇÕES DE TRABALHO COM DETECÇÃO E RESPOSTA.

1.1 – A solução deverá ser fornecida em ambiente do fabricante e deverá possuir alta disponibilidade;

1.2 - Gerais

1.3.1. Características Gerais Da Solução

1.3.1.1. A solução deverá ser compatível com pelo menos os seguintes sistemas operacionais:

1.3.1.1.1. Windows 7 SP1;

1.3.1.1.2. Windows 10;

1.3.1.1.3. Windows 11;

1.3.1.1.4. MacOs Catalina ou superior;

1.3.1.1.5. Ubuntu 10, 12, 14, 16, 18 e 20;

1.3.1.2. A console de gerenciamento deverá ser em nuvem ou on-premises, permitindo o gerenciamento das políticas de segurança através da Internet;

1.3.1.4. Caso a solução seja ofertada em nuvem, deverá ter conformidade com ISO 27001, ISO 27014, ISO 27017 e SOC 2;

1.3.1.5. Os ambientes em nuvem providos pelo fabricante devem passar por testes de penetração de forma recorrente como para garantir a segurança da solução provida

1.3.1.6. Deverá atuar com console unificada para a gerência das máquinas, atendo aos diferentes sistemas operacionais citados no item 1.2.1.1.

1.3.1.7. A solução deverá ser gerenciada por console Web, compatível com pelo menos os browsers Internet Explorer, Google Chrome e Firefox. Deve ainda suportar certificado digital para gerenciamento;

1.3.1.8. A solução deverá permitir aplicar tags de forma manual ou automática em eventos gerados para identificação de falso positivo como também permitir rápida identificação de eventos ou alertas críticos;

1.3.1.9. A solução deverá permitir a integração com pelo menos as seguintes plataformas de nuvem: Vmware vCloud, MS Azure e AWS;

1.3.1.10. Precisa ter a capacidade de controlar e gerenciar a segurança de múltiplas plataformas e sistemas operacionais, incluindo máquinas em nuvens externas a partir de uma console única e centralizada do próprio fabricante;

1.3.1.11. A solução deverá permitir a entrega de agentes por pelo menos duas dentre as principais ferramentas de distribuição de software do mercado: Microsoft System Center Configuration Manager, Novel Zen Works e Puppet;
1.3.1.12. A console de administração deverá permitir o envio de notificações via SMTP;
1.3.1.13. Todos os eventos e ações realizadas na console de gerenciamento precisam ser gravados para fins de auditoria;
1.3.1.14. A solução deverá possuir a funcionalidade tags para identificar falsos positivos ou facilitar a visualização de determinados alertas;
1.3.1.15. A solução deverá permitir a criação de widgets para facilitar a administração e visualização dos eventos;
1.3.1.16. A solução deverá permitir que a distribuição de patterns e novos componentes possa ser efetuada por agentes de atualização espalhados pelo ambiente;
1.3.1.17. A solução precisa permitir a criação de relatórios. A criação e envio destes relatórios deverá ocorrer sob-demanda, ou agendado com o envio automático do relatório via e-mail;
1.3.1.18. A solução deverá fornecer pelo menos dois tipos de relatórios nos seguintes formatos PDF, CSV, XLS e RTF;
1.3.1.19. A solução precisa permitir que relatórios no formato PDF, possam ser enviados com uma senha única para cada destinatário;
1.3.1.20. A solução deverá prover relatórios contendo no mínimo as seguintes informações; malware, regras de IPS aplicadas e Firewall;
1.3.1.21. Em caso de solução e nuvem, o ambiente do fabricante deverá fornecer alta disponibilidade;
1.3.1.22. A solução de segurança ter a capacidade de identificar ataques entre conteineres;
1.3.1.23. Os usuários devem ter a capacidade de receber determinados papéis para administração como "acesso total" e "acesso parcial", podendo ser customizado o que compõe o "acesso parcial";
1.3.1.24. Quando configurado o acesso parcial, este deve permitir que um usuário tenha permissões de poder gerenciar a segurança de um único computador, podendo ainda definir em quais módulos de proteção será possível ou não editar ou criar políticas de segurança;
1.3.1.25. A comunicação entre a console de gerenciamento e os agentes deverá ser criptografada;
1.3.1.26. Cada agente deverá ter sua própria chave para criptografia de modo que a comunicação criptografada seja feita de forma diferente para cada agente;
1.3.1.27. A console de gerenciamento deverá ter dashboards para facilidade de monitoração, as quais deverão ser customizadas pelo administrador em quantidade e período de monitoração;
1.3.1.28. Os agentes de atualização deverão buscar os updates das assinaturas e distribuí-las para os agentes. Quando ocorrer a atualização, esta deverá ocorrer de modo absolutamente seguro utilizando-se SSL/TLS com o servidor de onde ela buscará as informações;
1.3.1.29. Os agentes para plataforma Microsoft deverão ser instalados por pacote MSI e posteriormente ativados pela console de gerenciamento de forma a proporcionar maior segurança ao ambiente, ou de forma automatizada através de script PowerShell;
1.3.1.30. Os agentes para plataforma Linux deverão ser instalados por pacote RPM ou DEB e posteriormente ativados pela console de gerenciamento de forma a proporcionar maior segurança ao ambiente, ou de forma automatizada através de bash script;
1.3.1.31. Em servidores Windows e Linux, a solução deverá permitir a atualização automática dos agentes após sua ativação;
1.3.1.32. Para servidores Linux, a solução deverá possibilitar a atualização automática da versão quando o agente reiniciar;
1.3.1.33. Para efeito de administração, a solução deverá avisar quando um agente se encontrar não conectado a sua console de gerenciamento;
1.3.1.34. Deve permitir a remoção automática de agentes inativos, definindo o período para, pelo menos 1 semana, 1 mês e 12 meses;

1.3.1.35. A solução deve possuir a capacidade de criar políticas de forma global para todas as máquinas, por perfis e individualmente para cada host;
1.3.1.36. Cada perfil poderá ser atribuído para um host ou um conjunto de hosts;
1.3.1.37. A solução deverá vir com perfis pré-definidos e aptos a funcionarem de acordo com sua denominação;
1.3.1.38. A solução deverá mostrar quais máquinas estão usando determinada política;
1.3.1.39. Os agentes deverão ser capazes de executar rastreamento nas máquinas onde estão instalados e após isso deverão fornecer uma lista de todas as recomendações de segurança para os softwares que estejam instalados nas máquinas bem como do sistema operacional;
1.3.1.40. Esses rastreamentos devem ocorrer de forma periódica a ser definida pelo administrador;
1.3.1.41. A solução deverá permitir classificar os relatórios em pelo menos três tipos de classificação: Secreto, Confidencial, Uso Oficial, Sem classificação, Em branco e uso interno;
1.3.1.42. A solução deverá permitir a configuração de componentes de integração com o vCenter, a fim de permitir a sincronização das máquinas virtuais conectadas a ele;
1.3.1.43. Brechas de segurança descobertas deverão ser protegidas de forma automática e transparente, interrompendo somente o tráfego de rede malicioso;
1.3.1.44. O administrador do sistema de segurança deverá ter a possibilidade de não aplicar automaticamente a proteção para as vulnerabilidades escolhendo o perfil ou o host;
1.3.1.45. A solução deve possuir a capacidade de isolamento de placa de rede de forma que apenas uma fique funcionando de acordo com preferência do administrador;
1.3.1.46. A solução deverá ser capaz de aplicar políticas diferentes para placas de redes diferentes em um mesmo servidor;
1.3.1.47. A solução deverá ser capaz de executar bypass completo de rastreamento de tráfego de forma que os módulos não atuem em determinado tipo de conexão ou pacote;
1.3.1.48. Solução deverá permitir criar relatórios customizados de todas as suas funcionalidades;
1.3.1.49. Deve permitir enviar os relatórios para uma lista de contatos independente de login na console de administração;
1.3.1.50. As atualizações de assinaturas deverão ocorrer de forma agendada e automática possibilitando ser até mesmo de hora em hora;
1.3.1.51. Após a atualização deve ser informado o que foi modificado ou adicionado;
1.3.1.52. Deve ser possível baixar as assinaturas na console de gerenciamento, mas não as distribuir aos clientes;
1.3.1.53. A console de gerenciamento deve apresentar a capacidade de gerar rollback de suas atualizações de regras;
1.3.1.54. A solução deverá ter capacidade de gerar pacote de autodiagnóstico de modo a coletar arquivos relevantes para envio ao suporte do produto;
1.3.1.55. Deverá ter a capacidade de colocar etiquetas para a ocorrência de determinados eventos de modo a facilitar o gerenciamento, relatórios e visualização;
1.3.1.56. No gerenciamento de licenças, deve ser informada quantidade contratada e quantidade em utilização de clientes;
1.3.1.57. Solução deverá ter mecanismo de procura em sua console de gerenciamento de modo que seja facilitada a busca de regras;
1.3.1.58. Deverá possuir a capacidade de classificar eventos para que facilite a identificação e a visualização de eventos críticos em servidores críticos;
1.3.1.59. Deverá possibilitar colocar etiquetas em eventos para que se possam visualizar apenas os eventos desejados;

1.3.1.60. O fabricante deverá participar do programa “Microsoft Application Protection Program” para obtenção de informações de modo a permitir a criação de regras de proteção antes mesmo dos patches serem publicados pelo fabricante;
1.3.1.61. A console de gerenciamento deve se integrar com o Vmware vCloud, de modo a importar e sincronizar os objetos (hosts vmware e guests vm) para a console de gerenciamento da solução;
1.3.1.62. O fabricante da solução deverá manter programa de pesquisa em vulnerabilidades há, pelo menos, 5 anos;
1.3.1.63. A solução deve possuir API documentada para integração na esteira de automação;
1.3.1.64. A documentação da API deve conter exemplos prontos para implementação de determinadas funcionalidades, como cookbooks;
1.3.1.65. Precisa ter a capacidade de detectar e aplicar as regras necessárias dos módulos de IDS/IPS, Monitoramento de Integridade e Inspeção de Logs, para cada servidor, de forma automática e sem a intervenção do administrador;
1.3.1.66. A solução deve permitir desabilitar os módulos individualmente;
1.3.1.67. Precisa ter a capacidade de desabilitar as regras não mais necessárias dos módulos de IDS/IPS, Monitoramento de Integridade e Inspeção de Logs, para cada servidor, de forma automática e sem a intervenção do administrador.
1.3.1.68. O fabricante da solução deverá manter os logs da solução por no mínimo 45 dias após expiração da licença

1.3.2. Antimalware
1.3.2.1. A solução deve permitir a proteção contra códigos maliciosos através da instalação de agentes, permitindo rastrear ameaças em tempo real, varredura sob demanda e conforme agendamento, possibilitando a tomada de ações distintas para cada tipo de ameaça;
1.3.2.2. A solução deve possibilitar a criação de listas de exclusão, para que o processo do antivírus não execute a varredura de determinados diretórios ou arquivos do SO;
1.3.2.3. A solução deve possuir listas de exclusão separadas por módulo da proteção antimalware como exclusão das detecções por comportamento, exclusão por machine learning e exclusão por assinatura;
1.3.2.4. Em plataforma Windows, a solução deve permitir criar exclusões de escaneamento a partir do certificado digital das aplicações;
1.3.2.5. A solução deve possibilitar a verificação de ameaças dentro de arquivos compactados, efetuando a limpeza apenas de arquivos maliciosos em casos de detecção. A limpeza deve ocorrer sem a descompactação do arquivo;
1.3.2.6. Em servidores Windows, deve identificar e bloquear ameaças através de métodos de Machine Learning, quarentenando arquivos identificados;
1.3.2.7. A solução deverá possuir a funcionalidade de Monitoramento de Comportamento para detectar mudanças e atividades suspeitas não autorizadas;
1.3.2.8. A solução deverá oferecer escanear processos em memória em busca de Malware;
1.3.2.9. O scan de arquivos comprimidos deverá ser de no mínimo 6 camadas de compressão;
1.3.2.10. O scan de arquivos comprimidos do tipo OLE deverá ser de no minimo 20 camadas de compressão;
1.3.2.11. Para servidores Windows, a solução deverá permitir que o escaneamento agendado ocorra, ainda que o agente esteja offline na console de gerenciamento;
1.3.2.12. A solução deverá possuir ações pré-configuradas para cada tipo de ameaça detectada ou tomar uma ação baseada na configuração padrão da ferramenta;
1.3.2.13. Em servidores Windows, a solução deverá integrar-se com interface AMSI (Antimalware Scan Interface);
1.3.2.14. A solução deverá mostrar informação de data sobre o último scan agendado ou manual executado;
1.3.2.15. Possuir a capacidade de efetuar backup e restore de arquivos comprometidos por Ransomware;
1.3.2.16. Deve possuir cache dos arquivos verificados de modo a evitar a redundância da varredura;

1.3.2.17. Deve possibilitar o controle do consumo de memória durante as varreduras a fim de minimizar os impactos de desempenho no servidor;
1.3.2.18. A solução deve possuir opção para forçar a comunicação com o agente e coletar os respectivos logs;
1.3.2.19. Deverá possuir funcionalidades de de Detecção e Resposta;
1.3.2.20. Solução deve possuir módulo de investigação, detecção integrados;
1.3.2.21. Deve permitir que as detecções sejam correlacionadas com módulos de endpoint, rede e e-mail do próprio fabricante através de console dedicada. Não serão aceitas consoles de correlação de terceiros;
1.3.2.22. A console de correlação deve estar disponível na nuvem do próprio fabricante, o qual deve ser responsável pelas manutenções, atualizações e disponibilidade;
1.3.2.23. Deve possuir capacidade de encaminhar as atividades suspeitas identificadas nos servidores para a console de correlação centralizada;
1.3.2.24. O módulo de detecção e resposta deve atuar baseado em modelos de detecção de ataques avançados e furtivos;
1.3.2.25. Os logs de detecções devem estar disponíveis na console por, pelo menos, 30 dias;
1.3.2.26. A console de correlação centralizada deve possuir informações a respeito dos principais ataques que estão ocorrendo no mundo, quais plataformas e países são afetados, além de links para obter mais informações;
1.3.2.27. A solução deve permitir realizar buscas em todos os dados de atividades enviadas pelos servidores e demais sensores que estejam conectados na console, ainda que estas não sejam detectadas como maliciosas;
1.3.2.28. A console deve permitir o Single Sign-On através de SAML ou padrão equivalente;
1.3.2.29. Deve ser possível criar usuários com permissões distintas, contendo no mínimo, permissão total e permissão para realizar investigações;
1.3.2.30. Deve permitir habilitar ou desabilitar um determinado usuário sem excluí-lo da console;
1.3.2.31. Deve permitir o envio de notificações para os administradores através de email, API e integrações com SIEMs;
1.3.2.32. Deve prover visualização em linha do tempo com informações dos eventos monitorados em cada servidor;
1.3.2.33. Deve permitir a visualização entre usuários, servidores, processos/comandos, arquivos e demais componentes correlacionados em determinado ataque;
1.3.2.34. Deverá informar com qual técnica e tática do MITRE ATT&CK framework o ataque está relacionado, além de possuir link direto para o site da organização;
1.3.2.35. A solução deve mostrar, pelo menos, o timestamp, objetos envolvidos (comandos, processos, usuários, servidores);
1.3.2.36. Ao clicar em quaisquer dos objetos, a solução deve permitir realizar buscar específicas pelo objeto ou ainda executar ações como executar investigações mais aprofundadas.
1.3.2.37. A solução deverá por meio de agente único possibilitar a conexão com a plataforma de detecção e resposta do próprio fabricante de maneira nativa sem a necessidade de plug-ins ou agentes adicionais;
1.3.2.38. Esta conexão deverá garantir, sem qualquer configuração local, que o sensor de detecção e resposta esteja ativo e envie telemetria a plataforma;

1.6 CONSOLE DE GERENCIAMENTO DA PLATAFORMA DE DETECÇÃO E RESPOSTA ESTENDIDA
1.6.1 A solução deve fornecer uma console única para gerenciamento dos serviços de segurança, integrando-se com os outros componentes;
1.6.2 Capacidade de controlar e gerenciar a segurança de múltiplas plataformas e sistemas operacionais, incluindo máquinas em nuvens externas a partir de uma console única e centralizada do próprio fabricante;
1.6.3 A console de administração deverá permitir o envio de notificações via SMTP
1.6.4 Todos os eventos e ações realizadas na console de gerenciamento precisam ser registrados para fins de auditoria;

1.6.5 A solução deverá possuir a funcionalidade tags para identificar falsos positivos ou facilitar a visualização de determinados alertas;
1.6.6 A solução deverá permitir que a distribuição de patterns e novos componentes possa ser efetuada por agentes de atualização espalhados pelo ambiente;
1.6.7 Deverá orquestrar todas as funcionalidades descritas;
1.6.8 A solução precisa permitir a criação de relatórios. A criação e envio destes relatórios deverá ocorrer sob demanda, ou por tarefa agendada com o envio automático do relatório por e-mail;
1.6.9 O fabricante deve implementar e organizar os ataques baseados no framework MITRE ATT&CK, identificando técnicas e táticas dos ataques;
1.6.10 Prover nota de risco para o ambiente de TI da CONTRATANTE, baseada em diversos fatores e comparável com a de outras organizações da mesma região, indústria ou tamanho;
1.6.11 Deve suportar integração com os seguintes serviços de diretório:
1.6.11.1 Microsoft Active Directory;
1.6.11.2 Azure Active Directory;
1.6.11.3 Open LDAP;
1.6.12 A nota de risco deve ser calculada continuamente e deve ser possível analisar seu comportamento ao longo do tempo de forma gráfica;
1.6.13 As fontes de dados para cálculo do risco não devem se limitar àquelas desenvolvidas pelo FABRICANTE, sendo aceitas soluções de terceiros;
1.6.14 Deve prover um sumário dos itens referentes ao escopo de risco cibernético mapeado, apresentando as ações a serem executadas, a fim de diminuir o valor numérico do risco;
1.6.15 Deve apresentar alertas de possíveis comprometimentos de contas;
1.6.16 A solução deverá fornecer pelo menos dois tipos de relatórios nos seguintes formatos PDF, CSV, XLS e RTF;
1.6.17 Suporte a atribuição de papéis funcionais, para implantação de política de controle de acesso baseada em papéis (*RBAC - Role-based access control*);
1.6.18 A console de administração deve metrificar o nível de risco cibernético do ambiente, baseando-se na telemetria gerada pelas demais soluções citadas nos itens 1.1, 1.2, 1.3,1.4 e 1.5;
1.6.19 Deve mapear as vulnerabilidades existentes nas máquinas, elencando quanto ao nível de CVSS score e impacto no ambiente, apresentando as vulnerabilidades que estão sofrendo algum tipo de exploração a nível das máquinas e da rede;
1.6.20 Deve apontar as vulnerabilidades com o maior índice de risco presentes no ambiente;
1.6.21 Deve apresentar os alertas de ameaças direcionadas, suspeitas, e de dia zero, a fim de identificar possíveis ações maliciosas no ambiente da CONTRATANTE;
1.6.22 Tais alertas devem apresentar:
1.6.22.1 A relação entre máquinas e IPs;
1.6.22.2 Requisições de rede;
1.6.22.3 URLs e Hashs;
1.6.22.4 Usuários e domínios;
1.6.23 Deve ser possível customizar os modelos de detecção, a fim de atender as necessidades da CONTRATANTE;
1.6.24 Deve ser possível criar exceções para os modelos de detecção;
1.6.25 A solução deve ser baseada em inteligência artificial e aprendizagem de máquina, a fim de potencializar os níveis de detecção de comportamentos anômalos;
1.6.26 Deve possuir rede global de inteligência de ameaças;
1.6.27 Deve apresentar alertas caso os dados de telemetria gerados tenham relação com algum tipo de campanha de ameaças globais;
1.6.28 Deve possuir módulo de pesquisa forense de ameaças, possibilitando a coleta de logs remotamente;
1.6.29 Deve suportar conexões remotas via agente da solução, sendo possível:

1.6.29.1 Coleta de evidências forenses;
1.6.29.2 Isolar a máquina;
1.6.29.3 Terminar processo;
1.6.29.4 Dump de memória;
1.6.29.5 Listar as portas abertas na máquina;
1.6.29.6 Listar configurações de rede;
1.6.29.7 Listar os diretórios;
1.6.29.8 Deletar arquivo ou diretório;
1.6.30 Enumerar a superfície de ataque da CONTRATANTE, dependendo das fontes de dados conectadas, compreendendo:
1.6.30.1 As estações de trabalho, os servidores e os dispositivos móveis da CONTRATANTE;
1.6.30.2 Os usuários da CONTRATANTE, apontando inclusive aqueles que detêm poderes administrativos;
1.6.30.3 As aplicações acessadas por usuários e dispositivos da CONTRATANTE, apontando inclusive aquelas que passaram por recente vazamento de dados;
1.6.30.4 Os ativos mantidos pela CONTRATANTE sob custódia de Provedores de Serviços em Nuvem;
1.6.30.5 Os domínios da CONTRATANTE, suportando ao menos 10 domínios diferentes;
1.6.30.6 Os subdomínios da CONTRATANTE;
1.6.30.7 Os IPs Públicos associados à CONTRATANTE e seus respectivos hosts;
1.6.30.8 As portas de comunicação/serviços abertos em cada host público;
1.6.31 Deve mapear via rede da CONTRATANTE os dispositivos existentes e apontar aqueles que não são gerenciados pelos agentes da solução;
1.6.32 Deve apresentar a relação de máquinas que o usuário acessou;
1.6.33 Deve listar os alertas identificados no ambiente e correlacionar com técnicas, táticas e procedimentos do framework MITRE ATT&CK;
1.6.34 Tais alertas devem seguir o seguinte escopo de severidade quanto ao nível de risco:
1.6.34.1 Risco Crítico;
1.6.34.2 Risco Alto;
1.6.34.3 Risco Médio;
1.6.34.4 Risco Baixo.
1.6.35 Deve informar qual o escopo de impacto ou dimensionar o impacto em servidores, estações de trabalho e usuários, indicando a quantidade de componentes afetados no ataque;
1.6.36 Deve haver correlação entre eventos de detecção, a fim de apresentar um possível incidente de segurança;
1.6.37 Deve suportar que o usuário manualmente correlacione alertas em um incidente;
1.6.38 Deve possibilitar que um usuário atribua o alerta a outro usuário;
1.6.39 Deve possuir campo para observações e notas;
1.6.40 Cada alerta deverá ser listado com um status de:
1.6.40.1 Novo alerta;
1.6.40.2 Alerta sendo tratado;
1.6.40.3 Falso Positivo
1.6.40.4 Fechado;
1.6.40.5 Verdadeiro Positivo.
1.6.41 Deve listar todos as ações de resposta executadas, apresentando o status de cada uma;
1.6.42 Deve possuir lista customizável de indicadores de comprometimento e objetos suspeitos;
1.6.43 Deve permitir adicionar arquivos SHA-1, SHA-256, URLs, IPs, domínios e endereços de e-mail a lista de objetos suspeitos;
1.6.44 Deve permitir remover arquivos SHA-1, URLs, IPs ou domínios a lista de objetos suspeitos.

1.6.45 Deve informar com qual técnica e tática do MITRE ATT&CK framework o ataque está relacionado, além de possuir link direto para o site da organização;
1.6.46 A solução deve mostrar, pelo menos, o timestamp e objetos envolvidos (comandos, processos, usuários, servidores);
1.6.47 Ao clicar em quaisquer dos objetos, a solução deve permitir realizar buscas específicas pelo objeto ou ainda executar ações como executar investigações mais aprofundadas.
1.6.48 Para a integração com o sensor de inspeção de rede, a solução deverá receber os alertas advindos do sensor de inspeção de rede, processá-los e analisá-los, a fim de identificar os riscos de segurança existentes;
1.6.49 Com base na telemetria do sensor de inspeção de rede, deverá replicar a sequência de requisições ocorridas dentre as máquinas da rede da CONTRATANTE e endereços externos, a fim de apresentar eventos correlacionados para permitir investigações forenses;
1.6.50 Deverá correlacionar os logs do sensor de inspeção de rede e indicar quais vulnerabilidades existentes nas máquinas estão sofrendo tentativas de exploração;
1.6.51 A partir da identificação de uma exploração de vulnerabilidade em determinadas máquinas, a solução deverá ser capaz de disponibilizar as regras de proteção indicadas;
1.6.52 Deverá ser capaz de automaticamente enviar as regras de proteção frente as vulnerabilidades por meio da console do gerenciamento e aplicá-las diretamente no *appliance* de Prevenção de Intrusão de rede de 2ª Geração, sem necessidade de ação manual;
1.6.53 O fabricante deve implementar e organizar os ataques baseados no framework MITRE ATT&CK, identificando técnicas e táticas dos ataques;
1.6.54 Com base na telemetria gerada, deve apresentar de forma gráfica fases de um possível ataque, por meio das correlações aplicadas;
1.6.55 Deve fazer uso de inteligência artificial e inteligência de ameaças do fabricante da solução para analisar e correlacionar as atividades dos sensores do ambiente;
1.6.56 Possuir painéis que apresentem visualização executiva dos principais incidentes e atividades no ambiente com base nos usuários, aplicações acessadas e estações de trabalho;
1.6.57 Utilizar bases de inteligência de ameaças integrando relatórios de inteligência do fabricante e de terceiros para ajudar a identificar ameaças no ambiente;
1.6.58 Apresentar os alertas consolidados e correlacionados de ameaças para melhor investigação e resposta;
1.6.59 Deve ser capaz de realizar buscas avançadas para localizar dados ou objetos no ambiente para análise avançada de atividades ou detecções;
1.6.60 Capacidade de construir sequências de buscas para localizar os dados ou objetos no ambiente que será feita a análise;
1.6.61 Deve prover diferentes métodos de pesquisa, filtros e uma linguagem de consulta do tipo Kibana para identificar, categorizar e recuperar os resultados da pesquisa;
1.6.62 Deve ser possível realizar buscas através de strings parciais, exatas, valores nulos, wildcards e caracteres especiais;
1.6.63 Permitir investigar os alertas gerados pelos modelos de detecção por meio de uma análise impacto e análise de causa-raiz;
1.6.64 Deve consolidar e correlacionar diferentes modelos de ameaça relacionados a um único evento;
1.6.65 Deve exibir os eventos de forma a priorizar os alertas mais críticos para que o analista realize a investigação, como pontuações ou níveis de prioridade;
1.6.66 Reagir programaticamente, por meio de roteiros customizáveis, quando da detecção de alto risco de máquinas presentes no ambiente da CONTRATANTE;
1.6.67 Deve ser possível interagir com cada um dos objetos relacionados ao evento para análise avançada e resposta;
1.6.68 Deve destacar e organizar as atividades relacionadas a cada modelo de detecção por ordem cronológica, permitindo identificar a relação de cada atividade com os modelos de detecção;

1.6.69 Deve prover visualização em linha do tempo com informações dos eventos monitorados em cada estação de trabalho;
1.6.70 Deve elencar o nível de risco cibernético dos usuários da CONTRATANTE, identificando os que apresentem comportamentos anômalos de:
1.6.70.1 Comprometimento de credencial;
1.6.70.2 Ataque de força bruta;
1.6.70.3 Login atípico ou impossível;
1.6.70.4 Login via IPs suspeitos;
1.6.70.5 Múltiplas tentativas de login com sucesso e insucesso;

1.6.71 A partir da dos alertas de risco dos usuários, deve ser possível enviar ações de mitigação de risco:
1.6.71.1 Forçar reset de senha;
1.6.71.2 Desabilitar conta do usuário no serviço de diretório;
1.6.71.3 Forçar sign-out do usuário;

1.6.72 Deverá centralizar as ações e estender a visibilidade sob todas as funcionalidades, sendo elas:
1.5.72.1.1 inspeção de rede contra ameaças avançadas com detecção e resposta;
1.5.72.1.2 Detecção e resposta para Servidores e cargas de trabalho;
1.5.72.1.3 Detecção e resposta para estações de trabalho;
1.5.72.1.4 Controle de acesso a aplicações internas, externas e na nuvem;
1.5.72.1.5 Prevenção de Intrusão de rede;

1.6.73 A solução deverá prover relatórios contendo no mínimo as seguintes informações:
1.6.73.1 Top Ameaças;
1.6.73.2 Top usuários com risco;
1.6.73.3 Top vulnerabilidades identificadas;
1.6.73.4 Top Hosts com detecções;
1.6.73.5 Sumário de tráfego de rede inspecionado;

Item 2 - SOLUÇÃO DE SEGURANÇA PARA SERVIDORES E CARGAS DE TRABALHO HÍBRIDAS COM DETECÇÃO E RESPOSTA.

2.2.1. Precisa ter a capacidade de controlar e gerenciar a segurança de múltiplas plataformas e sistemas operacionais, incluindo máquinas em nuvens externas a partir de uma console única e centralizada do próprio fabricante;
2.2.2. A solução deverá permitir a integração com pelo menos as seguintes plataformas de nuvem: Vmware vCloud, Microsoft Azure, Amazon Web Services e Google Cloud Platform.
2.2.3. A console de administração deverá permitir o envio de notificações via SMTP;
2.2.4. Todos os eventos e ações realizadas na console de gerenciamento precisam ser registrados para fins de auditoria;
2.2.5. A solução deverá permitir a criação de widgets para facilitar a administração e visualização dos eventos;
2.2.6. A solução deverá permitir que a distribuição de patterns e novos componentes possa ser efetuada por agentes de atualização espalhados pelo ambiente;
2.2.7. A solução precisa permitir a criação de relatórios. A criação e envio destes relatórios deverá ocorrer sob demanda, ou por tarefa agendada com o envio automático do relatório por e-mail;
2.2.8. A solução deverá fornecer pelo menos dois tipos de relatórios nos seguintes formatos PDF, CSV, XLS e RTF;

2.2.9. A solução precisa permitir que relatórios no formato PDF, possam ser enviados com uma senha única para cada destinatário;
2.2.10. A solução deverá prover relatórios contendo no mínimo as seguintes informações; malware, regras de IPS aplicadas e Firewall;
2.2.11. Em caso de solução e nuvem, o ambiente do fabricante deverá fornecer alta disponibilidade;
2.2.12. A solução de segurança ter a capacidade de identificar ataques em estruturas de container.
2.2.13. Deve ser possível customizar os privilégios de administração da solução:
2.2.13.1. Acesso total;
2.2.13.2. Acesso somente leitura;
2.2.14. Deve ser possível assignar políticas de segurança em máquinas específicas, grupos estáticos e dinâmicos;
2.2.15. A comunicação entre a console de gerenciamento e os agentes deverá ser criptografada;
2.2.16. Cada agente deverá ter sua própria chave para criptografia de modo que a comunicação criptografada seja feita de forma diferente para cada agente;
2.2.17. A console de gerenciamento deverá ter dashboards para facilidade de monitoração, as quais deverão ser customizadas pelo administrador em quantidade e período de monitoração;
2.2.18. A solução deverá ser compatível com pelo menos os seguintes sistemas operacionais:
2.2.18.1. Windows Server 2000;
2.2.18.2. Windows Server 2003 SP1 e 2003 R2 SP2;
2.2.18.3. Windows Server 2008 e 2008 R2;
2.2.18.4. Windows Server 2012 e 2012 R2;
2.2.18.5. Windows Server 2016;
2.2.18.6. Windows Server 2019;
2.2.18.7. Windows Server 2022;
2.2.18.8. Red Hat Enterprise 5, 6, 7 e 8;
2.2.18.9. CentOS 5, 6, 7 e 8;
2.2.18.10. AIX 6.1, 7.1 e 7.2;
2.2.18.11. Oracle Linux 5, 6, 7 e 8;
2.2.18.12. SUSE Linux Enterprise Server 10, 11, 12 e 15;
2.2.18.13. Ubuntu 10, 12, 14, 16, 18 e 20;
2.2.18.14. Debian 6, 7, 8, 9 e 10;
2.2.18.15. Rocky Linux 8;
2.2.18.16. AlmaLinux 8;
2.2.18.17. Cloud Linux 5, 6, 7 e 8;
2.2.18.18. Amazon Linux 2 (x64)
2.2.19. Os agentes de atualização deverão buscar os updates das assinaturas e distribuí-las para os agentes. Quando ocorrer a atualização, esta deverá ocorrer de modo absolutamente seguro utilizando-se SSL/TLS com o servidor de onde ela buscará as informações;
2.2.20. Os agentes para plataforma Microsoft deverão ser instalados por pacote MSI e posteriormente ativados pela console de gerenciamento de forma a proporcionar maior segurança ao ambiente, ou de forma automatizada através de script PowerShell;
2.2.21. Os agentes para plataforma Linux deverão ser instalados por pacote RPM ou DEB e posteriormente ativados pela console de gerenciamento de forma a proporcionar maior segurança ao ambiente, ou de forma automatizada através de bash script;
2.2.22. Em servidores Windows e Linux, a solução deverá permitir a atualização automática dos agentes após sua ativação;
2.2.23. Para efeito de administração, a solução deverá avisar quando um agente se encontrar não conectado a sua console de gerenciamento;

2.2.24. Deve permitir a remoção automática de agentes inativos, definindo o período para, pelo menos 1 semana, 1 mês e 12 meses;
2.2.25. A solução deve possuir a capacidade de criar políticas de forma global para todas as máquinas, por perfis e individualmente para cada host;
2.2.26. Cada perfil poderá ser atribuído para um host ou um conjunto de hosts;
2.2.27. A solução deverá vir com perfis pré-definidos e aptos a funcionarem de acordo com sua denominação;
2.2.28. A solução deverá mostrar quais máquinas estão usando determinada política;
2.2.29. Os agentes deverão ser capazes de executar rastreamento nas máquinas onde estão instalados e após isso deverão fornecer uma lista de todas as recomendações de segurança para os softwares que estejam instalados nas máquinas bem como do sistema operacional;
2.2.30. Esses rastreamentos devem ocorrer de forma periódica a ser definida pelo administrador;
2.2.31. A solução deverá permitir a configuração de componentes de integração com o vCenter, a fim de permitir a sincronização das máquinas virtuais conectadas a ele;
2.2.32. Brechas de segurança descobertas deverão ser protegidas de forma automática e transparente, interrompendo somente o tráfego de rede malicioso;
2.2.33. O administrador do sistema de segurança deverá ter a possibilidade de não aplicar automaticamente a proteção para as vulnerabilidades escolhendo o perfil ou o host;
2.2.34. A solução deve possuir a capacidade de isolamento de placa de rede de forma que apenas uma fique funcionando de acordo com preferência do administrador;
2.2.35. A solução deverá ser capaz de aplicar políticas diferentes para placas de redes diferentes em um mesmo servidor;
2.2.36. A solução deverá ser capaz de executar bypass completo de rastreamento de tráfego de forma que os módulos não atuem em determinado tipo de conexão ou pacote;
2.2.37. A solução deverá ter a capacidade de se integrar com o Amazon SNS e os principais softwares de SIEMs contemplando, no mínimo: Splunk, HPArcSight e IBMQradar, de modo a permitir enviar os seus logs para essas soluções;
2.2.38. A solução deverá ter a possibilidade de enviar logs para SYSLOG servers;
2.2.39. Solução deverá permitir criar relatórios customizados de todas as suas funcionalidades;
2.2.40. Deve permitir enviar os relatórios para uma lista de contatos independente de login na console de administração;
2.2.41. As atualizações de assinaturas deverão ocorrer de forma agendada e automática possibilitando ser até mesmo de hora em hora;
2.2.42. Após a atualização deve ser informado o que foi modificado ou adicionado;
2.2.43. Deve ser possível baixar as assinaturas na console de gerenciamento, mas não as distribuir aos clientes;
2.2.44. A console de gerenciamento deve apresentar a capacidade de gerar roll back de suas atualizações de regras;
2.2.45. A solução deverá ter capacidade de gerar pacote de autodiagnóstico de modo a coletar arquivos relevantes para envio ao suporte do produto;
2.2.46. Deverá ter a capacidade de colocar etiquetas para a ocorrência de determinados eventos de modo a facilitar o gerenciamento, relatórios e visualização;
2.2.47. No gerenciamento de licenças, deve ser informada quantidade contratada e quantidade em utilização de clientes;
2.2.48. Solução deverá ter mecanismo de procura em sua console de gerenciamento de modo que seja facilitada a busca de regras;
2.2.49. Deverá possuir a capacidade de classificar eventos para que facilite a identificação e a visualização de eventos críticos em servidores críticos;

2.2.50. Deverá possibilitar colocar etiquetas em eventos para que se possam visualizar apenas os eventos desejados;
2.2.51. O fabricante deverá participar do programa “Microsoft Application Protection Program” para obtenção de informações de modo a permitir a criação de regras de proteção antes mesmo dos patches serem publicados pelo fabricante;
2.2.52. A console de gerenciamento deve se integrar com o Vmware vCloud, de modo a importar e sincronizar os objetos (hosts vmware e guests vm) para a console de gerenciamento da solução;
2.2.53. O fabricante da solução deverá manter programa de pesquisa em vulnerabilidades há, pelo menos, 5 anos;
2.2.54. A solução deve possuir API documentada para integração na esteira de automação;
2.2.55. A documentação da API deve conter exemplos prontos para implementação de determinadas funcionalidades, como cookbooks;
2.2.56. Precisa ter a capacidade de detectar e aplicar as regras necessárias dos módulos de IDS/IPS, Monitoramento de Integridade e Inspeção de Logs, para cada servidor, de forma automática e sem a intervenção do administrador;
2.2.57. A solução deve permitir desabilitar os módulos individualmente;
2.2.58. Precisa ter a capacidade de desabilitar as regras não mais necessárias dos módulos de IDS/IPS, Monitoramento de Integridade e Inspeção de Logs, para cada servidor, de forma automática e sem a intervenção do administrador;
2.2.59. A console deverá possibilitar a integração com o Microsoft Active Directory, listando as máquinas e grupos existentes na estrutura;
2.2.60. Em caso da solução ser ofertada em nuvem, deve ser compliance com ISO 27001, ISO 27014, ISO 27017 e SOC 2;
2.2.61. Os ambientes em nuvem providos pelo fabricante devem passar por testes de penetração de forma recorrente como para garantir a segurança da solução provida.
2.2.62. Deverá possuir funcionalidade de Antimalware;
2.2.63. A solução deve permitir a proteção contra códigos maliciosos através da instalação de agentes, permitindo rastrear ameaças em tempo real, varredura sob demanda e conforme agendamento, possibilitando a tomada de ações distintas para cada tipo de ameaça;
2.2.64. A solução deve possibilitar a criação de listas de exclusão, para que o processo do antivírus não execute a varredura de determinados diretórios ou arquivos do SO;
2.2.65. A solução deve possuir listas de exclusão separadas por módulo da proteção antimalware como exclusão das detecções por comportamento, exclusão por machine learning e exclusão por assinatura;
2.2.66. Em plataforma Windows, a solução deve permitir criar exclusões de escaneamento a partir do certificado digital das aplicações;
2.2.67. A solução deve possibilitar a verificação de ameaças dentro de arquivos compactados, efetuando a limpeza apenas de arquivos maliciosos em casos de detecção. A limpeza deve ocorrer sem a descompactação do arquivo;
2.2.68. Em servidores Windows, deve identificar e bloquear ameaças através de métodos de Machine Learning, quarentenando arquivos identificados;
2.2.69. A solução deverá possuir a funcionalidade de Monitoramento de Comportamento para detectar mudanças e atividades suspeitas não autorizadas;
2.2.70. A solução deverá oferecer escanear processos em memória em busca de Malware;
2.2.71. O scan de arquivos comprimidos deverá ser de no mínimo 6 camadas de compressão;
2.2.72. O scan de arquivos comprimidos do tipo OLE deverá ser de no minimo 20 camadas de compressão;
2.2.73. Para servidores Windows, a solução deverá permitir que o escaneamento agendado ocorra, ainda que o agente esteja offline na console de gerenciamento;
2.2.74. A solução deverá possuir ações pré-configuradas para cada tipo de ameaça detectada ou tomar uma ação baseada na configuração padrão da ferramenta;

2.2.75. Em servidores Windows, a solução deverá integrar-se com interface AMSI (Antimalware Scan Interface);
2.2.76. A solução deverá mostrar informação de data sobre o último scan agendado ou manual executado;
2.2.77. Possuir a capacidade de efetuar backup e restore de arquivos comprometidos por Ransomware;
2.2.78. Deve possuir cache dos arquivos verificados de modo a evitar a redundância da varredura;
2.2.79. Deve possibilitar o controle do consumo de memória durante as varreduras a fim de minimizar os impactos de desempenho no servidor;
2.2.80. A solução deve possuir opção para forçar a comunicação com o agente e coletar os respectivos logs;
2.2.81. Em servidores Windows, deve possuir capacidade de detectar ameaças por comportamento;
2.2.82. Deverá ter a possibilidade de escanear drivers de rede mapeados nos servidores.
2.2.83. Proteção Contra URLs Maliciosas
2.2.84. Deve permitir a proteção contra acesso a websites ou URLs consideradas maliciosas ou de baixa reputação;
2.2.85. A lista de URLs deve ser fornecida e atualizada automaticamente pelo fabricante, permitindo a consulta em uma base local ou na nuvem da reputação das URLs acessadas;
2.2.86. A solução deve permitir alterar o nível de sensibilidade para detecção de URLs maliciosas tendo, pelo menos, os níveis Alto, médio e baixo;
2.2.87. Deve permitir a criação de listas de exclusão, permitindo que usuários acessem determinadas URLs especificadas pelo administrador do sistema;
2.2.88. Deve permitir configurar notificações personalizadas para detecções desse módulo, deixando a cargo do administrador exibir ou não tais notificações;
2.2.89. Deverá ter capacidade de identificar acessos a URLs maliciosas além das portas padrão 80 e 443;
2.2.90. A solução deve permitir que o administrador reclassifique uma URL através do site do fabricante para evitar falsos positivos;
2.2.91. A proteção deve possibilitar proteção através da instalação de agente de segurança do fabricante da solução de segurança.
2.2.92. Deverá possuir funcionalidade de Firewall de host;
2.2.93. Operar como firewall de host, através da instalação de agente nos servidores protegidos;
2.2.94. Precisa ter a capacidade de controlar o tráfego baseado no Endereço MAC, Frame types, Tipos de Protocolos, Endereços IP e intervalo de portas;
2.2.95. Precisa ter a capacidade de controlar conexões TCP baseado nas Flags TCP;
2.2.96. Precisa ter a capacidade de definir regras distintas para interfaces de rede distintas;
2.2.97. A solução deverá ser capaz de reconhecer e possibilitar o bloqueio endereços IP que estejam realizando Network Scan, Port Scan, TCP Null Scan, TCP FYNSYN Scan, TCP Xmas Scan e Computer OS FIngerprint por até 30 minutos;
2.2.98. Precisa ter a capacidade de implementação de regras em determinados horários que podem ser customizados pelo administrador;
2.2.99. Precisa ter a capacidade de definição de regras para contextos específicos;
2.2.100. Para facilitar a criação e administração de regras de firewall, as mesmas poderão se apoiar em objetos que podem ser lista de ips, lista de MACs, lista de portas;
2.2.101. Regras de firewall poderão ou não ser válidas de acordo com o contexto em que a máquina se encontra (por exemplo, se está no domínio ou não);
2.2.102. Regras de firewall poderão ou não ser válidas de acordo com agendamento por horário ou dia da semana;
2.2.103. O firewall deverá ser stateful bidirecional;
2.2.104. O firewall deverá permitir liberar ou apenas logar eventos;
2.2.105. O firewall deverá ser passível de criação de regras através do protocolo, origem do tráfego, frame type, TCP header flags, destino e direção;

2.2.106. As regras de Firewall deverão ter as seguintes ações, ou equivalentes: Allow, log only, bypass, force allow, deny;
2.2.107. A solução, para facilidade de administração, deverá utilizar o conceito de regras implícitas para a regra ALLOW, negando o tráfego para todo o restante que não estiver liberado;
2.2.108. As ações também deverão ser possíveis de terem prioridades diferentes, sendo que a prioridade maior prevalece sobre a prioridade menor;
2.2.109. Deverá realizar pseudo stateful em tráfego UDP;
2.2.110. Deverá logar a atividade stateful;
2.2.111. Deverá permitir limitar o número de conexões entrantes e o número de conexões de saída de um determinado computador;
2.2.112. Deverá permitir limitar o número de meias conexões vindas de um computador;
2.2.113. Deverá prevenir ack storm;
2.2.114. Deverão existir regras default que possam ser utilizadas como modelo para a criação e adição de novas regras;
2.2.115. Deverá identificar escaneamentos ativos de porta ou da rede, bloqueando o IP ofensor por um período configurado pelo administrador;
2.2.116. Deverá permitir criar lista de exceções para identificar os IPs autorizados a realizar varreduras de portas ou da rede;
2.2.117. Poderá atuar no modo em linha para proteção contra-ataques ou modo escuta para monitoração e alertas.
2.2.118. Proteção contra Vulnerabilidades de Sistemas Operacionais e Aplicações
2.2.119. Precisa ter a capacidade de detectar e bloquear qualquer conexão indesejada que tente explorar vulnerabilidades do SO e demais aplicações;
2.2.120. Precisa ter a capacidade de varrer o servidor protegido detectando o tipo e versão do Sistema Operacional, detectando também as demais aplicações, recomendando e aplicando automaticamente regras IDS/IPS que blindem vulnerabilidades existentes no SO e aplicações. Esta varredura deverá poder ser executada sob demanda ou agendada;
2.2.121. A solução deverá conter regras pré-definidas para detecções de ransonware para as principais famílias deste tipo de malware;
2.2.122. Precisa ter a capacidade de detectar uma conexão maliciosa, com a possibilidade de bloquear esta conexão;
2.2.123. Precisa conter regras de defesa para blindagem de vulnerabilidades e ataques que explorem os seguintes sistemas operacionais: Windows 2003, 2008, 2012, 2016, 2019, Linux Red Hat, Suse, CentOS, Ubuntu, Debian, Solaris, AIX além de regras para aplicações padrão de mercado, incluindo Microsoft IIS, SQL Server, Microsoft Exchange, Oracle Database, Adobe Acrobat, Mozilla Firefox, Microsoft Internet Explorer, Google Chrome e Web Server Apache;
2.2.124. Precisa ter a capacidade de armazenamento do pacote capturado quando detectado um ataque;
2.2.125. Deverá possibilitar a criação de regras de IPS customizadas, para proteger aplicações desenvolvidas pelo cliente;
2.2.126. Precisa possuir a capacidade de detectar e controlar conexões de aplicações específicas incluindo Team Viewer, programas P2P e instant Messaging;
2.2.127. Precisa ter a capacidade de detectar e bloquear ataques em aplicações Web tais como SQL Injection e Cross Site Scripting. Deverá ainda existir a possibilidade de captura do pacote relacionado ao ataque para fins de investigação do incidente;
2.2.128. Deverá permitir customização avançada e criação de novas regras de proteção de aplicações web, protegendo contra vulnerabilidades específicas de sistemas web legados e/ou proprietários;
2.2.129. Ser capaz de permitir ou negar que métodos utilizados por Webservers por regras de IPS;
2.2.130. Regras de IDS/IPS poderão ou não ser válidas de acordo com o contexto em que a máquina se encontra (por exemplo se está no domínio ou não);

2.2.131. Regras de IDS/IPS poderão ou não ser válidas de acordo com agendamento por horário ou dia da semana;
2.2.132. Deverá ser capaz de inspecionar tráfego criptografado de entrada;
2.2.133. Deverá inspecionar tráfego de aplicações Web em servidores buscando identificar: SQL injection, Crossite script, tamanho de URI fora de padrão, caracteres fora de padrão para requisição de URI, Double Decoding Exploit;
2.2.134. As regras de blindagem contra vulnerabilidades deverão conter links com referências externas, isto quando aplicável, explicando a vulnerabilidade do fabricante ou CVE relacionado;
2.2.135. Deverá possibilitar a criação de regras manuais para o bloqueio de tráfego customizado. Como por exemplo, bloquear acesso a um determinado website ou bloquear acesso de uma aplicação X;
2.2.136. Deverá possibilitar a criação de regras manuais baseadas em padrão XML, forma de assinatura ou padrões que possuam começo e fim coincidentes;
2.2.137. Deverá bloquear tráfego por aplicação independente da porta que a aplicação utilize, de modo que a aplicação não consiga comunicar na rede, como por exemplo, bloqueio de tráfego de uma determinada web browser ou aplicação de backup;
2.2.138. Solução deve ser capaz de habilitar modo debug na coleta dos pacotes de forma a capturar o tráfego anterior e posterior ao que foi bloqueado para facilidade de análise;
2.2.139. As regras de IPS deverão obrigatoriamente ter descrições de seu propósito;
2.2.140. As regras de IPS poderão atuar detectando ou bloqueando os eventos que as violem de modo que o administrador possa optar por qual ação tomar;
2.2.141. As regras de IPS de vulnerabilidade deverão apresentar severidade baseada em CVEs;
2.2.142. As regras de IPS poderão ter sua capacidade de LOG desabilitado;
2.2.143. As regras de IPS quando disparadas poderão ter a possibilidade de emitir um alerta;
2.2.144. As regras devem ser atualizadas automaticamente pelo fabricante;
2.2.145. Poderá atuar no modo em linha para proteção contra-ataques ou modo escuta para monitoração e alertas.
2.2.146. Monitoramento De Integridade para Servidores
2.2.147. A solução deverá permitir a implantação nas plataformas Linux, Microsoft, Solaris, HP-UX, AIX, através da instalação de agentes;
2.2.148. Precisa ter a capacidade de detectar mudanças de integridade em arquivos e diretórios do SO e aplicações terceiras;
2.2.149. Precisa ser capaz de detectar mudanças no estado de portas em sistemas operacionais Linux;
2.2.150. Precisa ter a capacidade de monitorar o status de serviços e processos do sistema operacional;
2.2.151. Precisa ter a capacidade de monitorar mudanças efetuadas no registro do Windows;
2.2.152. Precisa ter a capacidade de criação de regras de monitoramento em chaves de registro, diretórios e subdiretórios e customização de XML para criação de regras avançadas;
2.2.153. Precisa ter a capacidade de varrer o sistema operacional e aplicações, recomendando e aplicando automaticamente regras de monitoramento de acordo com o resultado desta varredura. Esta varredura deverá poder ser executada sob demanda ou agendada;
2.2.154. O monitoramento poderá ser realizado em tempo real ou utilizando de scans periódicos para detectar mudanças de integridade;
2.2.155. Deverá alertar toda vez que uma modificação ocorrer em tempo real para ambiente Windows e pseudo real- time para ambiente Linux;
2.2.156. Deverá logar e colocar em relatório todas as modificações que ocorram;
2.2.157. As regras de monitoramento de integridade deverão ser atualizadas pelo fabricante ou melhoradas de forma automática;
2.2.158. Deverá poder classificar as regras de acordo com severidade para melhor verificação nos logs e recebimento de alertas;

2.2.159. Deverá possibilitar escolher o diretório onde o arquivo será monitorado e incluir ou não incluir determinados tipos de arquivos dentro desse mesmo diretório;
2.2.160. Algumas regras podem ser modificadas pelo administrador para adequação ao seu ambiente.
2.2.161. Deverá possuir capacidade de Inspeção de Logs para Servidores
2.2.162. A solução deverá permitir sua implantação nas plataformas Linux, Microsoft, Solaris, HP-UX, AIX;
2.2.163. Precisa ter a capacidade de monitorar e inspecionar arquivos de log do sistema operacional e demais aplicações, gravando uma cópia deste log em um banco de dados externo e notificando o administrador sobre eventos suspeitos;
2.2.164. Precisa ter a capacidade de varrer o sistema operacional e aplicações, recomendando e aplicando automaticamente regras de inspeção de logs de acordo com o resultado desta varredura. Esta varredura deverá poder ser executada sob demanda ou agendada;
2.2.165. Precisa permitir a criação de regras de inspeção de logs adicionais para auditoria de logs de aplicações terceiras;
2.2.166. Precisa permitir a customização de regras existentes, adicionando, removendo ou modificando regras de inspeção de logs;
2.2.167. Deverá rastrear e indicar/sugerir ao administrador do sistema quais softwares estão instalados e que possuem logs passíveis de inspeção;
2.2.168. Deverá possibilitar a criação de regras de inspeção de logs para aplicações customizadas;
2.2.169. Deverá ter inteligência para que a cada violação relevante no log inspecionado que possa comprometer a segurança do ambiente ou do servidor seja alertada;
2.2.170. Deverá ter inteligência para que a cada violação relevante no log inspecionado que seja suspeita no servidor seja alertada;
2.2.171. Deverá logar cada violação e colocar em relatório todas as violações relevantes que ocorram;
2.2.172. As regras poderão ser modificadas por severidade de ocorrência de eventos;
2.2.173. As regras devem se atualizar automaticamente pelo fabricante;
2.2.174. Permitir modificação pelo administrador em regras para adequação ao ambiente.
2.2.175. Deverá possuir capacidades de Controle De Aplicações
2.2.176. A solução deverá permitir sua implantação nas plataformas Linux e Microsoft Windows;
2.2.177. O controle de aplicações deverá ser realizado através de Hash, suportando no mínimo MD5, SHA1 e SHA256;
2.2.178. O agrupamento dos eventos deverá ser realizado pelo menos por Hash ou por máquina;
2.2.179. A console deverá exibir eventos de no mínimo 30 dias;
2.2.180. A solução deverá possuir um mecanismo ao qual permita a execução de aplicações e scripts automaticamente, sem intervenção manual, por um determinado período que deve ser no máximo 10 horas;
2.2.181. A solução deverá possuir no mínimo as funcionalidades de bloquear o que não for permitido explicitamente e permitir o que não for bloqueado explicitamente.
2.2.182. Deverá possuir funcionalidades de de Detecção e Resposta;
2.2.183. A solução deve possuir módulo de investigação, detecção integrados;
2.2.184. Deve permitir que as detecções sejam correlacionadas com módulos de endpoint, rede e e-mail do próprio fabricante através de console dedicada. Não serão aceitas consoles de correlação de terceiros;
2.2.185. A console de correlação deve estar disponível na nuvem do próprio fabricante, o qual deve ser responsável pelas manutenções, atualizações e disponibilidade;
2.2.186. Deve possuir capacidade de encaminhar as atividades suspeitas identificadas nos servidores para a console de correlação centralizada;
2.2.187. O módulo de detecção e resposta deve atuar baseado em modelos de detecção de ataques avançados e furtivos;
2.2.188. Os logs de detecções devem estar disponíveis na console por, pelo menos, 30 dias;

2.2.189. A console de correlação centralizada deve possuir informações a respeito dos principais ataques que estão ocorrendo no mundo, quais plataformas e países são afetados, além de links para obter mais informações;
2.2.190. A solução deve permitir realizar buscas em todos os dados de atividades enviadas pelos servidores e demais sensores que estejam conectados na console, ainda que estas não sejam detectadas como maliciosas;
2.2.191. A console deve permitir o Single Sign-On através de SAML ou padrão equivalente;
2.2.192. Deve ser possível criar usuários com permissões distintas, contendo no mínimo, permissão total e permissão para realizar investigações;
2.2.193. Deve permitir habilitar ou desabilitar um determinado usuário sem excluí-lo da console;
2.2.194. Deve permitir o envio de notificações para os administradores através de email, API e integrações com SIEMs;
2.2.195. Deve prover visualização em linha do tempo com informações dos eventos monitorados em cada servidor;
2.2.196. Deve permitir a visualização entre usuários, servidores, processos/comandos, arquivos e demais componentes correlacionados em determinado ataque;
2.2.197. Deverá informar com qual técnica e tática do MITRE ATT&CK framework o ataque está relacionado, além de possuir link direto para o site da organização;
2.2.198. A solução deve mostrar, pelo menos, o timestamp, objetos envolvidos (comandos, processos, usuários, servidores);
2.2.199. Ao clicar em quaisquer dos objetos, a solução deve permitir realizar buscar específicas pelo objeto ou ainda executar ações como executar investigações mais aprofundadas.
2.2.200. A solução deverá por meio de agente único possibilitar a conexão com a plataforma de detecção e resposta do próprio fabricante de maneira nativa sem a necessidade de plug-ins ou agentes adicionais;
2.2.201. Esta conexão deverá garantir, sem qualquer configuração local, que o sensor de detecção e resposta esteja ativo e envie telemetria a plataforma;

4 – PRAZO DE CONTRATO

O prazo de **vigência das licenças foi definido em 24 (vinte e quatro) meses**, considerando a natureza do objeto e a política de licenciamento adotada pelos principais fabricantes de soluções de antivírus corporativo.

Esse período é o mais adequado para garantir estabilidade técnica, continuidade operacional e economicidade na contratação, evitando interrupções frequentes para renovações e reduzindo custos administrativos e operacionais associados à gestão contratual.

A vigência de 2 (dois) anos também se mostra tecnicamente justificada, pois permite o acompanhamento completo de um ciclo de atualizações da solução, abrangendo eventuais evoluções de versão, ajustes de segurança e novas funcionalidades disponibilizadas pelo fabricante. Dessa forma, assegura-se à Administração o uso de tecnologia atualizada e plenamente funcional durante todo o período de licenciamento.

Sob o aspecto econômico, a contratação com vigência bienal permite a obtenção de melhores condições comerciais, uma vez que os fornecedores costumam praticar valores mais vantajosos em licenças com períodos de validade superiores a 12 meses. Assim, a medida contribui diretamente para a vantajosidade e economicidade da contratação, princípios que norteiam a atuação administrativa.

O **prazo contratual acompanhará a vigência das licenças, estabelecendo-se igualmente por 2 (dois) anos**, podendo ser prorrogado por iguais e sucessivos períodos, conforme o disposto no art. 107 da Lei nº

14.133/2021, desde que devidamente justificado e mantidas as condições de vantajosidade, economicidade e interesse público.

A possibilidade de prorrogação visa garantir continuidade na prestação dos serviços de proteção e segurança da informação, evitando descontinuidade do sistema e novos custos de implantação, treinamento ou migração, caso fosse necessária a substituição da solução.

Portanto, a definição do prazo de vigência das licenças e do contrato em dois anos, com previsão de prorrogação legalmente autorizada, encontra-se tecnicamente adequada, juridicamente amparada e economicamente vantajosa, assegurando à Administração a continuidade da política de segurança digital e o uso racional dos recursos públicos.

5 – REQUISITOS DA CONTRATAÇÃO

A contratação tem por finalidade garantir a continuidade da proteção dos ativos tecnológicos da Administração Municipal por meio de solução antivírus corporativa capaz de prevenir, detectar e responder a ameaças digitais.

A solução deverá manter o padrão tecnológico já utilizado no ambiente do Município, assegurando compatibilidade, estabilidade e continuidade operacional, evitando custos e riscos decorrentes de migrações desnecessárias.

A solução a ser contratada deverá oferecer proteção abrangente contra *vírus, malwares, ransomwares, spywares*, trojans e demais tipos de ameaças cibernéticas, atuando de forma proativa na identificação e bloqueio de comportamentos suspeitos. É indispensável que disponha de console centralizado de gerenciamento, permitindo à equipe técnica administrar de forma unificada as políticas de segurança, realizar a instalação remota de agentes, acompanhar o status de atualização e emitir relatórios gerenciais e técnicos sobre a situação de segurança dos equipamentos.

Deverá ainda possibilitar integração com o ambiente de rede já existente, incluindo servidores físicos e virtuais, estações de trabalho e diretórios de autenticação (*como o Active Directory*), de modo que não haja necessidade de reconfiguração da infraestrutura ou de substituição de componentes. A compatibilidade com diferentes sistemas operacionais (*Windows, Linux e macOS*) também é requisito essencial, considerando a diversidade de plataformas em uso pela Administração.

A solução deve apresentar desempenho otimizado, com baixo consumo de recursos e proteção mesmo em situações de ausência temporária de conexão com a internet. É desejável que incorpore mecanismos modernos de detecção e resposta a ameaças (*EDR*), permitindo isolar dispositivos potencialmente comprometidos e registrar eventos de segurança para análise posterior.

Durante toda a vigência contratual, deverão estar incluídos suporte técnico e atualizações contínuas do fabricante, garantindo que a ferramenta permaneça atualizada frente a novas ameaças e vulnerabilidades. O suporte deverá ser prestado em língua portuguesa, por meio de canais adequados como e-mail, telefone ou portal técnico.

As licenças fornecidas deverão ser corporativas, emitidas em nome da Administração Municipal, com prazo mínimo de vigência de 24 meses, abrangendo a quantidade necessária de estações de trabalho, servidores e dispositivos móveis. A entrega das licenças e o acesso ao console administrativo deverão ocorrer em prazo compatível com a necessidade de continuidade do serviço, sem interrupção da proteção vigente.

A manutenção da estrutura tecnológica já consolidada é fundamental para garantir a eficiência operacional, uma vez que os servidores municipais já estão capacitados no uso e na administração da solução atual. Essa continuidade evita retrabalho, elimina custos de migração e treinamento e assegura a proteção imediata dos sistemas municipais, que dependem do antivírus para manter a integridade das informações e a segurança dos serviços públicos prestados à população.

Dessa forma, os requisitos estabelecidos visam garantir a adoção de uma solução tecnicamente adequada, economicamente vantajosa e plenamente compatível com o ambiente tecnológico existente, assegurando a continuidade e a confiabilidade da infraestrutura de segurança da informação do Município.

5.1 - Subcontratação: Não será permitida a subcontratação;
5.2 – Garantia Contratual: Não será exigida garantia contratual;

6 – EXECUÇÃO DO OBJETO

A execução do objeto compreenderá o fornecimento das licenças de uso da solução antivírus corporativa, em formato digital, bem como o suporte técnico e as atualizações necessárias para garantir o pleno funcionamento do sistema durante toda a vigência contratual.

Após a formalização do contrato, a contratada deverá disponibilizar as licenças, através do e-mail *suporte@americana.sp.gov.br*, as chaves de ativação e o acesso ao console de gerenciamento centralizado, observando os prazos estabelecidos. As licenças deverão ser entregues em conformidade com a estrutura tecnológica atualmente implantada na Administração Municipal, de forma a garantir a continuidade do serviço e a proteção ininterrupta dos ativos de tecnologia da informação.

A ativação das licenças ocorrerá sob a supervisão da equipe técnica da área de TI do Município, que realizará as validações necessárias quanto à compatibilidade e integração com os sistemas já existentes. A contratada deverá prestar todo o apoio técnico necessário à instalação e configuração, inclusive por meio de atendimento remoto, assegurando o correto funcionamento do software em todos os equipamentos contemplados.

Durante o período de vigência, caberá à contratada garantir o acesso contínuo às atualizações de segurança, upgrades de versão e suporte técnico do fabricante, de forma a manter a solução permanentemente atualizada e eficaz contra novas ameaças. O suporte deverá incluir esclarecimento de dúvidas, tratamento de incidentes, correção de falhas e orientações sobre boas práticas de uso e administração do antivírus pelo fabricante.

A execução do objeto também inclui o acompanhamento operacional por parte da área técnica municipal, responsável por monitorar o desempenho, a cobertura de proteção e o cumprimento das condições contratuais.

Caso haja necessidade de ajustes de configuração, substituição de chaves ou realocação de licenças entre dispositivos, essas ações deverão ser realizadas de forma coordenada entre a contratada e a equipe interna, garantindo que não haja descontinuidade na proteção.

A contratada deverá ainda manter disponíveis os canais de atendimento técnico, preferencialmente em língua portuguesa, para suporte remoto durante todo o período contratual, bem como assegurar que a solução permaneça ativa, funcional e com atualizações automáticas de assinaturas e mecanismos de detecção de ameaças.

A execução será considerada satisfatória quando todas as licenças estiverem devidamente instaladas, ativas e integradas ao ambiente municipal, com o pleno funcionamento do console de gestão, relatórios operacionais acessíveis e proteção ativa em todos os dispositivos contemplados.

Assim, a execução do objeto visa assegurar a continuidade da política de segurança da informação do Município, garantindo proteção permanente, estabilidade da infraestrutura de TI e conformidade com as boas práticas de gestão tecnológica.

7 – GESTÃO DO CONTRATO

7.1 - O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133/2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial.
7.2 - A execução do Contrato deverá ser acompanhada e fiscalizada respectivamente por:

Gestor: Sandro Pereira Brito – Encarregado Serviços IV – Matrícula 15.496 (Secretaria de Comunicação e TI)
Fiscal: Agnaldo de Oliveira Junior – Diretor de Unidade - matrícula 13.423 (Secretaria de Saúde)

8 – MEDIÇÃO E PAGAMENTO

8.1 – O pagamento será mensal através de aceite ocorrido o recebimento da nota fiscal ou fatura quando da execução do objeto do Contrato.
8.2 - O pagamento será efetuado no prazo de até 30 (trinta) dias, contados do aceite da Nota Fiscal/Fatura.
8.3 – O pagamento será realizado através de ordem bancária, para crédito em banco, agência e conta corrente indicados pela contratada.
8.4 - A contratada deverá apresentar a Certidão Conjunta de Débitos Relativos a Tributos Federais e à Dívida Ativa da União, abrangendo contribuições sociais, nos termos da Portaria MF nº 358, de 05 de setembro de 2014 e a Certidão de Regularidade Fiscal – CRF do FGTS juntamente com a nota fiscal, para fins de comprovação das condições de habilitação.
8.5 - As retenções na fonte do Imposto de Renda (IR) incidentes sobre o pagamento destinados às pessoas físicas estarão sujeitos à legislação aplicada relativa ao imposto de renda retido na fonte de pessoas físicas, em especial, a IN nº 1.500, de 29/70/2014, e suas alterações.

9 – SELEÇÃO DO FORNECEDOR

O fornecedor será selecionado por meio da realização de procedimento de Licitação, na modalidade PREGÃO, sob a forma ELETRÔNICA, critério de julgamento menor preço global.
9.1 – Amostra ou Prova de Conceito - Não será necessário.
9.3 – Participação de Consórcio – Não será permitida a participação em consórcio por se tratar de serviço comum, que não demanda expertises, passível, portanto, a qualquer empresa do ramo, pequeno porte, médio ou grande, que detenha a qualificação técnica, econômica e a qualificação técnica, econômica e jurídica suficientes para a execução do serviço solicitado.
9.5 – Garantia de Proposta – Não se aplica.

10 - QUALIFICAÇÃO TÉCNICA

10.1 - HABITLITAÇÃO: (art. 67 da Lei 14.113/2021)

Comprovação da capacitação técnico-operacional, emitido(s) por pessoa jurídica de direito público ou privado, que comprove(m) o fornecimento da solução de antivírus corporativo, em quantidade e complexidade compatíveis com o objeto desta contratação.

10.2 – **DOCUMENTOS A SEREM ENTREGUES PELA DETENTORA DA MELHOR PROPOSTA:**

Caso o licitante não seja o fabricante da solução, deverá apresentar, sob pena de desclassificação, declaração emitida pelo fabricante que comprove ser o licitante revendedor, com autorização expressa para comercializar, no território nacional, as licenças de uso do software objeto da contratação.

11 – ESTIMATIVA DE PREÇO

Realizada conforme Art. 23 da Lei 14.133/2021 e Art. 29 do Decreto Municipal 13.826/2025.

Em razão da especificidade do objeto, que envolve solução de antivírus corporativo compatível com a infraestrutura tecnológica já existente na Administração Municipal, a estimativa de preço foi elaborada com base em análises técnicas especializadas e levantamento de valores praticados no mercado.

Devido à necessidade de assegurar a viabilidade de instalação e integração com o ambiente atual, foram realizadas consultas e cotações junto a fornecedores do ramo de segurança da informação, devidamente credenciados e autorizados a comercializar o software no Brasil. As empresas consultadas apresentaram propostas considerando as características técnicas exigidas e o porte da estrutura a ser atendida, permitindo à Administração avaliar as condições mais adequadas de fornecimento, suporte e licenciamento.

Além das cotações obtidas no mercado, a área técnica também realizou análise comparativa com contratos anteriormente firmados pela Administração Municipal, relativos ao mesmo objeto ou a soluções tecnológicas equivalentes. Essa comparação possibilitou verificar a manutenção da compatibilidade tecnológica, bem como a coerência dos preços atualmente praticados em relação ao histórico de contratações do Município.

Como forma de ampliar a base de referência e assegurar a fidedignidade da estimativa, foram ainda analisadas contratações realizadas por outros órgãos públicos de porte e necessidades semelhantes, cujos objetos apresentavam compatibilidade técnica com o presente processo. Essas referências adicionais contribuíram para validar a adequação dos valores estimados e reforçar a observância aos princípios da vantajosidade e da economicidade.

A estimativa final de preço, portanto, resultou da avaliação conjunta das propostas obtidas junto a fornecedores, dos valores contratados anteriormente pela Administração Municipal e dos preços praticados em contratações públicas correlatas, garantindo que o valor adotado como referência reflita o preço médio de mercado, tecnicamente justificado e economicamente viável.

Essa metodologia de apuração proporciona à Administração segurança quanto à adequação dos custos estimados, assegurando a conformidade com os princípios da razoabilidade, transparência e eficiência, conforme dispõe a Lei nº 14.133/2021, e garantindo que a futura contratação seja tecnicamente adequada e financeiramente vantajosa ao interesse público.

12 – ADEQUAÇÃO ORÇAMENTÁRIA

A Administração Municipal certifica que há programação orçamentária para essa despesa.

13 – FONTE DE RECURSO

Recursos Próprios de cada Secretaria (Secretaria de Comunicação e TI e Secretaria de Saúde)

ANEXO IV – MODELO DE PROPOSTA FINANCEIRA

PREGÃO ELETRÔNICO: 131/2025
PROCESSO ADMINISTRATIVO: N. º 9.444/2025

Este formulário poderá ser transformado em Proposta Financeira, desde que seja preenchido e assinado.

Proponente: _____
Endereço: _____
Bairro: _____
CEP: _____ **Cidade:** _____ **Estado:** _____
Telefone: _____ **Fax:** _____**E-mail**_____

LOTE ÚNICO

ITEM	Unid.	DESCRIÇÃO	Quant.	VALOR UNITÁRIO R$	VALOR TOTAL R$
1	serv.	RENOVAÇÃO LICENÇA DE USO DE PROGRAMAS DE COMPUT.TREND VISION ONE – ENDPOINT SECURITY (CORE) ESTAÇÕES DE TRABALHO. **RENEW - Part Number – VORA0026**	**650**		
2	serv.	RENOVAÇÃO LICENÇA DE USO DE PROGRAMAS DE COMPUT. TREND VISION ONE – ENDPOINT SECURITY (PRO-CLOUD) SERVIDORES. **RENEW - Part Number – VORA0041**	**3**		
3	serv.	AQUISIÇÃO LICENÇA DE USO DE PROGRAMAS DE COMPUT. - TREND VISION ONE - ENDPOINT SECURITY (CORE) ESTAÇÕES DE TRABALHO. **NEW - Part Number – VONA0028**	**400**		
		VALOR GLOBAL R$			

Serão aceitas até 02 (duas) casas decimais no preço unitário de cada item ofertado.

A(s) licitante(s) detentora(s) da melhor proposta deverá(ão) apresentar, por meio do sistema, no prazo de 02 (duas) horas, contadas da solicitação do Pregoeiro no sistema:

a) **Proposta de preços atualizada;**
b) **A documentação de habilitação;**
c) **Caso o licitante não seja o fabricante da solução, deverá apresentar, sob pena de desclassificação, declaração emitida pelo fabricante que comprove ser o licitante revendedor, com autorização expressa para comercializar, no território nacional, as licenças de uso do software objeto da contratação.**

CONDIÇÕES DE EXECUÇÃO: Conforme Termo de Referência do Anexo III.

***CONDIÇÕES DE PAGAMENTO*:** O pagamento será efetuado em até 30 dias do aceite da nota fiscal. A detentora da Ata deverá apresentar a Certidão Conjunta de Débitos Relativos a Tributos Federais e à Dívida Ativa da União, abrangendo contribuições sociais, nos termos da Portaria MF nº 358, de 05 de setembro de 2014 e a Certidão de Regularidade Fiscal – CRF do FGTS juntamente com a nota fiscal, para fins de comprovação das condições de habilitação conforme previsto no artigo 92, XVI da Lei Federal nº 14.133/2021.

VALIDADE DA PROPOSTA - 90 DIAS, a contar da data da abertura das propostas virtuais.

(Local) _____, _____ de _____ de 2025.

(Assinatura do interessado)

RESPONSÁVEL PELA ASSINATURA DO CONTRATO:
NOME _____
CARGO _____
RG Nº_____
CPF Nº_____
ENDEREÇO RESIDENCIAL_____