



EDITAL

MODALIDADE DE LICITAÇÃO: PREGÃO ELETRÔNICO Nº 52/2026

PROCESSO ADMINISTRATIVO Nº 8144/2026

CRITÉRIO DE JULGAMENTO: MENOR PREÇO TOTAL GLOBAL

MODO DE DISPUTA: ABERTO

LICITAÇÃO: AMPLA PARTICIPAÇÃO

DATA E HORA DA ABERTURA DA SESSÃO PÚBLICA: 13/07/2026, às 9H00

ENDEREÇO ELETRÔNICO: <https://pmstabarbara.smarapd.com.br/pregao/>

Torna-se público que o Município de Santa Bárbara d'Oeste, por meio do Setor de licitações, sediado na Avenida Monte Castelo, nº 1.000, 4º andar- Jd. Primavera, Santa Bárbara d'Oeste, realizará licitação, na modalidade PREGÃO, na forma ELETRÔNICA, nos termos da Lei nº 14.133, de 1º de abril de 2021 e demais legislação aplicável e, ainda, de acordo com as condições estabelecidas neste Edital. A Agente de Contratação Sueli Sousa dos Santos, nomeada pela Portaria nº 226 de 21 de dezembro de 2023, será designada para a condução do certame, auxiliada pela equipe de apoio.

1 DO OBJETO

1.1. O objeto da presente licitação é a contratação de empresa para prestação de serviços de fornecimento de solução de segurança da informação, englobando licenças de uso Endpoint Protection (antivírus), solução de detecção e resposta de endpoint (EDR), instalação, migração, manutenção, treinamento e suporte técnico, conforme condições e exigências estabelecidas neste Edital e seus anexos.

1.2. A licitação será realizada conforme constante no Termo de Referência.

2 DA PARTICIPAÇÃO NA LICITAÇÃO



Município de Santa Bárbara d'Oeste

2.1 Poderão participar deste Pregão os interessados que estiverem previamente credenciados no Sistema Eletrônico de Compras adotado pelo Município.

2.2 O licitante responsabiliza-se exclusiva e formalmente pelas transações efetuadas em seu nome, assume como firmes e verdadeiras suas propostas e seus lances, inclusive os atos praticados diretamente ou por seu representante, excluída a responsabilidade do provedor do sistema ou do órgão ou entidade promotora da licitação por eventuais danos decorrentes de uso indevido das credenciais de acesso, ainda que por terceiros.

2.3 É de responsabilidade do cadastrado conferir a exatidão dos seus dados cadastrais no Sistema relacionado no item anterior e mantê-los atualizados junto ao Município, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados.

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

2.5 A participação da referida licitação se dará por meio de ampla participação, nos termos do art. 49 da Lei Complementar nº 123, de 14 de dezembro de 2006.

2.6 Será concedido tratamento favorecido para as empresas que se enquadram nos limites previstos da Lei Complementar nº 123, de 2006 e do Decreto n.º 8.538, de 2015.

2.7 Não poderão disputar esta licitação:

2.7.1 aquele que não atenda às condições deste Edital e seu(s) anexo(s);

2.7.2 pessoa física ou jurídica que se encontre, ao tempo da licitação, impossibilitada de participar da licitação em decorrência de sanção que lhe foi imposta;

2.7.3 aquele que mantenha 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 licitação ou atue na fiscalização ou na gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau;

2.7.4 empresas controladoras, controladas ou coligadas, nos termos da Lei nº 6.404, de 15 de dezembro de 1976, concorrendo entre si;



2.7.5 pessoa física ou jurídica que, nos 5 (cinco) anos anteriores à divulgação do edital, tenha sido condenada judicialmente, com trânsito em julgado, por exploração de trabalho infantil, por submissão de trabalhadores a condições análogas às de escravo ou por contratação de adolescentes nos casos vedados pela legislação trabalhista;

2.7.6 agente público da Administração;

2.7.7 Organizações da Sociedade Civil de Interesse Público - OSCIP, atuando nessa condição;

2.7.8 Não poderá participar, direta ou indiretamente, da licitação ou da execução do contrato agente público da Administração, devendo ser observadas as situações que possam configurar conflito de interesses no exercício ou após o exercício do cargo ou emprego, nos termos da legislação que disciplina a matéria, conforme § 1º do art. 9º da Lei nº 14.133, de 2021.

2.8 O impedimento de que trata o item 2.7.2 será também aplicado ao licitante que atue em substituição a outra pessoa, física ou jurídica, com o intuito de burlar a efetividade da sanção a ela aplicada, inclusive a sua controladora, controlada ou coligada, desde que devidamente comprovado o ilícito ou a utilização fraudulenta da personalidade jurídica do licitante.

2.9 Não poderão participar desta licitação, associações sem fins lucrativos de qualquer espécie, nos termos do contido em sentença judicial expedida nos autos do processo nº 1002824-77.2014.8.26.0533 – 2ª Vara Cível de Santa Bárbara d'Oeste.

3 DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

3.1 Na presente licitação, a fase de habilitação sucederá as fases de apresentação de propostas e lances e de julgamento.

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

3.3 No cadastramento da proposta inicial, o licitante declarará, em campo próprio do sistema, que:



3.3.1 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;

3.3.2 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 artigo 7º, XXXIII, da Constituição;

3.3.3 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;

3.3.4 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.

3.4 O fornecedor enquadrado como microempresa, empresa de pequeno porte deverá declarar, ainda, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no artigo 3º da Lei Complementar nº 123, de 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 n.º 14.133, de 2021.

3.5 A falsidade da declaração de que trata os itens 3.4 ou 3.5 sujeitará o licitante às sanções previstas na Lei nº 14.133, de 2021, e neste Edital.

3.6 Os licitantes poderão retirar ou substituir a proposta até a abertura da sessão pública.

3.7 Não haverá ordem de classificação na etapa de apresentação da proposta e dos documentos de habilitação pelo licitante, 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 Desde que disponibilizada a funcionalidade no sistema, o licitante poderá parametrizar o seu valor final mínimo 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 parametrizado no sistema poderá ser alterado pelo fornecedor durante a fase de disputa, sendo vedado:

3.10.1 valor superior a lance já registrado pelo fornecedor no sistema, quando adotado o critério de julgamento por menor preço; e

3.11 Caberá ao licitante interessado em participar da licitação acompanhar as operações no sistema eletrônico durante o processo licitatório e se responsabilizar pelo ônus decorrente da perda de negócios diante da inobservância de mensagens emitidas pela Administração ou de sua desconexão.

3.12 O licitante deverá comunicar imediatamente ao provedor do sistema qualquer acontecimento que possa comprometer o sigilo ou a segurança, para imediato bloqueio de acesso.

4 EXIGÊNCIAS DE HABILITAÇÃO

Para fins de habilitação, deverá o licitante comprovar os seguintes requisitos:

Habilitação jurídica

4.1 Pessoa física: cédula de identidade (RG) ou documento equivalente que, por força de lei, tenha validade para fins de identificação em todo o território nacional;

4.2 Empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

4.3 Microempreendedor Individual - MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio <https://www.gov.br/empresas-e-negocios/pt-br/empreendedor>;



4.4 Sociedade empresária, sociedade limitada unipessoal – SLU ou sociedade identificada como empresa individual de responsabilidade limitada - EIRELI: inscrição do ato constitutivo, estatuto ou contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhada de documento comprobatório de seus administradores;

4.5 Sociedade empresária estrangeira: portaria de autorização de funcionamento no Brasil, publicada no Diário Oficial da União e arquivada na Junta Comercial da unidade federativa onde se localizar a filial, agência, sucursal ou estabelecimento, a qual será considerada como sua sede, conforme Instrução Normativa DREI/ME n.º 77, de 18 de março de 2020.

4.6 Sociedade simples: inscrição do ato constitutivo no Registro Civil de Pessoas Jurídicas do local de sua sede, acompanhada de documento comprobatório de seus administradores;

4.7 Decreto de autorização, em se tratando de empresa ou sociedade estrangeira em funcionamento no País, e ato de registro ou autorização para funcionamento expedidos pelo órgão competente, quando a atividade assim o exigir.

4.8 Os documentos apresentados deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

Habilitação fiscal, social e trabalhista

4.9 Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso;

4.10 Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02 de outubro de 2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.

4.11 Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

4.12 Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa ou positiva com efeito



de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto- Lei Federal nº 5.452, de 1º de maio de 1943;

4.13 Prova de inscrição no cadastro de contribuintes Estadual e/ou Municipal relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

4.14 Prova de regularidade com a Fazenda Municipal do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre;

4.15 O fornecedor enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar n. 123, de 2006, estará dispensado da prova de inscrição nos cadastros de contribuintes estadual e municipal.

Qualificação Econômico-Financeira

4.16 Certidão negativa de insolvência civil expedida pelo distribuidor do domicílio ou sede do licitante, caso se trate de pessoa física, desde que admitida a sua participação na licitação (art. 5º, inciso II, alínea “c”, da Instrução Normativa Seges/ME nº 116, de 2021), ou de sociedade simples.

4.17 Certidão negativa de falência expedida pelo distribuidor da sede ou domicílio do fornecedor - Lei Federal nº 14.133, de 2021, art. 69, caput, inciso II);

Qualificação Técnica

4.18 Comprovação de aptidão para execução de serviço similar, de complexidade tecnológica e operacional equivalente ou superior à do objeto desta contratação, ou do item pertinente, por meio da apresentação de certidões ou atestados emitidos por pessoas jurídicas de direito público ou privado, ou pelo conselho profissional competente, quando for o caso.

4.18.1 Para fins da comprovação de que trata este subitem, os atestados deverão dizer respeito a contrato(s) executado(s) com 50% (cinquenta por cento) do item 01, ou seja, fornecimento de 750 licenças de proteção antivírus Endpoint Protection e EDR pelo período de 02 anos.

4.18.2 Serão admitidos, para fins de comprovação de quantitativo mínimo de serviço, a apresentação e o somatório de diferentes atestados de serviços executados de forma concomitante.



Outras Comprovações

4.19 O licitante deverá apresentar declaração de comprovação que no site do fabricante tem canal autorizado a fornecer e instalar os produtos da marca.

5 DO PREENCHIMENTO DA PROPOSTA

5.1 O licitante deverá enviar sua proposta mediante o preenchimento, no sistema eletrônico, dos seguintes campos:

5.1.1 Valor unitário e total global;

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

5.2.1 O licitante não poderá oferecer proposta em quantitativo inferior ao previsto para contratação.

5.3 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.

5.4 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.

5.5 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.

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

5.7 Os licitantes deverão deter ciência plena e, se vencedores do presente certame, cumprir, com rigor, os termos do Decreto Municipal nº 7.468/2023 e Anexo Único (Anexo VIII), sob pena de não pagamento dos valores devidos, inclusive.

5.8 Na presente licitação, a Microempresa e a Empresa de Pequeno Porte poderão se beneficiar do regime de tributação pelo Simples Nacional.

5.9 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.

5.9.1 O prazo de validade da proposta não será inferior a 60 (sessenta) dias, a contar da data de sua apresentação.

5.9.2 Os licitantes devem respeitar os preços máximos estabelecidos nas normas de regência de contratações públicas, quando participarem de licitações públicas;

5.10 O descumprimento das regras supramencionadas pela Administração por parte dos Contratados pode ensejar a responsabilização pelo Tribunal de Contas do Estado de São Paulo e, após o devido processo legal, gerar as seguintes consequências: assinatura de prazo para a adoção das medidas necessárias ao exato cumprimento da lei, nos termos do art. 71, inciso IX, da Constituição; ou condenação dos agentes públicos responsáveis e da empresa contratada ao pagamento dos prejuízos ao erário, caso verificada a ocorrência de superfaturamento por sobrepreço na execução do contrato.

6 DA ABERTURA DA SESSÃO, CLASSIFICAÇÃO DAS PROPOSTAS E FORMULAÇÃO DE LANCES

6.1 A abertura da presente licitação dar-se-á automaticamente em sessão pública, por meio de sistema eletrônico, na data, horário e local indicados neste Edital.

6.2 O sistema disponibilizará campo próprio para troca de mensagens entre o Agente de Contratação e os licitantes.

6.3 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.

6.4 O lance deverá ser ofertado conforme critério de julgamento.

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

6.6 O procedimento seguirá de acordo com o modo de disputa adotado.

6.7 O envio de lances no pregão eletrônico, no modo de disputa “aberto”, os licitantes apresentarão lances públicos e sucessivos, com prorrogações.



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

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

6.7.3 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.

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

6.9 Não serão aceitos dois ou mais lances de mesmo valor, prevalecendo aquele que for recebido e registrado em primeiro lugar no sistema eletrônico.

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

6.11 No caso de desconexão com o Agente de Contratação, no decorrer da etapa competitiva do Pregão, o sistema eletrônico poderá permanecer acessível aos licitantes para a recepção dos lances.

6.12 Quando a desconexão do sistema eletrônico para o Agente de Contratação persistir por tempo superior a dez minutos, a sessão pública será suspensa e reiniciada somente após decorridas vinte e quatro horas da comunicação do fato pelo Agente de Contratação aos participantes, no sítio eletrônico utilizado para divulgação.

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

6.14 Em relação a itens não exclusivos para participação de microempresas e empresas de pequeno porte, uma vez encerrada a etapa de lances, será efetivada a verificação automática, junto à Receita Federal, do porte da entidade empresarial. O sistema identificará em coluna própria 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, de 2006.

6.14.1 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.

6.14.2 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 eletrônico, contados após a comunicação automática para tanto.

6.14.3 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.

6.14.4 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.

6.16 Havendo eventual empate entre propostas ou lances, o critério de desempate será aquele previsto no art. 60 da Lei nº 14.133, de 2021, nesta ordem:

6.16.1 disputa final, hipótese em que os licitantes empatados poderão apresentar nova proposta em ato contínuo à classificação;

6.16.2 avaliação do desempenho contratual prévio dos licitantes, para a qual deverão preferencialmente ser utilizados registros cadastrais para efeito de atesto de cumprimento de obrigações previstos nesta Lei;

6.16.3 desenvolvimento pelo licitante de ações de equidade entre homens e mulheres no ambiente de trabalho, conforme Decreto Federal nº 11.430, de 2023, § 1º, incisos I a VI, com a eventual apresentação do chamado Selo Empresa Amiga da Mulher, conforme Lei Federal 14.682 de 2023;

6.16.4 desenvolvimento pelo licitante de programa de integridade, conforme orientações dos órgãos de controle.



6.17 Persistindo o empate, será assegurada preferência, sucessivamente, aos bens e serviços produzidos ou prestados por:

6.17.1 empresas estabelecidas no território do Estado ou do Distrito Federal do órgão ou entidade da Administração Pública estadual ou distrital licitante ou, no caso de licitação realizada por órgão ou entidade de Município, no território do Estado em que este se localize;

6.17.1.1 empresas brasileiras;

6.17.1.2 empresas que invistam em pesquisa e no desenvolvimento de tecnologia no País;

6.17.1.3 empresas que comprovem a prática de mitigação, nos termos da Lei nº 12.187, de 29 de dezembro de 2009.

6.18 As regras previstas acima não prejudicarão a aplicação do disposto no artigo 44 da Lei Complementar 123, de 14 de dezembro de 2006.

6.19 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 Agente de Contratação poderá negociar condições mais vantajosas, após definido o resultado do julgamento.

6.19.1 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.

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

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

6.19.4 O Agente de Contratação solicitará ao licitante mais bem classificado que, no prazo de 2 (duas) horas, envie a proposta adequada ao último lance ofertado após a negociação realizada, acompanhada, se for o caso, dos documentos complementares, como por exemplo: fichas, catálogos, laudos, certificações, caso solicitado em Edital.

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



6.20 Após a negociação do preço, o Agente de Contratação iniciará a fase de aceitação e julgamento da proposta.

7 DA FASE DE JULGAMENTO

7.1 Encerrada a etapa de negociação, o Agente de Contratação 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 2.7 do Edital, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

7.1.1 Cadastro Nacional de Empresas Inidôneas e Suspensas - CEIS, mantido pela Controladoria-Geral da União (<https://www.portaltransparencia.gov.br/sancoes/ceis>); e

7.1.2 Cadastro Nacional de Empresas Punidas – CNEP, mantido pela Controladoria-Geral da União (<https://www.portaltransparencia.gov.br/sancoes/cnep>).

7.2 A consulta aos cadastros será realizada em nome da empresa licitante e também de seu sócio majoritário, por força da vedação de que trata o artigo 12 da Lei nº 8.429, de 1992.

7.3 Caso conste na Consulta de Situação do licitante a existência de Ocorrências Impeditivas Indiretas, o Agente de Contratação diligenciará para verificar se houve fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas.

7.3.1 A tentativa de burla será verificada por meio dos vínculos societários, linhas de fornecimento similares, dentre outros.

7.3.2 O licitante será convocado para manifestação previamente a uma eventual desclassificação.

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

7.4 Caso o licitante provisoriamente classificado em primeiro lugar tenha se utilizado de algum tratamento favorecido às ME/EPPs, o Agente de Contratação verificará se faz jus ao benefício, em conformidade com o item 3.4 deste Edital.

7.5 Verificadas as condições de participação e de utilização do tratamento favorecido, o Agente de Contratação 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.

7.6 Será desclassificada a proposta vencedora que:

7.6.1 conter vícios insanáveis;

7.6.2 não obedecer às especificações técnicas contidas no Termo de Referência;

7.6.3 apresentar desconformidade com quaisquer outras exigências deste Edital ou seus anexos, desde que insanável.

7.7 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.

7.8 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;

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

7.8.2 Considera-se erro no preenchimento da planilha passível de correção a indicação de recolhimento de impostos e contribuições na forma do Simples Nacional, quando não cabível esse regime.

7.9 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.

8 DA FASE DE HABILITAÇÃO

8.1 Os documentos previstos no item 04, necessários e suficientes para demonstrar a capacidade do licitante de realizar o objeto da licitação, serão exigidos para fins de habilitação, nos termos dos arts. 62 a 70 da Lei nº 14.133, de 2021.

8.2 Quando permitida a participação de empresas estrangeiras que não funcionem no País, as exigências de habilitação serão atendidas mediante documentos equivalentes, inicialmente apresentados em tradução livre.



8.3 Na hipótese de o licitante vencedor ser empresa estrangeira que não funcione no País, para fins de assinatura do contrato, os documentos exigidos para a habilitação serão traduzidos por tradutor juramentado no País e apostilados ou consularizados pelos respectivos consulados ou embaixadas.

8.4 Os documentos exigidos para fins de habilitação poderão ser apresentados em original ou por cópia.

8.5 Será verificado se o licitante apresentou declaração de que atende aos requisitos de habilitação, e o declarante responderá pela veracidade das informações prestadas, na forma da lei (art. 63, I, da Lei nº 14.133/2021).

8.6 A habilitação será verificada por meio do sistema eletrônico de compras, nos documentos por ele abrangidos.

8.6.1 Somente haverá a necessidade de comprovação do preenchimento de requisitos mediante apresentação dos documentos originais não-digitais quando houver dúvida em relação à integridade do documento digital ou quando a lei expressamente o exigir.

8.7 É de responsabilidade do licitante conferir a exatidão dos seus dados cadastrais no sistema eletrônico de compras e mantê-los atualizados, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados.

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

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

8.8.1 Os documentos exigidos para habilitação serão enviados por meio do sistema, em formato digital, no prazo de no mínimo, duas horas, prorrogável por igual período, contado da solicitação do Agente de Contratação.

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

8.9 Após a entrega dos documentos para habilitação, não será permitida a substituição ou a apresentação de novos documentos, salvo em sede de diligência, conforme disposto na Lei 14.133/21, art. 64.



8.9.1 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

8.9.2 atualização de documentos cuja validade tenha expirado após a data de recebimento das propostas;

8.10 Na análise dos documentos de habilitação, a comissão de contratação 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.

8.11 Na hipótese de o licitante não atender às exigências para habilitação, o Agente de Contratação examinará a proposta subsequente e assim sucessivamente, na ordem de classificação, até a apuração de uma proposta que atenda ao presente Edital.

8.12 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 item anterior.

9 DA CONTRATAÇÃO

9.1 Homologado o resultado da licitação, o licitante mais bem classificado terá o prazo de 05 (cinco) dias úteis, contados a partir da data de sua convocação, para assinar o contrato, cujo prazo de validade encontra-se nela fixado, sob pena de decadência do direito à contratação, sem prejuízo das sanções previstas na Lei nº 14.133, de 2021.

9.2 O prazo de convocação poderá ser prorrogado uma vez, por igual período, mediante solicitação do licitante mais bem classificado ou do fornecedor convocado, desde que:

(a) a solicitação seja devidamente justificada e apresentada dentro do prazo; e

(b) a justificativa apresentada seja aceita pela Administração.

9.3 O contrato será assinado por meio de assinatura digital.

9.4 Na hipótese de o convocado não assinar o contrato no prazo e nas condições estabelecidas, fica facultado à Administração convocar os licitantes



remanescentes, na ordem de classificação, para fazê-lo em igual prazo e nas condições propostas pelo primeiro classificado.

10 DOS RECURSOS

10.1 A interposição de recurso referente ao julgamento das propostas, à habilitação ou inabilitação de licitantes, à anulação ou revogação da licitação, observará o disposto no art. 165 da Lei nº 14.133, de 2021.

10.2 O prazo recursal é de 3 (três) dias úteis, contados da data de intimação ou de lavratura da ata.

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

10.3.1 a intenção de recorrer deverá ser manifestada imediatamente, sob pena de preclusão;

10.3.2 o prazo para a manifestação da intenção de recorrer será de 30 (trinta) minutos.

10.3.3 o prazo para apresentação das razões recursais será iniciado na data de intimação ou de lavratura da ata de habilitação ou inabilitação;

10.4 Os recursos deverão ser encaminhados em campo próprio do sistema.

10.5 O recurso será dirigido à autoridade que tiver editado o ato ou proferido a decisão recorrida, a qual poderá 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.

10.6 Os recursos interpostos fora do prazo não serão conhecidos.

10.7 O prazo para apresentação de contrarrazões ao recurso pelos demais licitantes será de 3 (três) dias úteis, contados da data da intimação pessoal ou da divulgação da interposição do recurso, assegurada a vista imediata dos elementos indispensáveis à defesa de seus interesses.

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

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



10.10 Os autos do processo permanecerão com vista franqueada aos interessados no sítio eletrônico <https://pmstabarbara.smarapd.com.br/pregao/>.

11 DAS INFRAÇÕES ADMINISTRATIVAS E SANÇÕES

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

11.1.1 deixar de entregar a documentação exigida para o certame ou não entregar qualquer documento que tenha sido solicitado pelo/a Agente de Contratação/a durante o certame;

11.1.2 Salvo em decorrência de fato superveniente devidamente justificado, não manter a proposta em especial quando:

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

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

11.1.2.3 pedir para ser desclassificado quando encerrada a etapa competitiva; ou

11.1.2.4 apresentar proposta em desacordo com as especificações do edital;

11.1.3 não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;

11.1.3.1 recusar-se, sem justificativa, a assinar o contrato ou a aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração;

11.1.4 apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação

11.1.5 fraudar a licitação

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

11.1.6.1 agir em conluio ou em desconformidade com a lei;

11.1.6.2 induzir deliberadamente a erro no julgamento;

11.1.7 praticar atos ilícitos com vistas a frustrar os objetivos da licitação

11.1.8 praticar ato lesivo previsto no art. 5º da Lei n.º 12.846, de 2013.



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

11.2.1 advertência;

11.2.2 multa;

11.2.3 impedimento de licitar e contratar e

11.2.4 declaração de inidoneidade para licitar ou contratar, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida sua reabilitação perante a própria autoridade que aplicou a penalidade.

11.3 Na aplicação das sanções serão considerados:

11.3.1 a natureza e a gravidade da infração cometida.

11.3.2 as peculiaridades do caso concreto

11.3.3 as circunstâncias agravantes ou atenuantes

11.3.4 os danos que dela provierem para a Administração Pública

11.3.5 a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

11.4 A multa será recolhida em percentual de 0,5% a 30% incidente sobre o valor do contrato licitado, recolhida no prazo máximo de 30 (trinta) dias úteis, a contar da comunicação oficial.

11.4.1 Para as infrações previstas nos itens 11.1.1, 11.1.2 e 11.1.3, a multa será de 0,5% a 15% do valor do contrato licitado.

11.4.2 Para as infrações previstas nos itens 11.1.4, 11.1.5, 11.1.6, 11.1.7 e 11.1.8, a multa será de 15% a 30% do valor do contrato licitado.

11.5 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.

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

11.7 A sanção de impedimento de licitar e contratar será aplicada ao responsável em decorrência das infrações administrativas relacionadas nos itens 11.1.1, 11.1.2 e 11.1.3, quando não se justificar a imposição de penalidade mais grave, e impedirá o responsável de licitar e contratar no âmbito da Administração



Pública direta e indireta do ente federativo a qual pertencer o órgão ou entidade, pelo prazo máximo de 3 (três) anos.

11.8 Poderá ser aplicada ao responsável a sanção de declaração de inidoneidade para licitar ou contratar, em decorrência da prática das infrações dispostas nos itens 11.1.4, 11.1.5, 11.1.6, 11.1.7 e 11.1.8, bem como pelas infrações administrativas previstas nos itens 11.1.1, 11.1.2 e 11.1.3 que justifiquem a imposição de penalidade mais grave que a sanção de impedimento de licitar e contratar, cuja duração observará o prazo previsto no art. 156, §5º, da Lei n.º 14.133/2021.

11.9 A recusa injustificada do adjudicatário em assinar o contrato ou em aceitar/retirar o instrumento equivalente no prazo estabelecido pela Administração, nos termos do item 11.1.3, caracterizará o descumprimento total da obrigação assumida e o sujeitará às penalidades e à imediata desconsideração total da proposta.

11.10 A apuração de responsabilidade relacionada às sanções de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar demandará a instauração de processo de responsabilização a ser conduzido por comissão composta por 2 (dois) ou mais servidores estáveis, que avaliará fatos e circunstâncias conhecidos e intimará o licitante ou o adjudicatário para, no prazo de 15 (quinze) dias úteis, contado da data de sua intimação, apresentar defesa escrita e especificar as provas que pretenda produzir.

11.11 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.

11.12 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.

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



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

12 DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

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

12.2 A resposta à impugnação ou ao pedido de esclarecimento será divulgado em sítio eletrônico oficial no prazo de até 3 (três) dias úteis, limitado ao último dia útil anterior à data da abertura do certame.

12.3 A impugnação e o pedido de esclarecimento deverão ser realizados por forma eletrônica, protocolizadas junto ao sítio www.santabarbara.sp.gov.br no link <https://santabarbara.1doc.com.br/b.php?pg=wp/wp&itd=5>, ou diretamente na plataforma SMARAPD <https://pmstabarbara.smarapd.com.br/pregao/>

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

12.4.1 A concessão de efeito suspensivo à impugnação é medida excepcional e deverá ser motivada pelo agente de contratação, nos autos do processo de licitação.

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

13 DAS DISPOSIÇÕES GERAIS

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

13.2 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.

13.3 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.



Município de Santa Bárbara d'Oeste

13.4 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.

13.5 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.

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

13.7 O Edital e seus anexos estão disponíveis, na íntegra, no Portal Nacional de Contratações Públicas (PNCP) e endereço eletrônico www.santabarbara.sp.gov.br.

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

13.8.1 ANEXO I - Termo de Referência

13.8.1.1 Apêndice do Anexo I – Estudo Técnico Preliminar

13.8.2 ANEXO II- Planilha Proposta

13.8.3 ANEXO III- Minuta Termo de Contrato

13.8.4 ANEXO IV – Termo de Ciência e Notificação

13.8.5 ANEXO V – Modelo de Declaração de Fatos Impeditivos

13.8.6 ANEXO VI- Cadastro de Representante

13.8.7 ANEXO VII- LC-02- Declaração de Documentos à Disposição do TCE – SP

13.8.8 ANEXO VIII- Decreto Municipal nº 7.468 de 25 de agosto de 2.023

Santa Bárbara d'Oeste, 24 de junho de 2026.

MONICA MOSNA
Secretária Municipal de Administração



ANEXO I- TERMO DE REFERÊNCIA

1. DAS CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. Contratação de empresa para prestação de serviços de fornecimento de solução de segurança da informação, englobando licenças de uso Endpoint Protection (antivírus), solução de detecção e resposta de endpoint (EDR), instalação, migração, manutenção, treinamento e suporte técnico neste instrumento.

ITEM	CÓDIGO	DESCRIÇÃO	UNIDADE DE MEDIDA	QTDE
1	2.01.02.0069.6	Licença proteção antivírus Endpoint Protection e EDR	Unidade x anual	3.000 (1.500 x 2 anos)
2	2.01.02.0076.9	Migração e implantação da proteção antivírus (Endpoint Protection)	Unidade	01
3	2.01.02.0077.7	Treinamento proteção antivírus Endpoint Protection	Unidade	01
4	2.01.02.0078.5	Suporte técnico em proteção antivírus Endpoint Protection	Anual	02

1.2. O objeto possui natureza de **serviço comum de tecnologia da informação**, pois seus padrões de desempenho e qualidade podem ser definidos objetivamente por especificações usuais de mercado.

1.3. O serviço é enquadrado como **continuado**, tendo em vista que a proteção dos ativos tecnológicos e o suporte são necessidades permanentes da Administração

1.4. O prazo de vigência da contratação será de **24 (vinte e quatro) meses**, contados a partir da data de sua assinatura, podendo ser prorrogado na forma dos arts. 106 e 107 da Lei Federal nº 14.133/2021, desde que demonstrada a vantajosidade e observados os requisitos legais aplicáveis.

1.5. O contrato oferece maior detalhamento das regras que serão aplicadas em relação à vigência da contratação.



2. DA FUNDAMENTAÇÃO E DA DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

2.1. A fundamentação da contratação encontra-se pormenorizada em tópico específico dos Estudos Técnicos Preliminares, apêndice deste Termo de Referência.

2.2. A crescente digitalização dos processos administrativos e a ampliação do uso de sistemas informatizados na Administração Pública Municipal tornam indispensável a adoção de mecanismos robustos de segurança da informação, capazes de proteger os ativos tecnológicos e os dados institucionais contra ameaças cibernéticas cada vez mais sofisticadas.

2.3. Atualmente, os ambientes computacionais utilizados pela municipalidade - compostos por estações de trabalho, notebooks e servidores - armazenam e processam grande volume de informações institucionais, dados pessoais de cidadãos e informações estratégicas para a gestão pública. Nesse contexto, a inexistência ou insuficiência de soluções modernas de proteção pode expor a infraestrutura tecnológica a riscos relevantes, tais como infecções por malwares, ataques de ransomware, exploração de vulnerabilidades, indisponibilidade de serviços públicos digitais e comprometimento da integridade, confidencialidade e disponibilidade das informações.

2.4. Diante desse cenário, torna-se necessária a contratação de solução integrada de segurança de endpoints, contemplando ferramentas avançadas de Endpoint Protection (antivírus) e Detecção e Resposta de Endpoint (EDR), permitindo a identificação preventiva de falhas de segurança, o monitoramento contínuo do ambiente computacional e a resposta rápida a incidentes.

2.5. A solução pretendida permitirá a proteção de aproximadamente 1.500 equipamentos (estações de trabalho, notebooks e servidores), abrangendo os ambientes operacionais utilizados pela municipalidade, bem como a implementação de console centralizado de gerenciamento, possibilitando maior controle, visibilidade e eficiência na administração das políticas de segurança.



2.6. Além disso, a contratação prevê instalação, migração, manutenção, treinamento e suporte técnico especializado, com monitoramento contínuo 24 horas por dia, 7 dias por semana (24x7), por meio de NOC físico localizado no Brasil, assegurando maior agilidade na detecção e tratamento de incidentes de segurança, bem como maior confiabilidade operacional da solução.

2.7. A adoção de ferramentas especializadas de segurança cibernética alinha-se às boas práticas de governança de tecnologia da informação e segurança da informação, contribuindo para a proteção dos ativos tecnológicos municipais, para a continuidade dos serviços públicos digitais e para a mitigação de riscos associados a incidentes cibernéticos.

2.8. Assim, a contratação da solução proposta mostra-se tecnicamente necessária e estrategicamente adequada, visando fortalecer a postura de segurança da informação da Administração Municipal, garantindo maior proteção à infraestrutura tecnológica e aos dados sob sua responsabilidade, bem como assegurando a continuidade e a confiabilidade dos serviços públicos prestados à população.

3. DA DESCRIÇÃO DA SOLUÇÃO COMO UM TODO.

3.1. A solução como um todo consiste no fornecimento integrado de licenças de segurança para endpoints, funcionalidades de EDR, console de gerenciamento centralizado, instalação, migração da solução atual, atualização contínua, suporte técnico, treinamento dos servidores responsáveis pela administração da ferramenta, garantia e acompanhamento durante toda a vigência contratual.

3.2. O ciclo de vida do objeto compreenderá, no mínimo: planejamento; apresentação e aprovação do plano de migração; implantação; instalação; configuração; migração do ambiente existente; ativação das licenças; disponibilização do console de gerenciamento; treinamento; operação assistida; manutenção preventiva, corretiva, adaptativa e evolutiva; suporte técnico;



atualização de versões, assinaturas e bases de vulnerabilidades; monitoramento de incidentes; e encerramento contratual com transição segura, se aplicável.

3.3. A solução deverá proteger os endpoints da infraestrutura municipal, incluindo estações de trabalho, notebooks e servidores, contra vírus, malwares, ransomwares, ameaças persistentes, exploração de vulnerabilidades e demais códigos ou comportamentos maliciosos.

3.4. A solução deverá permitir a gestão centralizada das políticas de segurança, a identificação, análise e gerenciamento de vulnerabilidades, a detecção e resposta a incidentes, a emissão de relatórios, a rastreabilidade das ações administrativas e a atualização permanente dos mecanismos de proteção.

3.5. A prestação dos serviços deverá ocorrer com suporte técnico integral, com monitoramento 24x7 por NOC físico no Brasil, assegurando maior agilidade na detecção e no tratamento de incidentes de segurança e maior confiabilidade operacional.

3.6. Ao final da vigência, caso não haja prorrogação, O Contratado deverá colaborar com a transição para eventual nova solução ou encerramento ordenado da execução, resguardando a continuidade dos serviços, a integridade das informações e a segurança do ambiente municipal.

4. DOS REQUISITOS DA CONTRATAÇÃO

4.1. A presente contratação deverá atender aos requisitos de negócio, legais, técnicos, de capacitação, segurança, privacidade, manutenção, suporte, garantia, sustentabilidade e comprovação técnica descritos neste item.

4.2. Proteger os endpoints da infraestrutura municipal, incluindo estações de trabalho, notebooks e servidores, contra ameaças cibernéticas como vírus, malwares, ransomwares e demais códigos maliciosos;

4.3. Detectar e responder rapidamente a incidentes de segurança, por meio da utilização de solução de Detecção e Resposta de Endpoint (EDR), permitindo a



identificação, análise e mitigação de comportamentos suspeitos ou atividades maliciosas no ambiente computacional;

4.4. Identificar, analisar e gerenciar vulnerabilidades existentes nos sistemas operacionais e softwares instalados nas estações e servidores, reduzindo riscos de exploração por agentes maliciosos;

4.5. Centralizar a gestão das políticas de segurança, possibilitando o gerenciamento unificado das soluções implantadas por meio de console administrativo única, proporcionando maior controle e eficiência operacional;

4.6. Garantir a atualização contínua das soluções de segurança, incluindo assinaturas de antivírus, mecanismos de detecção e bases de vulnerabilidades, assegurando proteção atualizada contra novas ameaças;

4.7. Proporcionar monitoramento contínuo do ambiente computacional, com suporte técnico especializado e acompanhamento permanente da solução, visando maior rapidez na identificação e tratamento de incidentes;

4.8. Assegurar a continuidade e a confiabilidade dos serviços públicos digitais, por meio da proteção adequada dos ativos tecnológicos e das informações institucionais da Administração Municipal;

4.9. O processo deverá observar a Lei Federal nº 14.133/2021, a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), as normas municipais aplicáveis e as políticas internas de segurança da informação e de tecnologia da informação.

4.10. A solução deverá atender aos princípios de confidencialidade, integridade, disponibilidade, autenticidade, rastreabilidade e proteção de dados, inclusive quanto a controles de acesso, registros de auditoria, logs, relatórios, comunicação de incidentes e uso restrito das informações acessadas pelo Contratado.



4.11. Os serviços deverão ser prestados por técnicos devidamente capacitados na solução ofertada, com todos os recursos, ferramentas e meios necessários à instalação, implantação, suporte e manutenção.

4.12. O Contratado deverá observar boas práticas de sustentabilidade, priorizando documentação digital, execução remota quando tecnicamente possível, redução de deslocamentos desnecessários e descarte ambientalmente adequado de eventuais materiais utilizados na execução.

4.13. Requisitos técnicos mínimos da solução:

4.13.1. Especificações Do Objeto

4.13.1.1. A contratação compreende o fornecimento de solução integrada de segurança da informação para proteção de endpoints da infraestrutura tecnológica do Município, contemplando licenciamento de softwares especializados, implantação da solução, migração do ambiente existente, treinamento e suporte técnico especializado, conforme as especificações a seguir.

4.13.2. Do módulo de proteção de endpoint

4.13.2.1. A solução proposta deverá proteger os sistemas operacionais abaixo:

4.13.2.1.1. Windows 7, Windows 8, Windows 8.1, Windows 10, Windows 11 e superior; Windows Server 2008 R2, 2012 R2, 2016, 2019, 2022 e superior;

4.13.2.1.2. Debian GNU/Linux: Versões 11.x e 12.x, Ubuntu Server/Desktop: Versões 20.04 e 22.04, CentOS / CentOS Stream: Versões 7.x, 8.x e 9.x

4.13.2.2. A solução proposta deverá suportar as seguintes plataformas virtuais:

4.13.2.2.1. VMware Workstation 17.0.2 Pro;

4.13.2.2.2. VMware a partir de ESXi 6.7 em diante;

4.13.2.2.3. Microsoft Hyper-V a partir da versão 2012 em diante;



4.13.3. Do módulo de gerenciamento

4.13.3.1. A solução deverá:

4.13.3.1.1. Suportar arquitetura cloud-native e on-premise;

4.13.3.1.2. Fornecer a capacidade de integração com as soluções Managed Endpoint Detection and Response (MDR) e Anti-APT do próprio fornecedor, para caça ativa a ameaças e resposta automatizada a incidentes;

4.13.3.1.3. Ter a capacidade de permitir aplicações baseadas em seus certificados de assinatura digital, MD5, SHA256, metadados, caminho do arquivo e categorias de segurança pré-definidas;

4.13.3.1.4. Suportar Single Sign On (SSO) usando NTLM e Kerberos;

4.13.3.1.5. O administrador deve ser capaz de adicionar manualmente novos dispositivos à lista de equipamentos ou editar informações sobre equipamentos já existentes na rede;

4.13.3.1.6. Incluir uma ferramenta integrada para realizar diagnósticos remotos e coletar logs de solução de problemas sem exigir acesso físico ao computador;

4.13.3.1.7. Incorporar no sensor de endpoint distribuição/retransmissão para transferir ou fazer proxy de solicitações de reputação de ameaças dos terminais para o servidor de gerenciamento;

4.13.3.1.8. Suportar o download de arquivos diferenciais em vez de pacotes completos de atualização;

4.13.3.1.9. Incluir Role Based Access Control (RBAC) com funções predefinidas personalizáveis;

4.13.3.1.10. O servidor de gerenciamento primário deve ser capaz de retransmitir atualizações e serviços de reputação em nuvem.

4.13.3.2. O servidor de gerenciamento deve ter funcionalidade para criar múltiplos perfis dentro de uma política de proteção com diferentes configurações



de proteção que possam estar simultaneamente ativas em uns único/múltiplos dispositivos com base nas seguintes regras de ativação:

4.13.3.2.1. Status do dispositivo;

4.13.3.2.2. Tag;

4.13.3.2.3. Diretório ativo;

4.13.3.2.4. Proprietários de dispositivos;

4.13.3.2.5. Hardware;

4.13.3.3. Suportar os seguintes canais de entrega de notificação: E-mail e Registro de sistema.

4.13.3.4. Ter a capacidade de etiquetar/marcar computadores com base em:

4.13.3.4.1. Atributos de rede;

4.13.3.4.2. Nome;

4.13.3.4.3. Domínio e/ou Sufixo de Domínio;

4.13.3.4.4. Endereço de IP;

4.13.3.4.5. Endereço IP para servidor de gerenciamento;

4.13.3.4.6. Localização no Active Directory;

4.13.3.4.7. Unidade organizacional;

4.13.3.4.8. Grupo;

4.13.3.4.9. Sistema operacional;

4.13.3.4.10. Número do pacote de serviço;

4.13.3.4.11. Arquitetura Virtual;

4.13.3.4.12. Registro de aplicativos;

4.13.3.4.13. Nome da Aplicação;

4.13.3.4.14. Versão do aplicativo;

4.13.3.4.15. Fabricante;



4.13.3.4.16. Tipo e versão;

4.13.3.4.17. Arquitetura.

4.13.3.5. Ter a capacidade de criar/definir configurações com base na localização de um computador na rede, e não no grupo ao qual pertence no servidor de gestão.

4.13.3.6. Ter a funcionalidade de adicionar um mediador de conexão unidirecional entre o servidor de gerenciamento e o endpoint conectado pela internet/rede pública.

4.13.3.7. As informações sobre o equipamento deverão ser atualizadas após cada nova pesquisa na rede. A lista de equipamentos detectados deve abranger o seguinte:

4.13.3.7.1. Dispositivos Desktop/Servidores;

4.13.3.7.2. Dispositivos móveis;

4.13.3.7.3. Dispositivos de rede;

4.13.3.7.4. Dispositivos virtuais;

4.13.3.7.5. Componentes OEM;

4.13.3.7.6. Periféricos de computador;

4.13.3.7.7. Dispositivos IoT conectados;

4.13.3.7.8. Telefones VoIP;

4.13.3.8. Permitir ao administrador criar categorias/grupos de aplicação com base em:

4.13.3.8.1. Nome da Aplicação;

4.13.3.8.2. Caminho do aplicativo;

4.13.3.8.3. Metadados do aplicativo;

4.13.3.8.4. Aplicativo Certificado digital;

4.13.3.8.5. Categorias de aplicativos predefinidas pelo fornecedor;



4.13.3.8.6. SHA256 e MD5;

4.13.3.9. A solução proposta deverá permitir especificamente o bloqueio dos seguintes dispositivos:

4.13.3.9.1. Bluetooth;

4.13.3.9.2. Dispositivos móveis;

4.13.3.9.3. Modems externos;

4.13.3.9.4. Cd/Dvd;

4.13.3.9.5. Câmeras e scanners;

4.13.3.9.6. MTPs;

4.13.3.9.7. Transferência de dados para dispositivos móveis.

4.13.3.10. Ter capacidade de ler informações do Active Directory para obter dados sobre contas de computadores na organização.

4.13.3.11. Ter funcionalidade integrada para conectar-se remotamente ao endpoint usando a tecnologia Windows Desktop Sharing. Além disso, a solução deve ser capaz de manter a auditoria das ações do administrador durante a sessão.

4.13.3.12. A solução proposta deverá possuir a funcionalidade de criar uma estrutura de grupos de administração utilizando a hierarquia de Grupos, com base nos seguintes dados:

4.13.3.12.1. Estruturas de domínios e grupos de trabalho do Windows;

4.13.3.12.2. Estruturas de grupos do Active Directory;

4.13.3.12.3. Conteúdo de um arquivo de texto criado manualmente pelo administrador;

4.13.3.13. Ser capaz de recuperar informações sobre os equipamentos detectados durante uma pesquisa na rede. O inventário resultante deverá abranger todos os equipamentos conectados à rede da organização.



- 4.13.3.14. Permitir realizar as seguintes ações para endpoints:
 - 4.13.3.14.1. Verificação manual;
 - 4.13.3.14.2. Verificação no acesso;
 - 4.13.3.14.3. Verificação por demanda;
 - 4.13.3.14.4. Verificação de arquivos compactados
 - 4.13.3.14.5. Verificação de arquivos individuais, pastas e unidades;
 - 4.13.3.14.6. Bloqueio e verificação de scripts
 - 4.13.3.14.7. Proteção contra alteração de registros;
 - 4.13.3.14.8. Proteção contra estouro de buffer;
 - 4.13.3.14.9. Verificação em segundo plano/inativa
- 4.13.3.15. suportar a instalação do sensor de endpoint juntamente com soluções de terceiros, seja utilizando somente o módulo de EDR ou anti-malware.
- 4.13.3.16. O servidor de gerenciamento deve manter um histórico de revisões das políticas, tarefas, pacotes, grupos de gerenciamento criados, para que modificações em uma determinada política/tarefa possam ser revisadas.
- 4.13.3.17. Ter a capacidade de definir um intervalo de endereços IP, de forma a limitar o tráfego do cliente para o servidor de gestão com base no tempo e na velocidade.
- 4.13.3.18. Ter a capacidade de realizar inventário em scripts e arquivos, tais como: dll, exe, bat e etc.
- 4.13.3.19. Prever a criação de uma cópia de segurança do sistema de administração com o auxílio de ferramentas integradas do sistema de administração.
- 4.13.3.20. Incluir alguma forma de sistema para controlar epidemias de vírus.



4.13.3.21. Incluir Role Based Access Control (RBAC), e isso deve permitir que as restrições sejam replicadas em todos os servidores de gerenciamento na hierarquia.

4.13.3.22. O servidor de gestão da solução proposta deverá incluir funções de segurança pré-definidas para o Admin da Solução.

4.13.3.23. Permitir ao administrador criar um túnel de conexão entre um dispositivo cliente remoto e o servidor de gerenciamento caso a porta usada para conexão ao servidor de gerenciamento não esteja disponível no dispositivo.

4.13.3.24. Ser capaz de registrar operações de arquivos (Escrita e Exclusão) em dispositivos de armazenamento USB.

4.13.3.25. Ter capacidade de bloquear a execução de qualquer executável do dispositivo de armazenamento USB.

4.13.3.26. Contar com filtragem de firewall por endereço local, interface física e Time-To-Live (TTL) de pacotes.

4.13.3.27. Ter a capacidade de restringir as atividades do aplicativo dentro do sistema de acordo com o nível de confiança atribuído ao aplicativo e de limitar os direitos dos aplicativos de acessar determinados recursos, incluindo arquivos do sistema e do usuário utilizando de módulo específico de prevenção de intrusão.

4.13.3.28. Ter a capacidade de excluir automaticamente as regras de controle de aplicativos se um aplicativo não for iniciado durante um intervalo especificado. O intervalo deve ser configurável.

4.13.3.29. Incluir múltiplas formas de notificar o administrador sobre eventos importantes que ocorreram (notificação por e-mail, anúncio sonoro, janela pop-up, entrada de log).

4.13.3.30. Incluir Controle de inicialização de aplicativos para o sistema operacional Windows Server.



4.13.3.31. Distribuir automaticamente as contas de computador por grupo de gerenciamento caso novos computadores apareçam na rede. Deve fornecer a capacidade de definir as regras de transferência de acordo com o endereço IP, tipo de sistema operacional e localização nas Unidades Organizacionais do Active Directory.

4.13.3.32. Permitir o teste de atualizações baixadas por meio do software de administração centralizado antes de distribuí-las às máquinas dos clientes e a entrega das atualizações aos locais de trabalho dos usuários imediatamente após recebê-las.

4.13.3.33. Permitir a criação de uma hierarquia de servidores de administração a um nível arbitrário e a capacidade de gerir centralmente toda a hierarquia a partir do nível superior.

4.13.3.34. Suportar o Modo de Serviços Gerenciados para servidores de administração, para que instâncias de servidores de administração isoladas logicamente possam ser configuradas para diferentes usuários e grupos de usuários.

4.13.3.35. Ser capaz de realizar inventários de software e hardware instalados nos computadores dos usuários.

4.13.3.36. Ter um mecanismo de notificação para informar os usuários sobre eventos no software e nas configurações anti-malware instalados, e para distribuir notificações sobre eventos por e-mail.

4.13.3.37. Permitir a instalação centralizada de aplicativos de terceiros em todos ou em computadores selecionados.

4.13.3.38. Ter a capacidade de especificar qualquer computador da organização como centro de retransmissão de atualizações e pacotes de instalação, a fim de reduzir a carga da rede no sistema principal do servidor de administração.

4.13.3.39. Ter a capacidade de especificar qualquer computador da organização como centro de encaminhamento de eventos do sensor de endpoint do grupo



selecionado de computadores clientes para o servidor de administração centralizado, a fim de reduzir a carga da rede no sistema do servidor de administração principal.

4.13.3.40. Ser capaz de gerar relatórios gráficos para eventos de software anti-malware e dados sobre inventário de hardware e software, licenciamento, etc.

4.13.3.41. Permitir que o administrador defina configurações restritas nas configurações de política/perfil, para que uma tarefa de verificação de vírus possa ser acionada automaticamente quando um determinado número de vírus for detectado durante um período de tempo definido. Os valores para o número de vírus e escala de tempo devem ser configuráveis.

4.13.3.42. permitir ao administrador personalizar relatórios.

4.13.3.43. Permitir ao administrador definir um período de tempo após o qual um computador não conectado ao servidor de gerenciamento e seus dados relacionados serão automaticamente excluídos do servidor.

4.13.3.44. Permitir ao administrador definir diferentes condições de mudança de status para grupos de endpoint no servidor de gerenciamento.

4.13.3.45. O servidor de gerenciamento primário deve ser capaz de recuperar relatórios de informações detalhadas sobre o status de integridade, etc., dos terminais gerenciados dos servidores de gerenciamento secundários.

4.13.3.46. A solução proposta deve permitir instalar o modulo de gerenciamento on- premissa nos seguintes sistemas operacionais: Windows e Linux

4.13.3.47. A solução proposta deverá suportar os seguintes servidores de banco de dados para ambiente Windows:

4.13.3.47.1. Microsoft SQL Server;

4.13.3.47.2. Microsoft Banco de dados SQL do Azure;

4.13.3.47.3. MySQL Standard e Enterprise;

4.13.3.47.4. MariaDB;



4.13.3.47.5. PostgreSQL;

4.13.3.48. A solução proposta deverá suportar os seguintes servidores de banco de dados para ambiente Linux:

4.13.3.48.1. MySQL;

4.13.3.48.2. MariaDB;

4.13.3.48.3. PostgreSQL;

4.13.3.49. A solução proposta deverá suportar as seguintes plataformas virtuais:

4.13.3.49.1. VMware a partir de vSphere 6.7 em diante;

4.13.3.49.2. . Estação de trabalho VMware 17.0.2 Pro;

4.13.3.49.3. Servidor Microsoft Hyper-V a partir da versão 2012 em diante;

4.13.4. Do Módulo De Gerenciamento Simplificado

4.13.4.1. A solução proposta deve suportar arquitetura clou4.

4.13.4.2. A solução proposta deve incluir um console web integrado para o gerenciamento dos endpoint, que não deve exigir nenhuma instalação adicional.

4.13.4.3. O console de gerenciamento web da solução proposta deve ser simples de usar e deve suportar dispositivos com tela sensível ao toque.

4.13.4.4. A solução proposta deve permitir ao administrador gerar relatórios pré-definidos.

4.13.4.5. A solução proposta deve suportar a descoberta de uso por parte do usuário de aplicações e exibir informações detalhadas de uso de aplicações utilizadas por meios de navegadores e aplicações instaladas no endpoint.

4.13.4.6. A solução proposta deve atender as condições apontadas no item e subítemos "Requisitos Gerais".

4.13.4.7. A solução proposta deve suportar sistemas operacionais Windows e Linux.

4.13.4.8. A solução proposta deve incluir informações do endpoint:



4.13.4.8.1. IP público de internet;

4.13.4.8.2. IP interno do dispositivo;

4.13.4.8.3. Versão do agente de proteção;

4.13.4.8.4. Última comunicação com a console, contendo data e hora;

4.13.4.8.5. Informações do sistema operacional;

4.13.5. Requisitos Gerais

4.13.5.1. A solução proposta deve ser capaz de detectar os seguintes tipos de ameaças:

4.13.5.1.1. Malwares, Worms, Trojans, Backdoors, Rootkits, Spyware, Adware, Ransomware, Keyloggers, Crimeware, sites e links de phishing, vulnerabilidades do tipo ZeroDay e outros softwares maliciosos e indesejados.

4.13.5.2. solução proposta deve ser de um único fornecedor e suportar todos módulos descritos neste termo de referência.

4.13.5.3. A solução proposta deve suportar integração com Anti-malware Scan Interface (AMSI).

4.13.5.4. A solução proposta deve ter capacidade de integração com a central de segurança do Windows Defender.

4.13.5.5. A solução proposta deve suportar o subsistema Linux no Windows.

4.13.5.6. A solução proposta deve fornecer tecnologias de proteção da próxima geração, sendo no mínimo:

4.13.5.6.1. Proteção contra ameaças sem arquivos (Fileless);

4.13.5.6.2. Fornecimento de proteção baseada em machine learning em várias camadas e análise comportamental durante diferentes estágios da cadeia de ataque;

4.13.5.7. A solução proposta deve fornecer varredura de memória para estações de trabalho Windows;



4.13.5.8. A solução proposta deve fornecer varredura de memória do kernel para estações de trabalho Linux;

4.13.5.9. A solução proposta deve fornecer a capacidade de alternar para o modo nuvem para proteção contra ameaças, diminuindo o uso de RAM e disco rígido em máquinas com recursos limitados;

4.13.5.10. A solução proposta deve ter componentes dedicados para monitorar, detectar e bloquear atividades em endpoint de Windows e Linux, para proteção contra ataques remotos de criptografia;

4.13.5.11. A solução proposta deve incluir componentes sem assinatura para detectar ameaças mesmo sem atualizações frequentes. A proteção deve ser alimentada por machine learning estático para pré-execução e machine learning dinâmico para estágios pós-execução da cadeia de eliminação em endpoints e na nuvem para servidores e estações de trabalho Windows;

4.13.5.12. A solução proposta deve fornecer análise comportamental baseada em machine learning;

4.13.5.13. A solução proposta deve incluir a capacidade de configurar e gerenciar configurações de firewall integradas aos sistemas operacionais Windows Server e Linux, através de seu console de gerenciamento;

4.13.5.14. A solução proposta deve incluir os seguintes componentes no sensor instalado no endpoint;

4.13.5.14.1. Controles de aplicativos;

4.13.5.14.2. Controle web e dispositivos;

4.13.5.14.3. HIPS e Firewall;

4.13.5.14.4. Descoberta de patches e vulnerabilidades de sistemas operacionais Windows;



4.13.5.15. A capacidade de detectar e bloquear hosts não confiáveis na detecção de atividades semelhantes à criptografia em recursos compartilhados do servidor.

4.13.5.16. A solução proposta deve ser protegida por senha para evitar que o processo do anti-malware seja interrompido sendo a autoproteção, independentemente do nível de autorização do usuário no sistema.

4.13.5.17. A solução proposta deve ter bancos de dados de reputação locais e globais.

4.13.5.18. A solução proposta deve ser capaz de verificar o tráfego HTTPS, HTTP, SMTP e FTP contra malwares.

4.13.5.19. A solução proposta deve incluir um módulo capaz, no mínimo, de:

4.13.5.19.1. Bloqueio de aplicativos com base em sua categorização;

4.13.5.19.2. Bloqueio/permissão de pacotes, protocolos, endereços IP, portas e direção de tráfego específicos;

4.13.5.19.3. A adição de sub redes e a modificação de permissões de atividade;

4.13.5.20. A solução proposta deve impedir a conexão de dispositivos USB reprogramados emulando teclados e permitir o controle do uso de teclados na tela mediante autorização.

4.13.5.21. A solução proposta deve ser capaz de bloquear ataques à rede e reportar a origem da infecção.

4.13.5.22. A solução proposta deve ter armazenamento local nos endpoint para manter cópias dos arquivos que foram excluídos ou modificados durante a desinfecção. Esses arquivos devem ser armazenados em um formato específico que garanta que não representem qualquer ameaça.

4.13.5.23. A solução proposta deve ter uma abordagem proativa para impedir que malware explore vulnerabilidades existentes em servidores e estações de trabalho.



4.13.5.24. A solução proposta deve suportar a tecnologia AM-PPL (Anti-Malware Protected Process Light) para proteção contra ações maliciosas.

4.13.5.25. A solução proposta deve incluir proteção contra ataques que explorem vulnerabilidades no protocolo ARP para falsificar o endereço MAC do dispositivo.

4.13.5.26. A solução proposta deve incluir um componente de controle capaz de aprender a reconhecer o comportamento típico do usuário em um indivíduo ou grupo específico de computadores protegidos e, em seguida, identificar e bloquear ações anômalas e potencialmente prejudiciais realizadas por esse terminal ou usuário.

4.13.5.27. A solução proposta deve fornecer funcionalidade Anti-Bridging para estações de trabalho Windows para evitar pontes não autorizadas para a rede interna que contornem as ferramentas de proteção de perímetro. Os administradores devem ser capazes de proibir o estabelecimento simultâneo de conexões com fio, Wi-Fi e modem.

4.13.5.28. A solução proposta deve incluir um componente dedicado para verificação de conexões criptografadas.

4.13.5.29. A solução proposta deve ser capaz de descriptografar e verificar o tráfego de rede transmitido por conexões criptografadas.

4.13.5.30. A solução proposta deve ter a capacidade de excluir automaticamente recursos da web quando ocorre um erro de verificação durante a execução de uma verificação de conexão criptografada. Esta exclusão deve ser exclusiva do host e não deve ser compartilhada com outros endpoint;

4.13.5.31. A solução proposta deve incluir funcionalidade para apagar dados remotamente das estações de trabalho;

4.13.5.32. A solução proposta deve incluir funcionalidade para excluir automaticamente os dados caso não haja conexão com o servidor de gerenciamento de endpoint.



4.13.5.33. A solução proposta deve suportar detecção baseadas em multicamadas sendo no mínimo: assinatura, heurística, machine learning ou assistida por nuvem.

4.13.5.34. A solução proposta deve ter a capacidade de gerar um alerta, limpar e excluir uma ameaça detectada.

4.13.5.35. A solução proposta deve ter a capacidade de acelerar as verificações ignorando os objetos que não foram alterados desde a verificação anterior.

4.13.5.36. A solução proposta deve permitir que o administrador exclua arquivos/pastas/aplicativos/certificados digitais específicos da verificação, seja no acesso (proteção em tempo real) ou durante verificações sob demanda.

4.13.5.37. A solução proposta deve verificar automaticamente as unidades removíveis em busca de malware quando elas estiverem conectadas a qualquer endpoint.

4.13.5.38. A solução proposta deve ser capaz de bloquear o uso de dispositivos de armazenamento USB ou permitir o acesso apenas aos dispositivos permitidos.

4.13.5.39. A solução proposta deve ser capaz de diferenciar dispositivos de armazenamento USB, impressoras, celulares e outros periféricos.

4.13.5.40. A solução proposta deve ter a capacidade de bloquear/permitir o acesso do usuário aos recursos da web com base nos sites e tipo de conteúdo.

4.13.5.41. A solução proposta deve ter categoria de detecção para bloquear banners de sites.

4.13.5.42. A solução proposta deve fornecer a capacidade de configurar redes Wi-Fi com base no nome da rede, tipo de autenticação e tipo de criptografia em dispositivos móveis;

4.13.5.43. A solução proposta deve suportar políticas baseadas no usuário para controle de dispositivos, web e aplicativos.



4.13.5.44. A solução proposta deve apresentar integração na nuvem, para fornecer atualizações mais rápidas possíveis sobre malware e ameaças potenciais.

4.13.5.45. A solução proposta deve ter capacidade de gerenciar direitos de acesso de usuários para operações de leitura e gravação em CDs/DVDs, dispositivos de armazenamento removíveis e dispositivos MTP.

4.13.5.46. A solução proposta deve permitir que o administrador monitore o uso de portas personalizadas/aleatórias pelo aplicativo;

4.13.5.47. A solução proposta deve suportar o bloqueio de aplicativos proibidos (lista de negações) de serem lançados no endpoint e o bloqueio de todos os aplicativos que não sejam aqueles incluídos nas listas de permissões.

4.13.5.48. A solução proposta deve ter um componente de controle de aplicativos integrado à nuvem para acesso imediato às atualizações mais recentes sobre classificações e categorias de aplicativos.

4.13.5.49. A solução proposta deve incluir filtragem de malware de tráfego, verificação de links da web e controle de recursos da web com base em categorias de nuvem.

4.13.5.50. O componente de controle web da solução proposta deve incluir uma categoria criptomoedas e mineração.

4.13.5.51. O componente de controle de aplicações da solução proposta deve incluir os modos operacionais lista de negações e lista de permissões.

4.13.5.52. A solução proposta deve suportar o controle de scripts executados em PowerShell.

4.13.5.53. A solução proposta deve suportar modo teste com geração de relatórios sobre execução de aplicativos bloqueados.

4.13.5.54. A solução proposta deve ter a capacidade de controlar o acesso do sistema/aplicativo do usuário a dispositivos de gravação de áudio e vídeo.



4.13.5.55. A solução proposta deve fornecer um recurso para verificar os aplicativos listados em cada categoria baseada em nuvem.

4.13.5.56. A solução proposta deve ter capacidade de integração com um sistema avançado de proteção contra ameaças específico do fornecedor.

4.13.5.57. A solução proposta deve ter a capacidade de regular automaticamente a atividade dos programas em execução, incluindo o acesso ao sistema de arquivos e ao registro, bem como a interação com outros programas.

4.13.5.58. A solução proposta deve ter a capacidade de categorizar automaticamente os aplicativos iniciados antes da instalação da proteção de endpoint.

4.13.5.59. A solução proposta deve ter proteção contra ameaças de e-mail de endpoint com:

4.13.5.59.1. Filtro de anexos.

4.13.5.59.2. Verificação de mensagens de e-mail ao receber, ler e enviar.

4.13.5.60. A solução proposta deve ter a capacidade de verificar vários redirecionamentos, URLs encurtados, URLs sequestrados e atrasos baseados em tempo.

4.13.5.61. A solução proposta deve permitir que o usuário do computador verifique a reputação de um arquivo;

4.13.5.62. A solução proposta deve incluir a verificação de todos os scripts, incluindo quaisquer scripts WSH (JavaScript, Visual Basic, etc.);

4.13.5.63. A solução proposta deve fornecer proteção contra malware ainda desconhecido com base na análise do seu comportamento e verificação de alterações no registro do sistema, juntamente com mecanismo de remediação para restaurar automaticamente quaisquer alterações no sistema feitas pelo malware.



4.13.5.64. A solução proposta deve fornecer proteção contra ataques de hackers por meio de um firewall com sistema de prevenção de intrusões e regras de atividade de rede para aplicações mais populares ao trabalhar em redes de computadores de qualquer tipo, incluindo redes sem fio.

4.13.5.65. A solução proposta deve incluir suporte ao protocolo IPv6.

4.13.5.66. A solução proposta deve oferecer a verificação de seções críticas do computador como uma tarefa independente.

4.13.5.67. A solução proposta deve incorporar a tecnologia de autoproteção de aplicação:

4.13.5.67.1. Protegendo contra o gerenciamento remoto não autorizado de um serviço de aplicativo.

4.13.5.67.2. Protegendo o acesso aos parâmetros do aplicativo definindo uma senha. Evitando a desativação da proteção por malware, criminosos ou usuários.

4.13.5.68. A solução proposta deve oferecer a capacidade de escolher quais componentes de proteção contra ameaças instalar.

4.13.5.69. A solução proposta deve incluir a verificação anti-malware e desinfecção de arquivos em arquivos nos formatos RAR, ARJ, ZIP, CAB, LHA, JAR, ICE, incluindo arquivos protegidos por senha.

4.13.5.70. A solução proposta deve proteger contra malware ainda desconhecido pertencente a famílias cadastradas, com base em análise heurística.

4.13.5.71. A solução proposta deve notificar o administrador sobre eventos importantes que ocorreram através de notificação por e-mail.

4.13.5.72. A solução proposta deve permitir ao administrador criar um único pacote de instalação do sensor de proteção com a configuração necessária.

4.13.5.73. A solução proposta deve fornecer controles de aplicativos e dispositivos para estações de trabalho Windows.



4.13.5.74. A proteção da solução proposta para servidores e estações de trabalho deve incluir um componente dedicado para proteção contra atividades de ransomware/malwares que criptografa os recursos compartilhados.

4.13.5.75. A solução proposta deve, ao detectar atividades semelhantes a ransomware/criptografia, bloquear automaticamente o computador atacante por um intervalo especificado e listar informações sobre o IP e carimbo de data/hora do computador atacante e o tipo de ameaça.

4.13.5.76. A solução proposta deve fornecer uma lista predefinida de exclusões de verificação para aplicativos e serviços Microsoft.

4.13.5.77. A solução proposta deve suportar a instalação de proteção de endpoint em servidores sem a necessidade de reinicialização.

4.13.5.78. A solução proposta deve permitir a instalação de software com funcionalidades de anti-malware e detecção e resposta de incidente a partir de um único pacote de distribuição.

4.13.5.79. A solução proposta deve suportar endereços IPv6.

4.13.5.80. A solução proposta deve suportar verificação em duas etapas (autenticação).

4.13.5.81. A solução proposta deve prever a instalação, atualização e remoção centralizada de software anti-malware, juntamente com configuração, administração centralizada e visualização de relatórios e informações estatísticas sobre o seu funcionamento.

4.13.5.82. A solução proposta deverá contar com a remoção centralizada (manual e automática) de aplicações incompatíveis do centro de administração.

4.13.5.83. A solução proposta deve fornecer métodos flexíveis para instalação do sensor de endpoint via: RPC, GPO e um agente de administração para instalação remota e a opção de criar um pacote de instalação independente para instalação do endpoint de segurança localmente.



4.13.5.84. A solução proposta deve permitir a instalação remota do sensor de endpoint com os bancos de dados anti-malware mais recentes.

4.13.5.85. A solução proposta deve permitir a atualização automática do sensor de endpoint e de bases de dados de anti-malware.

4.13.5.86. A solução proposta deve contar com recursos de busca automática de vulnerabilidades em aplicações e no sistema operacional em máquinas protegidas.

4.13.5.87. A solução proposta deve permitir a gestão de um componente que proíba a instalação e/ou execução de programas.

4.13.5.88. A solução proposta deve permitir a gestão de um componente que controle o trabalho com dispositivos de E/S externos.

4.13.5.89. A solução proposta deve permitir o gerenciamento de componente que controle a atividade do usuário na internet.

4.13.5.90. A solução proposta deve ser capaz de implantar automaticamente proteção para infraestruturas virtuais baseadas em VMware ESXi, Microsoft Hyper-V, plataforma de virtualização Citrix XenServer ou hipervisor.

4.13.5.91. A solução proposta deve incluir a distribuição automática de licenças nos computadores clientes.

4.13.5.92. A solução proposta deverá ser capaz de exportar relatórios para arquivos PDF, CSV ou XLS.

4.13.5.93. A solução proposta deve proporcionar a administração centralizada de armazenamentos de backup e quarentenar em todos os recursos da rede onde o sensor de endpoint está instalado.

4.13.5.94. A solução proposta deve prever a criação de contas internas para autenticar administradores no servidor de administração.

4.13.5.95. A solução proposta deverá ter capacidade de gerenciar dispositivos móveis através de comandos remotos.



4.13.5.96. A solução proposta deve ter a capacidade de excluir atualizações baixadas.

4.13.5.97. A solução proposta deve mostrar claramente informações sobre a distribuição de vulnerabilidades entre computadores gerenciados.

4.13.5.98. A interface do servidor de gerenciamento da solução proposta deverá suportar o idioma Inglês e português.

4.13.5.99. A solução proposta deve ter um painel customizável gerando e exibindo estatísticas em tempo real dos sensores de endpoints.

4.13.5.100. A solução proposta deve incorporar funcionalidade de distribuição/retransmissão para suportar a entrega de proteção, atualizações, patches e pacotes de instalação para locais e remotos.

4.13.5.101. Os relatórios da solução proposta devem incluir informações sobre cada ameaça e a tecnologia que a detectou.

4.13.5.102. A solução proposta deve incluir a opção para implantar uma console de gerenciamento local ou usar o console de gerenciamento baseado em nuvem fornecido pelo fornecedor.

4.13.5.103. A solução proposta deve ser capaz de se integrar ao console de gerenciamento baseado em nuvem do fornecedor para gerenciamento de endpoint sem custo adicional.

4.13.5.104. A solução proposta deve permitir a migração rápida do console de gerenciamento local para o console de gerenciamento baseado em nuvem do fornecedor.

4.13.5.105. A solução proposta deve fornecer mecanismos de atualização de banco de dados, incluindo:

4.13.5.105.1. Múltiplas formas de atualização, incluindo canais de comunicação globais através do protocolo HTTPS, recursos compartilhados em rede local e mídia removível.



4.13.5.105.2. Verificação da integridade e autenticidade das atualizações por meio de assinatura digital eletrônica.

4.13.5.106. A solução proposta deve permitir monitorar vulnerabilidades existentes em dispositivos gerenciados.

4.13.5.107. A solução proposta deve gerar relatórios de vulnerabilidades encontradas nos dispositivos com sensor de endpoint instalado.

4.13.6. Do Módulo De Edr

4.13.6.1. Deve apresentar um gráfico de propagação de ameaças com os principais processos, conexões de rede, DLLs, seções de registro afetado ou envolvido no alerta.

4.13.6.2. Todas as detecções são destacadas no gráfico, fornecendo ao analista o contexto completo para o incidente e facilitando o processo de revelação dos componentes afetados.

4.13.6.3. A solução proposta deve permitir detectar e erradicar ataques avançados, realizar análises de causa raiz com um gráfico visualizado da cadeia de desenvolvimento de ameaças;

4.13.6.4. Deve apresentar as seguintes informações:

4.13.6.4.1. Processo;

4.13.6.4.2. Arquivos;

4.13.6.4.3. Chaves de registros;

4.13.6.4.4. Conexões de rede;

4.13.6.4.5. SHA256 e MD5

4.13.6.5. Dever ser integrado ao portal de inteligência do fornecedor para enriquecimento dos detalhes da análise;

4.13.6.6. Deve apresentar informações detalhadas contendo:



4.13.6.6.1. Usuário que executou a ação;

4.13.6.6.2. Informações acesso privilegiado;

4.13.7. Documentação Da Solução

4.13.7.1. A solução ofertada incluindo ferramentas de administração, deve incluir os seguintes documentos:

4.13.7.1.1. Ajuda on-line para administradores

4.13.7.1.2. Ajuda on-line para melhores práticas de implementação

4.13.7.1.3. Ajuda on-line para proteção de servidores de administração

4.13.7.2. A documentação do software anti-malware fornecida deve descrever detalhadamente os processos de instalação, configuração e uso do software anti-malware.

4.13.7.3. Deve estar disponível página com informações de ciclo de vida das soluções e módulos.

4.14. Requisitos de garantia e suporte técnico:

4.14.1. A garantia e o suporte técnico devem obrigatoriamente prover, sem ônus adicional, ao Contratante e durante todo o prazo de vigência contratual;

4.14.2. Atualização das versões dos softwares fornecidos, se novas versões forem disponibilizadas;

4.14.3. Atualização dos softwares fornecidos, se houver lançamento de novos softwares em substituição aos fornecidos, ou mesmo não sendo uma substituição, se ficar caracterizada uma descontinuidade dos softwares fornecidos;

4.14.4. O Contratado deverá garantir o funcionamento dos consoles de gerenciamento e atualização (inclusive na instalação ou atualização de versões/releases) ou problemas de incompatibilidade com outros softwares do



Município de Santa Bárbara d'Oeste

Município de Santa Bárbara d'Oeste, fornecer o suporte técnico no horário comercial, das 8 h às 18 h ininterruptamente, nos dias úteis e em caso emergencial para os Serviços totalmente indisponíveis deverá possuir atendimento 24x7 com o SLA conforme a tabela Prazos de Atendimentos;

4.14.5. O serviço de suporte poderá ser remoto, desde que seja possível a resolução do problema conforme a tabela 1 e 2, abaixo descritas, para os prazos de atendimentos. Em caso de necessidade, o serviço de suporte deverá ser feito na modalidade on-site.

4.14.6. Em caso de necessidade de melhorias, nova instalação, ou nova versão ou correção, O Contratado deverá prestar suporte quanto a essas operações, assim como atuar on-site na correspondente instalação, se necessário ou mediante solicitação do Contratante;

4.14.7. O Contratado deverá fazer uma visita anual de 8h presenciais sem ônus adicionais ao Contratante, durante a vigência do contrato, para efetuar verificação da solução implementada, realizando ajustes, se houver, manutenções, suporte presencial preventivo e melhorias nas políticas de segurança, executar análise de vulnerabilidades, para zelar pela segurança da infraestrutura de servidores e estações do Município de Santa Bárbara d'Oeste contra as possíveis ameaças existentes e falhas em políticas de segurança;

4.14.8. O serviço de suporte deverá ser prestado através de contato telefônico, sítio na Internet (website do fabricante ou do fornecedor), correio eletrônico (e-mail do fabricante ou do fornecedor) ou no local (provido pelo fabricante ou pelo fornecedor), conforme os níveis de severidade e prazos de atendimento especificados nas tabelas 1 e 2.

4.14.9. O suporte técnico deverá ser obrigatoriamente fornecido em língua portuguesa, oral ou escrito;

4.14.10. O(s) software(s) fornecido(s) deverá garantir a detecção, limpeza e/ou remoção de ocorrências nas estações e servidores protegidos, de forma



Município de Santa Bárbara d'Oeste

automática e, em pelo menos, 99,9% dos casos. Caso o software não detecte e remova a infecção automaticamente, O Contratado será acionada e deverá fornecer e executar a vacina on-site para solucionar o problema;

4.14.11. O Contratado deverá possuir site - Helpdesk para abertura de "chamados", disponibilizando telefones para aberturas de chamados técnicos em português, DDR local ou 0800 para a abertura de chamados;

4.14.12. O Contratado deverá apresentar, por declaração, comprovando possuir condições para a prestação dos serviços para o Município de Santa Bárbara d'Oeste nas condições estipuladas acima.

Nível	Descrição
1	Serviços totalmente indisponíveis.
2	Serviços parcialmente indisponíveis ou com degradação de tempo de resposta no acesso aos aplicativos.
3	Serviços disponíveis com ocorrência de alarmes de avisos, consultas sobre problemas, dúvidas gerais sobre o software de antivírus.

Modalidade de atendimento	Prazo	Severidade 1	Severidade 2	Severidade 3
On-site e telefone	Início de atendimento	2 horas úteis	4 horas úteis	24 horas úteis
On-site e telefone	Término de atendimento	8 horas úteis	16 horas úteis	72 horas úteis
Telefone, e-mail e web/helpdesk	Início de atendimento	-	-	24 horas úteis
Telefone, e-mail e web/helpdesk	Término de atendimento	-	-	72 horas úteis



4.15. Requisitos de treinamento:

4.15.1. O treinamento deverá ser ministrado nas dependências da Diretoria de Gestão de Tecnologia da Informação do Município de Santa Bárbara d'Oeste, em ambiente próprio e dedicado para este fim. Caso o treinamento seja realizado fora do Município de Santa Bárbara d'Oeste, o Contratado será responsável pelas despesas de transporte, hospedagem e alimentação e outras necessárias ao treinamento, sem que isso gere ônus adicionais ao Contratante.

4.15.2. O treinamento englobará o conteúdo de todos os módulos ofertados na solução de segurança.

4.15.3. O treinamento deverá ter carga horária de no mínimo 5 horas.

4.15.4. Para todos os efeitos, inclusive de emissão do Termo de Recebimento, este treinamento faz parte do processo de instalação e aceitação da solução, que deverá iniciar em até 15 dias após a assinatura do contrato.

4.15.5. O programa para o treinamento deverá ser previamente aprovado pelo Município de Santa Bárbara d'Oeste e eventuais mudanças de conteúdo solicitadas deverão constar no material didático a ser entregue pelo Contratado.

4.15.6. No caso de o treinamento fornecido não ser satisfatório, mediante avaliação tempestiva e fundamentada, tanto em relação à qualidade ou à carga horária efetiva, O Contratado deverá realizar novo treinamento sem ônus adicional ao Município de Santa Bárbara d'Oeste.

4.15.7. O material didático deverá ser oficial da marca cotada e estar incluído, sem ônus adicional para o Município de Santa Bárbara d'Oeste.

4.15.8. O treinamento deverá ser ministrado para a equipe de infraestrutura do Município de Santa Bárbara d'Oeste, composta por 07 funcionários.

4.15.9. Deverá ser emitido certificado de participação ao final do curso.

4.16. Visita técnica:



4.16.1. A visita técnica é facultativa e tem por objetivo dar ao Município de Santa Bárbara d'Oeste à Municipalidade a certeza e a comprovação de que todos os licitantes conhecem integralmente o objeto da licitação e, por consequência, que suas propostas de preços possam refletir com exatidão a sua plena execução, evitando-se futuras alegações de desconhecimento das características do objeto licitado, resguardando ao Município de Santa Bárbara d'Oeste de possíveis inexecuções contratuais.

4.16.2. Para as licitantes que optarem pela não realização da vistoria, não serão aceitas alegações posteriores quanto ao detalhamento, especificações e obrigações que compõe esta contratação, não podendo o Contratado, na execução do contrato, alegar desconhecimento das condições técnicas e outras necessárias para justificar a inexecução da prestação dos serviços do objeto do Edital.

4.16.3. A visita técnica deverá ser previamente agendada pela licitante junto ao Departamento de Tecnologia da Informação do Município de Santa Bárbara d'Oeste pelo telefone (19) 3455-8264 ou pelo e-mail gilson.barbosa@santabarbara.sp.gov.br deverá, obrigatoriamente, ser realizada por representante da licitante que tenha condições técnicas suficientes para identificar com clareza os recursos necessários que deverão ser utilizados no objeto da licitação em comento, para possibilitar a correta formulação da proposta comercial a ser apresentada na sessão pública.

4.16.4. O representante da licitante designado para realizar a visita técnica de que trata este item, deverá apresentar ao Município de Santa Bárbara d'Oeste, no momento da visita, documento oficial de identificação, bem como autorização emitida pelo licitante para a realização de vistoria técnica.

4.16.5. Ao final da Visita Técnica acima mencionada será confeccionado Termo de Vistoria assinado pelo representante da licitante, o qual será juntado ao dossiê da licitação.



4.16.6. A visita técnica realizar-se-á no período compreendido entre a data da publicação deste Termo de Referência e o último dia útil anterior à sessão pública do processo licitatório, das 07h30min às 15h00min.

4.16.7. Não haverá visita sem prévio agendamento e em mesma data/horário por mais de uma Licitante, tampouco no dia da sessão pública.

5. DO MODELO DE EXECUÇÃO DO OBJETO

5.1. A execução do objeto deverá ser iniciada após a assinatura do contrato e emissão da Ordem de Serviço pela Contratante.

5.2. A empresa vencedora será inteiramente responsável pela migração da solução atual para a nova solução e a instalação de todos os componentes que englobam este documento, não afetando o funcionamento dos sistemas, recursos ou equipamentos atualmente em operação do Município de Santa Bárbara d'Oeste, atendendo integralmente aos requisitos técnicos descritos neste Termo de Referência.

5.3. O Contratado deverá garantir as atualizações do software, sem custo adicional para a Contratante durante a vigência do contrato.

5.4. A empresa vencedora deverá apresentar, para aprovação do Departamento de Tecnologia da Informação do Município de Santa Bárbara d'Oeste, plano detalhado de migração e instalação, especificando os procedimentos e prazos a serem adotados, com até 05 (cinco) dias úteis após o dia de assinatura do contrato.

5.5. Todos os serviços necessários à implementação da solução proposta deverão ser obrigatoriamente descritos no plano de migração, considerando a alocação de técnicos certificados pelo fabricante em análise e segurança de rede, sendo que todas as despesas de locomoção, alimentação, pernoites, etc. serão de exclusiva responsabilidade do Contratado.



Município de Santa Bárbara d'Oeste

5.6. Os técnicos especializados se reunirão com a equipe da Diretoria de Gestão de Tecnologia da Informação do Município de Santa Bárbara d'Oeste para rever todas as premissas que servirão de base para o presente projeto e determinar todos os objetivos para a implementação da solução Contratada, definindo sua arquitetura, abrangência, forma e pré-requisitos.

5.7. A migração dos softwares instalados nas estações de trabalho deverá ser realizada sem causar indisponibilidade de uso da mesma em prazo inferior a 30 (trinta) minutos e a migração dos softwares instalados nos servidores deverão ser realizadas sem causar indisponibilidade dos mesmos.

5.8. Toda a migração será acompanhada por representante(s) da equipe da Diretoria de Gestão de Tecnologia da Informação do Município de Santa Bárbara d'Oeste.

5.9. A instalação deverá ser executada silenciosa e automaticamente sem a interferência do usuário final. Na sua impossibilidade, esvaziado todas as tentativas, por GPO, Scripts, etc., o Contratado deverá proceder à instalação presencial de forma manual, sem exceção, em todos os 1.500 equipamentos.

5.10. A instalação não poderá causar interferência nos aplicativos do Município de Santa Bárbara d'Oeste e em produção. Caso isso aconteça a responsabilidade de correção deverá ser totalmente do Contratado.

5.11. O prazo total para apresentação de plano de migração não poderá ser superior a 05 (cinco) dias úteis, a partir da assinatura do contrato.

5.12. O prazo total da migração das estações de trabalho e servidores não poderá ser superior a 45 (quarenta e cinco) dias corridos, tanto o parque central como as demais unidades, a partir da data de aprovação do plano de migração.

5.13. A instalação com a respectiva migração de regras da solução adota anteriormente abrange todas as unidades do Município de Santa Bárbara d'Oeste, compreendendo 1.500 equipamentos distribuídos no Paço Municipal e algumas localizadas externas de todas as Secretarias Municipais.



5.14. São definidos como mecanismos formais de comunicação, entre o Contratante e o Contratado, os seguintes:

5.15. Ordem de Serviço;

5.16. Sistema de abertura de chamados;

5.17. E-mails.

5.18. O Contratado deverá ter um canal para abertura de chamados, que poderá ser por meio de telefone, e-mail ou canal de internet.

5.19. A execução será considerada satisfatória quando a solução estiver implantada, licenciada, atualizada, monitorada, documentada, testada, com treinamento realizado, suporte ativo e aceite formal do Contratante, sem prejuízo das correções que se mostrarem necessárias durante a vigência contratual.

6. DO MODELO DE GESTÃO DO CONTRATO

6.1. O Contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133, de 2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

6.2. As comunicações entre o Contratante e o Contratado devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

6.3. O Contratante poderá convocar representante da empresa para adoção de providências que devam ser cumpridas em face deste Contrato.

6.4. Após a assinatura do contrato, o Contratante poderá convocar o representante do Contratado para reunião inicial para apresentação do plano de fiscalização, que conterà informações acerca das obrigações, dos mecanismos de fiscalização, das estratégias para execução/entrega do objeto, do plano complementar de execução do Contrato, quando houver, do método de aferição dos resultados e das sanções aplicáveis, dentre outros.



6.5. A gestão e fiscalização do Contrato deverão ser executadas fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133, de 2021, e do Decreto Municipal nº 7.506/2023 e cada parte responderá pelas consequências de sua inexecução total ou parcial.

6.6. A gestão deste contrato será realizada pelo gestor e fiscal abaixo:

Gestor: Danieli Amorim de Oliveira Camargo

Fiscal: Gilson Silva Barbosa

Manutenção de Sigilo e Normas de Segurança

6.7. O Contratado deverá manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo Contratante a tais documentos.

6.8. O Termo de Compromisso e Manutenção de Sigilo, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes do Contratante, a ser assinado pelo representante legal do Contratado, e Termo de Ciência, a ser assinado por todos os empregados do Contratado diretamente envolvidos na contratação.

7. DOS CRITÉRIOS DE MEDIÇÃO E DE PAGAMENTO

Recebimento do Objeto

7.1. Os serviços serão recebidos provisoriamente, de forma sumária, no ato da entrega, juntamente com a nota fiscal ou instrumento de cobrança equivalente, pelo(a) responsável pelo acompanhamento e fiscalização do instrumento contratual, para efeito de posterior verificação de sua conformidade com as especificações constantes neste Termo de Referência e na proposta.



7.2. Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, devendo ser substituídos no prazo de **05 dias (cinco)**, a contar da notificação do Contratado, às suas custas, sem prejuízo da aplicação das penalidades.

7.3. O recebimento definitivo ocorrerá após recebimento da nota fiscal ou instrumento de cobrança equivalente pelo Contratante, e após a verificação da qualidade e quantidade do material e consequente aceitação mediante termo detalhado.

7.4. O prazo para recebimento definitivo poderá ser excepcionalmente prorrogado, de forma justificada, por igual período, quando houver necessidade de diligências para a aferição do atendimento das exigências contratuais.

7.5. No caso de controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, deverá ser observado o teor do art. 143 da Lei nº 14.133, de 2021, comunicando-se à empresa para emissão de Nota Fiscal no que pertinente à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.

7.6. O prazo para a solução, pelo Contratado, de inconsistências na execução do objeto ou de saneamento da nota fiscal ou instrumento de cobrança equivalente, verificadas pelo Contratante durante a análise prévia à liquidação de despesa, não será computado para os fins do recebimento definitivo.

7.7. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança do serviço nem a responsabilidade ético-profissional pela perfeita execução do instrumento contratual.

Condição de pagamento

7.8. O Contratado deverá emitir na data após entrega do respectivo serviço a nota fiscal correspondente.



7.9. O pagamento dos serviços de implantação, migração e treinamento (Itens 2 e 3) será efetuado em parcela única, após a execução integral, ateste de conformidade e recebimento definitivo desta etapa.

7.10. O pagamento do licenciamento e suporte técnico (Itens 1 e 4) será efetuado de forma anual, de serviço efetivamente disponibilizado e prestado, sendo vedada a antecipação integral do valor contratual.

7.10.1. O pagamento das licenças de uso somente ocorrerá após o ateste definitivo da fase de implantação e entrada em operação do sistema.

7.11. O pagamento será efetuado no prazo de até 30 (trinta) dias corridos contados do Recebimento Definitivo, por crédito em conta corrente em nome do Contratado, mediante a apresentação do(s) original(is) da(s) nota(s) fiscal(is).

7.12. O Contratado deverá deter ciência plena em cumprir, com rigor, os termos do Decreto Municipal nº 7.468/23 e Anexo Único, sob pena de não pagamento dos valores devidos.

7.13. 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 IPC-FIPE de correção monetária.

8. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

8.1. O valor estimado da contratação possui caráter sigiloso devendo ser tornado público apenas depois do julgamento das propostas, com vistas a fomentar a competitividade entre os licitantes e potencializar a vantajosidade em eventual negociação a ser firmada pelo Agente de Contratação.

9. DA FORMA E CRITÉRIOS DE SELEÇÃO DO CONTRATADO



Forma de seleção e critério de julgamento da proposta

9.1. O fornecedor será selecionado por meio da realização de procedimento de **licitação**, na modalidade **pregão**, sob a **forma eletrônica**, com adoção do critério de julgamento pelo menor preço global.

Proposta

ITEM	CÓDIGO	DESCRIÇÃO	UNIDADE DE MEDIDA	QTDE	VALOR UNITÁRIO R\$	VALOR TOTAL R\$
1	2.01.02.0069.6	Licença proteção antivírus Endpoint Protection e EDR	Unidade x anual	3.000 (1.500 x 2 anos)		
2	2.01.02.0076.9	Migração e implantação da proteção antivírus (Endpoint Protection)	Unidade	01		
3	2.01.02.0077.7	Treinamento proteção antivírus Endpoint Protection	Unidade	01		
4	2.01.02.0078.5	Suporte técnico em proteção antivírus Endpoint Protection	Anual	02		
Valor Total da Contratação						

9.2. Conforme previsto no item 7.10, o licenciamento e suporte técnico (Itens 1 e 4) será efetuado de forma anual, de serviço efetivamente disponibilizado e prestado.

9.2.1. Serão disponibilizado 1.500 Licenças (Item 01) anualmente, totalizando 3.000 licenças na vigência do contrato (dois anos).

9.2.2. O Suporte técnico (Item 04) possuirá medição anual e deverá ser prestado durante todo período do contrato (dois anos).



Qualificação técnica:

9.3. Para participar da licitação, os proponentes deverão conter apresentar as seguintes documentações:

9.3.1. Comprovação de aptidão para execução de serviço similar, de complexidade tecnológica e operacional equivalente ou superior à do objeto desta contratação, ou do item pertinente, por meio da apresentação de certidões ou atestados emitidos por pessoas jurídicas de direito público ou privado, ou pelo conselho profissional competente, quando for o caso.

9.3.1.1 Para fins da comprovação de que trata este subitem, os atestados deverão dizer respeito a contrato(s) executado(s) com 50% (cinquenta por cento) do item 01, ou seja, fornecimento de 750 licenças de proteção antivírus Endpoint Protection e EDR pelo período de 02 anos.

9.3.1.2. Serão admitidos, para fins de comprovação de quantitativo mínimo de serviço, a apresentação e o somatório de diferentes atestados de serviços executados de forma concomitante.

9.4. O licitante deverá apresentar declaração de comprovação que no site do fabricante tem canal autorizado a fornecer e instalar os produtos da marca.

9.5. Por ocasião da assinatura do contrato deverá apresentar o certificado do profissional da proponente que deverá implementar a solução

9.5.1. A proponente deverá apresentar 02 (dois) ou mais analistas certificados na solução.

9.5.2. O certificado deverá ser emitido pelo(s) fabricante(s) oficiais dos *Softwares* com a sua respectiva data de emissão, validade e comprovação do vínculo com a empresa mediante contrato social, registro na carteira profissional, ficha de empregado ou contrato de trabalho, sendo possível a contratação de profissional autônomo que preencha os requisitos e se responsabilize tecnicamente pela execução dos serviços.



10. DA ADEQUAÇÃO ORÇAMENTÁRIA

10.1. A contratação será atendida pelas seguintes dotações: Unidade Orçamentária: 02.01.02 – Planejamento Estratégico; 02.02.01 – Educação Infantil; 02.02.02 – Ensino Fundamental; 02.0.3.01 – Saúde Geral Natureza de Despesa: 3.3.90.40.00 - OUTROS SERVIÇOS DE TIC - PJ- Vínculo 01 – Próprio, suplementadas, se necessário.

MONICA MOSNA
Secretária Municipal de Administração

TÂNIA MARA DA SILVA
Secretária Municipal de Educação

MARCUS PENSUTI
Secretário Municipal de Saúde



Apêndice do Anexo I – Estudo Técnico Preliminar

ORGÃO(ÕES) SOLICITANTES(S)*:

Secretaria Municipal de Administração
Secretaria Municipal de Educação
Secretaria Municipal de Saúde

I - **DESCRIÇÃO DA NECESSIDADE***: A presente contratação decorre da necessidade imperiosa de fortalecer a segurança da informação e a integridade da infraestrutura tecnológica no âmbito das Secretarias Municipais de Administração, Educação e Saúde do Município de Santa Bárbara d'Oeste. Diante do cenário contemporâneo de sofisticação e aumento exponencial das ameaças cibernéticas, tais como malwares, ransomwares, técnicas de phishing, exploração de vulnerabilidades zero-day e tentativas de acessos indevidos a dados institucionais, a proteção dos ativos digitais tornou-se um requisito crítico para a governança pública. Atualmente, o parque tecnológico que atende às demandas finalísticas das referidas Secretarias conta com aproximadamente 1.500 endpoints, abrangendo estações de trabalho, notebooks e servidores. Essa infraestrutura processa, transmite e armazena diariamente um volume massivo de informações sensíveis, incluindo dados pessoais e biométricos de cidadãos (notadamente nas áreas de saúde e educação), prontuários médicos, registros escolares e dados estratégicos para a gestão orçamentária e administrativa municipal. Sob a égide do Princípio da Eficiência (art. 37, caput, da CF) e em estrita observância às diretrizes da Lei Geral de Proteção de Dados Pessoais (LGPD — Lei Federal nº 13.709/2018), a Administração Pública tem o dever de mitigar riscos de incidentes de segurança. A ausência ou a obsolescência de ferramentas de proteção expõe o Município a sérios riscos de vazamento de informações, sequestro de dados com perdas financeiras correlatas, sanções administrativas e judiciais, além da iminente paralisação de serviços públicos digitais essenciais, o que afetaria diretamente o atendimento à população barbareense. Portanto, evidencia-se a necessidade pública de contratação de empresa especializada para o fornecimento de licenças de uso de solução integrada de segurança de endpoints, contemplando proteção antivírus (Endpoint Protection), detecção e resposta a incidentes (Endpoint Detection and Response- EDR), gerenciamento de vulnerabilidades e serviços associados de implantação, migração de dados das ferramentas legadas, suporte técnico especializado e monitoramento contínuo. Essa medida visa garantir a continuidade dos serviços, a confidencialidade dos dados e a resiliência cibernética municipal.

II - **DESCRIÇÃO DA PREVISÃO NO PLANEJAMENTO ANUAL DE CONTRATAÇÕES***: A presente contratação encontra-se formal e previamente



prevista nos Documentos de Formalização de Demandas (DFDs) sob os nºs 565/2026, de interesse da Secretaria Municipal de Administração; 610/2026, de interesse da Secretaria Municipal de Saúde; e 871/2026, de interesse da Secretaria Municipal de Educação. Tais instrumentos foram devidamente consolidados e ratificados no Plano de Contratações Anual (PCA) do Município de Santa Bárbara d'Oeste para o exercício de 2026.

III - DESCRIÇÃO DOS REQUISITOS DA CONTRATAÇÃO*: A solução a ser contratada deverá atender aos requisitos técnicos, operacionais e de segurança necessários à adequada proteção dos ativos de tecnologia da informação do Município de Santa Bárbara d'Oeste, observando os seguintes parâmetros fundamentais de qualidade, desempenho, conformidade legal e sustentabilidade:

1. **Padrões Mínimos de Qualidade, Desempenho e Interoperabilidade:** A solução integrada de segurança cibernética a ser contratada deve atuar na proteção de estações de trabalho, notebooks e servidores, devendo unificar as tecnologias de proteção antivírus baseada em assinaturas (Endpoint Protection) e detecção e resposta dinâmica a incidentes (EDR), além de possuir um módulo específico voltado à gestão preditiva e mapeamento de vulnerabilidades. Exige-se que a plataforma de software licitada possua arquitetura dotada de versatilidade híbrida nativa, demonstrando capacidade técnica de gerenciamento e operação tanto sob o modelo de nuvem pública (SaaS) quanto em infraestrutura local (On-Premise) a ser eventualmente implantada no datacenter do Município. O software deve assegurar compatibilidade integral com sistemas operacionais que constam nos equipamentos da rede municipal, englobando as versões vigentes e legadas do Microsoft Windows 7, 8, 8.1, 10 e 11, e Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022 ou superior. Na vertente de código aberto, o agente de segurança deve operar de forma homologada sobre as distribuições Debian GNU/Linux nas versões 11.x e 12.x; Ubuntu Server ou Desktop nas versões 20.04 e 22.04; e CentOS Stream nas versões 7.x, 8.x e 9.x. A solução proposta deverá também suportar as seguintes plataformas virtuais: VMware Workstation 17.0.2 Pro, VMware a partir de ESXi 6.7, e Microsoft Hyper-V a partir da versão 2012. Visando manter o isolamento lógico e a integridade fiduciária de sistemas de alta sensibilidade, a console administrativa da solução deve suportar o controle detalhado de privilégios com base em perfis de acesso customizáveis (RBAC) e permitir a integração com mecanismos corporativos de Single Sign-On (SSO) utilizando os protocolos NTLM e Kerberos. O agente instalado no endpoint deve incorporar mecanismos de autoproteção invioláveis e protegidos por senhas administrativas contra desativações não autorizadas por softwares maliciosos ou usuários locais. Além disso, a ferramenta deve executar varreduras em profundidade nas seções críticas de memória de estações Windows e do kernel em plataformas Linux, realizando a busca e a desinfecção de ameaças complexas, inclusive em arquivos compactados sob os formatos



RAR, ARJ, ZIP, CAB, LHA, JAR e ICE, mesmo que protegidos por criptografia ou senha. Para segurança das transações na internet, exige-se a capacidade de decifrar, inspecionar e filtrar o tráfego de rede criptografado sob os protocolos HTTPS, HTTP, SMTP e FTP. Na camada de controle periférico e de rede local, o sistema deve bloquear ou autorizar de forma seletiva o uso de tecnologias Bluetooth, dispositivos móveis, modems externos, unidades de CD/DVD, câmeras, scanners, MTPs e canais de transferência de dados por barramento USB, registrando operações de escrita e exclusão e impedindo o tráfego baseado em emulação de teclados por hardware. Devem estar integradas proteções avançadas contra ataques de falsificação de endereço de rede na camada de enlace (ARP Spoofing), mitigação ativa contra intrusões de rede (HIPS/Firewall com filtragem por TTL), bloqueio de ameaças sem arquivo físico (fileless), controle de execução de scripts de administração em ambiente PowerShell, e contenção imediata de criptografia remota ou ataques semelhantes a ransomware em recursos de rede compartilhados, com o bloqueio temporário automático do host atacante.

2. Nível de Serviço e Suporte Técnico: O suporte técnico especializado será prestado de forma continuada, adotando-se um modelo de atendimento híbrido estruturado de acordo com a gravidade dos incidentes de segurança cibernética. Para as demandas ordinárias, consultas técnicas de rotina, esclarecimento de dúvidas operacionais ou apoio na parametrização de políticas de segurança na console de gerenciamento, o atendimento remoto e telefônico ocorrerá em horário comercial, compreendido entre as 8h e as 18h, de forma ininterrupta, nos dias úteis. Em contrapartida, em situações de extrema gravidade em que os serviços de segurança ou monitoramento fiquem totalmente indisponíveis (Severidade 1), o suporte técnico operará em regime ininterrupto de plantão de vinte e quatro horas por dia, sete dias por semana (24x7). Este atendimento especializado será prestado por intermédio de Centro de Operações de Rede (NOC) físico instalado em território nacional, garantindo atendimento obrigatório em idioma português e observando os estritos tempos de início e encerramento de chamados parametrizados na matriz de severidade do Termo de Referência (início do atendimento em até 2 horas úteis e término do atendimento em no máximo 8 horas corridas para Severidade 1).

3. Regulamentações Específicas e Segurança da Informação: A solução e a execução dos serviços deverão observar estritamente os ditames da Lei Geral de Proteção de Dados Pessoais (LGPD – Lei Federal nº 13.709/2018) e do Marco Civil da Internet (Lei Federal nº 12.965/2014), assegurando o sigilo, a confidencialidade e a rastreabilidade no tratamento dos dados e logs coletados. Devem ser seguidas, ainda, as boas práticas internacionais de governança de TI e segurança da informação (tais como as normas da família ISO/IEC 27000).



4. Critérios e Práticas de Sustentabilidade: Em consonância com os critérios para Contratações Sustentáveis, a contratação adota a sustentabilidade sob a vertente da otimização de recursos e eficiência energética. A arquitetura flexível da console (prioritariamente operada em nuvem pública no modelo SaaS) elimina a necessidade de o Município adquirir, manter, climatizar e gerenciar novos servidores físicos em seu datacenter para a proteção geral do parque, diminuindo o consumo de energia elétrica de forma sintonizada com os critérios de sustentabilidade socioambiental. Adicionalmente, o fornecimento por meio de licenciamento digital extingue a produção e descarte de mídias físicas e embalagens plásticas, enquanto o agente de proteção deve ser otimizado para apresentar baixo consumo de recursos de hardware (CPU e memória) nos endpoints, prolongando a vida útil tecnológica dos computadores atuais da Prefeitura e reduzindo o descarte precoce de lixo eletrônico.

IV - ESTIMATIVA DAS QUANTIDADES PARA CONTRATAÇÃO*: A estimativa quantitativa dos ativos e serviços que compõem o escopo desta contratação foi balizada pelo inventário oficial de Tecnologia da Informação do Município e reflete as necessidades integradas das Secretarias de Administração, Saúde e Educação.

V - LEVANTAMENTO DE MERCADO*: Para a definição da arquitetura tecnológica da solução, a Administração Municipal avaliou as seguintes opções e cenários disponíveis no mercado:

1. Opções Avaliadas: Modelo Exclusivo Local (On-Premise): Consiste na instalação obrigatória da console de gerenciamento dentro da infraestrutura interna do Município. Este cenário exigiria a aquisição ou alocação dedicada de novos servidores físicos, storages, memória e licenças de sistemas operacionais de servidores. Além disso, demandaria custos contínuos com manutenção de hardware, refrigeração de datacenter e suporte técnico local, mantendo o risco de indisponibilidade da gestão de segurança caso a rede interna da Prefeitura sofresse incidentes físicos ou lógicos. Modelo de Console Híbrido (Versatilidade Cloud e On-Premise): Consiste em uma plataforma de segurança flexível que suporta, nativamente, tanto a console em nuvem pública (SaaS) quanto a console instalada localmente (On-Premise), operando de forma integrada.

2. Justificativa do Modelo Tecnológico Adotado: A escolha recaiu sobre uma plataforma dotada de versatilidade e arquitetura híbrida, que permite a orquestração do console de gerenciamento tanto em nuvem pública quanto em servidor local. Esta modelagem estratégica visa equilibrar as vantagens operacionais do modelo Software as a Service (SaaS) com as severas exigências de segurança de rede da infraestrutura de tecnologia municipal. Para o parque tecnológico geral que atende às demandas administrativas cotidianas das Secretarias de Administração, Saúde e Educação, o console baseado em



nuvem será prioritariamente empregado. Essa abordagem se traduz em significativa economicidade e eficiência técnica, haja vista que elimina a necessidade de o Município adquirir, manter, climatizar e gerenciar novos servidores físicos em seu datacenter para hospedar a aplicação central, diminuindo o consumo de energia elétrica de forma perfeitamente sintonizada com os critérios de sustentabilidade socioambiental. Adicionalmente, o console hospedado em nuvem assegura resiliência operacional total, garantindo que a equipe de tecnologia da informação acesse as ferramentas de segurança e realize a resposta a incidentes a partir de qualquer conexão à rede, resguardando o controle da segurança mesmo em casos de blecautes ou desastres físicos nos prédios públicos locais. Paralelamente, o suporte nativo à instalação de consoles de gerenciamento locais (on-premise) e a compatibilidade com servidores locais de bancos de dados (Microsoft SQL Server, Azure SQL, MySQL, MariaDB e PostgreSQL) são exigências técnicas essenciais para viabilizar a proteção de zonas desmilitarizadas (DMZ) e de redes locais de alta segurança operadas pelo Município. Diversas unidades municipais de saúde, escolas e prédios da prefeitura gerenciam prontuários eletrônicos, dados orçamentários críticos e biometria de usuários em servidores locais protegidos que, por razões de conformidade de segurança e controle de dados pessoais, não dispõem de tráfego direto de saída para a internet pública. Para essas sub-redes isoladas, a consolidação híbrida da ferramenta de segurança permite a implantação de um mediador de conexão unidirecional ou servidor local de retransmissão de atualizações e reputação de assinaturas de malware. Essa capacidade otimiza significativamente o uso de largura de banda de internet de toda a municipalidade ao evitar o download individual de pacotes diferenciais de vírus por cada um dos 1.500 equipamentos da rede diretamente das nuvens globais, garantindo uma logística de dados interna limpa, eficiente e de baixo custo operacional.

VI - ESTIMATIVA DO VALOR DA CONTRATAÇÃO*: A estimativa do valor econômico para a presente contratação foi realizada por meio de ampla pesquisa de preços, através da Plataforma Fonte de Preço. Utilizou-se como método matemático para a definição do valor estimado a mediana dos preços obtidos no mercado, mitigando distorções de valores extremos.

VII - DESCRIÇÃO DA SOLUÇÃO COMO UM TODO*: A solução estratégica definida para o atendimento unificado das Secretarias Municipais de Administração, Saúde e Educação consiste na contratação de empresa especializada para o fornecimento integrado de ferramentas de segurança da informação para proteção de endpoints, contemplando antivírus (Endpoint Protection), detecção e resposta a incidentes (EDR) e módulo de gestão e análise de vulnerabilidades, com gerenciamento híbrido versátil (nuvem/local). A contratação compreende, além do licenciamento das ferramentas, um conjunto



de serviços técnicos especializados indissociáveis, estruturados da seguinte forma:

1. Licenciamento e Escopo Funcional (Subscrição por 24 Meses): Volumetria: Fornecimento de 1.500 licenças de uso simultâneas (computadas como 3.000 unidades na métrica de faturamento anual do período de 2 anos) para a proteção integral de computadores de mesa, notebooks e servidores do Município. Operação e Monitoramento: A solução deverá operar com monitoramento contínuo do ambiente computacional, com alta capacidade de detecção, prevenção e resposta a ameaças cibernéticas em tempo real, garantindo a proteção dos ativos tecnológicos, a integridade, a confidencialidade e a disponibilidade das informações corporativas e a estrita continuidade dos serviços públicos digitais entregues à população.

2. Serviços Técnicos Integrados: Implantação e Configuração Inicial: Execução do planejamento e parametrização inicial das políticas de segurança na console, com a consequente homologação do ambiente técnico do Município. Migração do Ambiente Existente: Desinstalação segura e completa das ferramentas antivírus legadas atualmente ativas no parque tecnológico da Prefeitura e a instalação automatizada e gradativa do novo agente, mitigando riscos de janelas de vulnerabilidade ou conflitos de software. Treinamento da Equipe: Realização de capacitação prática para os servidores da Divisão de TI do Município, assegurando a transferência de conhecimento necessária para a operação diária, extração de relatórios e monitoramento de alertas.

3. Manutenção, Assistência Técnica e Suporte (Período de 24 Meses): Prestação de serviços de suporte técnico especializado durante toda a vigência contratual, incluindo: Atualizações contínuas e em tempo real das bases de proteção. Correções evolutivas e corretivas de bugs ou falhas lógicas da ferramenta. Atendimento técnico por meio de suporte remoto e, quando a criticidade do incidente assim exigir, atendimento presencial (on-site) com SLA predefinido.

VIII - JUSTIFICATIVA PARA O PARCELAMENTO OU NÃO DA CONTRATAÇÃO*: Em estrita observância ao art. 40, § 2º, da Lei Federal nº 14.133/2021, a presente contratação não será parcelada, sendo adotado o modelo de adjudicação por Lote Único Global. A decisão de não parcelar o objeto fundamenta-se nos seguintes aspectos técnicos e jurídicos:

1. Inviabilidade Técnica e Interdependência do Objeto: O objeto consiste no fornecimento de uma solução integrada de segurança da informação, composta por ferramentas e módulos nativamente interdependentes — Endpoint Protection (EPP), Detecção e Resposta a Incidentes (EDR) e Gestão de Vulnerabilidades. A eficácia prática e a resiliência cibernética de toda a infraestrutura tecnológica



do Município dependem obrigatoriamente de uma operação unificada, com gerenciamento centralizado em uma console unificada de administração (Single Console).

2. Riscos à Eficiência Administrativa e à Segurança da Informação: O parcelamento da contratação (como a aquisição de licenças separadas dos serviços, ou de módulos de fabricantes distintos) comprometeria gravemente a eficiência e a efetividade da proteção digital das Secretarias solicitantes. A fragmentação dificultaria a integração nativa entre os módulos de detecção; a correlação automatizada de eventos e alertas de segurança em tempo real; o compartilhamento imediato de informações de inteligência de ameaças entre as camadas de proteção; e a resposta rápida e coordenada a incidentes cibernéticos complexos (como ataques de ransomware).

3. Complexidade Operacional e Responsabilização: A divisão do objeto aumentaria drasticamente a complexidade de gerenciamento por parte da Divisão de TI do Município e traria imensos riscos de incompatibilidade técnica entre soluções de diferentes fornecedores. Ademais, sob a vertente jurídica e contratual, o não parcelamento assegura o princípio da responsabilidade única (Single Point of Contact), evitando o cruzamento de culpas entre empresas distintas em caso de falhas na implantação, brechas de segurança ou indisponibilidade nos sistemas públicos digitais.

IX - DEMONSTRATIVO DOS RESULTADOS PRETENDIDOS*: A contratação da solução integrada de segurança da informação visa alcançar os seguintes resultados de interesse público, divididos por suas respectivas dimensões de impacto:

1. Eficiência Econômica e Governança: Proporcionar maior economicidade na gestão dos recursos públicos por meio da adoção de uma ferramenta unificada, gerando uma expressiva redução de custos operacionais e administrativos que hoje seriam necessários para a manutenção, suporte e renovação de múltiplas soluções isoladas. Consolidar funcionalidades em uma única plataforma, eliminando o retrabalho, reduzindo custos ocultos de TI e elevando o nível de governança corporativa no âmbito da Administração Municipal.

2. Continuidade e Segurança dos Serviços Públicos: Promover uma melhoria significativa na proteção dos ativos tecnológicos do Município, mitigando drasticamente os riscos de incidentes cibernéticos graves. Evitar a indisponibilidade de sistemas institucionais e a perda de dados críticos, assegurando de forma contínua a confiabilidade, a confidencialidade e a segurança dos serviços públicos digitais prestados à população barbareense.



4. Otimização Operacional da Equipe de TI: Permitir o melhor aproveitamento dos recursos humanos da Divisão de TI, por meio da automação dos processos de detecção, análise de assinaturas e resposta imediata a incidentes de segurança. Garantir à equipe técnica total visibilidade, controle e rastreabilidade dos eventos de segurança em todo o ambiente tecnológico das Secretarias de Administração, Saúde e Educação, otimizando o tempo de resposta e a eficiência nas tomadas de decisão.

4. Maturidade Estratégica e Resiliência Cibernética: Fortalecer de maneira sustentável a postura de segurança cibernética da Prefeitura Municipal, dotando-a de maior capacidade preditiva, preventiva e reativa contra ameaças digitais complexas. Reduzir a superfície de risco cibernético do ecossistema municipal, elevando o grau de maturidade institucional frente às exigências e diretrizes da Lei Geral de Proteção de Dados (LGPD).

X - PROVIDÊNCIAS A SEREM ADOTADAS*: Para assegurar a adequada execução, controle e eficácia do objeto a ser contratado, a Administração Municipal de Santa Bárbara d'Oeste deverá adotar, previamente e durante a celebração do contrato, as seguintes providências administrativas e operacionais:

1. Gestão e Fiscalização da Contratação: Realizar a indicação e designação formal, por meio de ato próprio, do Gestor e do Fiscal do contrato, em estrita observância ao art. 117 da Lei Federal nº 14.133/2021. Definir claramente as atribuições de cada agente público na fiscalização das entregas e na validação das faturas.

2. Capacitação e Alinhamento das Equipes: Providenciar a capacitação básica e o alinhamento dos servidores públicos envolvidos na operacionalização e fiscalização do contrato. Essa preparação focará especificamente nas características técnicas da ferramenta de EPP/EDR, no entendimento das métricas de Nível de Serviço (SLA) estipuladas e nos mecanismos formais de acompanhamento e notificação da execução contratual.

3. Infraestrutura e Liberação de Acessos: Garantir previamente a disponibilidade da infraestrutura interna mínima e dos privilégios de acesso necessários nos servidores e redes para a instalação do console em nuvem e distribuição do agente único (single agent). Coordenar o alinhamento interno entre as equipes técnicas das Secretarias de Administração, Saúde e Educação para o cronograma das atividades de migração, desinstalação do antivírus legado e homologação da nova solução, assegurando condições adequadas para o pleno cumprimento do objeto sem interrupção das rotinas administrativas do Município.



XI - **CONTRATAÇÕES CORRELATAS E/OU INTERDEPENDENTES***: Não foram identificadas contratações correlatas em andamento ou planejadas com objeto similar ou correspondente à presente contratação. Da mesma forma, não se verificam contratações interdependentes que influenciem ou sejam influenciadas pela execução do objeto, sendo a solução de segurança da informação autônoma quanto à sua implantação e operação. Ressalta-se que a solução poderá integrar-se ao ambiente tecnológico existente da Administração, sem depender de contratações adicionais para o pleno atendimento da necessidade, garantindo sua implementação de forma independente e eficaz.

XII - **DESCRIÇÃO DE POSSÍVEIS IMPACTOS AMBIENTAIS***: A presente contratação apresenta impacto ambiental extremamente reduzido e positivo sob a vertente da sustentabilidade ecológica e eficiência energética, devido às seguintes características intrínsecas do objeto.

1. **Arquitetura em Nuvem e Eficiência Energética**: Por tratar-se de uma solução baseada prioritariamente com hospedagem na nuvem. Essa abordagem elimina a necessidade de aquisição, instalação e manutenção de novos servidores físicos ou storages locais de grande porte dedicados no Datacenter do Município para essa console, o que evita o aumento do consumo de energia elétrica com alimentação e refrigeração de hardware local, reduzindo a pegada de carbono da Administração Municipal.

2. **Otimização de Recursos e Logística Verde**: O fornecimento das 1.500 licenças dar-se-á por meio puramente digital (via chaves de ativação e downloads), extinguindo a necessidade de produção, transporte e posterior descarte de mídias físicas (CDs/DVDs), manuais impressos e embalagens plásticas. Além disso, a especificação de um agente único leve (single agent) garante o uso racional do hardware atual, evitando a obsolescência tecnológica precoce das estações de trabalho e notebooks das Secretarias de Administração, Saúde e Educação, prolongando a vida útil dos equipamentos existentes e reduzindo a geração de lixo eletrônico (e-waste).

XIII - **POSICIONAMENTO CONCLUSIVO SOBRE A ADEQUAÇÃO DE CONTRATAÇÃO PARA O ATENDIMENTO DA NECESSIDADE A QUE SE DESTINA***: Diante de todo o detalhamento técnico e mercadológico compilado no presente instrumento, e em estrita consonância com o preconizado pelo art. 18, § 1º, inciso XIII, da Lei Federal nº 14.133/2021 e regulamentos editados pelo Decreto Municipal nº 14.354/2023 de Santa Bárbara d'Oeste, declara de forma motivada que a contratação de empresa para o fornecimento de solução integrada de Endpoint Protection e Detecção e Resposta a Incidentes (EDR) revela-se plenamente viável, oportuna e de elevado interesse público.



Município de Santa Bárbara d'Oeste

ISSO POSTO, ENCAMINHO O PRESENTE ETP PARA APROVAÇÃO SECRETARIAL, NOS TERMOS DO DISPOSTO NO ART. 4º DO DECRETO MUNICIPAL Nº 7508/2023.



Município de Santa Bárbara d'Oeste

ANEXO II- PLANILHA PROPOSTA

ITEM	CÓDIGO	DESCRIÇÃO	UNIDADE DE MEDIDA	QTDE	VALOR UNITÁRIO R\$	VALOR TOTAL R\$
1	2.01.02.0069.6	Licença proteção antivírus Endpoint Protection e EDR	Unidade x anual	3.000 (1.500 x 2 anos)		
2	2.01.02.0076.9	Migração e implantação da proteção antivírus (Endpoint Protection)	Unidade	01		
3	2.01.02.0077.7	Treinamento proteção antivírus Endpoint Protection	Unidade	01		
4	2.01.02.0078.5	Suporte técnico em proteção antivírus Endpoint Protection	Anual	02		
Valor Total da Contratação						

Valor Total da Proposta por extenso:

(_____)

Declaro que os preços apresentados contemplam todos os custos diretos e indiretos incorridos na data da apresentação da proposta, incluindo, dentre outros: tributos, encargos sociais, material, despesas administrativas, seguro, frete e lucro.

Declaro que os serviços ofertados atendem a todas as especificações exigidas no Termo de Referência - Anexo I do Edital.

Santa Bárbara d' Oeste, de _____ 2.026.

DADOS DA PROPONENTE:

Nome:

Razão Social:

Endereço completo

Telefone/E-mail:

Validade da Proposta: Não inferior a 60 dias



Município de Santa Bárbara d'Oeste

Representante Legal

Cargo

RG:



ANEXO III- MINUTA TERMO DE CONTRATO

PREGÃO ELETRÔNICO 52/2026 PROCESSO ADMINISTRATIVO 8144/2026

Contratação de empresa para a prestação de serviços de

.....

O Município de Santa Bárbara d'Oeste, com sede na Avenida Monte Castelo, nº 1.000, na cidade de Santa Bárbara d'Oeste/SP, inscrito(a) no CNPJ sob o nº 46.422.408/0001-52, neste ato representado por **RAFAEL PIOVEZAN**, Prefeito Municipal e **MONICA MOSNA**, Secretária Municipal de Administração, **TÂNIA MARA DA SILVA**, Secretária Municipal de Educação e **MARCUS PENSUTI**, Secretário Municipal de Saúde, doravante denominado CONTRATANTE, e o(a), inscrito(a) no CNPJ/MF sob o nº, sediado(a) na, doravante designado CONTRATADO, neste ato representado(a) 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 8144/2026, e em observância às disposições da Lei nº 14.133, de 1º de abril de 2021, e demais legislação aplicável, resolvem celebrar o presente Termo de Contrato, decorrente do Pregão Eletrônico nº 52/2026, mediante as cláusulas e condições a seguir enunciadas.

CLÁUSULA PRIMEIRA – OBJETO

1.1. O objeto da presente licitação é a contratação de empresa para prestação de serviços de fornecimento de solução de segurança da informação, englobando licenças de uso Endpoint Protection (antivírus), solução de detecção e resposta de endpoint (EDR), instalação, migração, manutenção, treinamento e suporte técnico, conforme constante no Anexo I- Termo de Referência.

1.2. Vinculam esta contratação, independentemente de transcrição:

- 1.2.1.** O Termo de Referência;
- 1.2.2.** O Edital da Licitação;
- 1.2.3.** A Proposta do Contratado;
- 1.2.4.** Eventuais anexos dos documentos supracitados.



CLÁUSULA SEGUNDA – VIGÊNCIA E PRORROGAÇÃO

- 2.1** O prazo de vigência da contratação é de 24 (vinte e quatro) meses, contados da assinatura do contrato, podendo ser prorrogado nos termos na lei vigente.
- 2.2** O Contratado não tem direito subjetivo à prorrogação contratual.
- 2.3** A prorrogação de contrato poderá ser promovida mediante celebração de termo aditivo.
- 2.4** O contrato não poderá ser prorrogado quando o Contratado tiver sido penalizado nas sanções de declaração de inidoneidade ou impedimento de licitar e contratar com poder público, observadas as abrangências de aplicação.

CLÁUSULA TERCEIRA – MODELOS DE EXECUÇÃO E GESTÃO CONTRATUAIS

- 3.1** O regime de execução contratual, os modelos de gestão e de execução, assim como os prazos e condições de conclusão, entrega, observação e recebimento do objeto constam no Termo de Referência, anexo a este Contrato.

CLÁUSULA QUARTA – SUBCONTRATAÇÃO

- 4.1** Não será admitida a subcontratação do objeto contratual.

CLÁUSULA QUINTA – PREÇO

- 5.1** O valor total da contratação é de R\$..... (.....).
- 5.2** 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.
- 5.3** O valor acima é meramente estimativo, de forma que os pagamentos devidos ao Contratado dependerão dos quantitativos efetivamente fornecidos.



CLÁUSULA SEXTA - PAGAMENTO

6.1. O pagamento devido à Contratada será efetuado em conformidade com os prazos, critérios e condições estabelecidos no Termo de Referência, anexo integrante deste Instrumento.

6.2. O pagamento ficará condicionado à regular apresentação do documento fiscal correspondente, devidamente atestado pelo setor competente, bem como à comprovação da regularidade fiscal da Contratada.

CLÁUSULA SÉTIMA – REAJUSTAMENTO

7.1 Nos termos do artigo 92, inciso V, e §§ 3º e 4º, inciso I, os preços inicialmente Contratados são fixos e irrevogáveis no prazo de um ano contado da data do orçamento estimado, em __/__/__ (DD/MM/AAAA).

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

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

7.4 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).

7.5 Nas aferições finais, o(s) índice(s) utilizado(s) para reajuste será(ão), obrigatoriamente, o(s) definitivo(s).

7.6 Caso o(s) índice(s) estabelecido(s) para reajustamento venha(m) a ser extinto(s) ou de qualquer forma não possa(m) mais ser utilizado(s), será(ão) adotado(s), em substituição, o(s) que vier(em) a ser determinado(s) pela legislação então em vigor.

7.7 Cuidando-se de contrato de serviços contínuos, sem regime de dedicação exclusiva de mão de obra ou predominância desta, o reajustamento será em sentido estrito, mediante previsão de índices específicos ou setoriais (IPC-FIPE), nos termos do artigo 92, § 4º inciso I.



CLÁUSULA OITAVA - OBRIGAÇÕES DO CONTRATANTE

8.1 São obrigações do Contratante:

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

8.1.2 Receber o objeto no prazo e condições estabelecidas no Termo de Referência;

8.1.3 Notificar o Contratado, por escrito, sobre vícios, defeitos ou incorreções verificadas no serviço prestado, para que seja por ele reparado ou corrigido, no total ou em parte, às suas expensas;

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

8.1.5 Efetuar o pagamento ao Contratado do valor correspondente ao fornecimento do objeto, no prazo, forma e condições estabelecidos no presente Contrato e no Termo de Referência.

8.1.6 Aplicar ao Contratado as sanções previstas na lei e neste Contrato;

8.1.7 Disponibilizar todas as informações e os meios necessários para que ocorra o fiel cumprimento das disposições existentes;

8.1.8 Autorizar os serviços e emitir os documentos específicos para tal;

8.1.9 Exercer a fiscalização dos serviços por servidores especialmente designados, conforme especificado na Lei n. 14133/21.

8.1.10 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.

8.1.11 Notificar os emitentes das garantias quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais.

8.1.12 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 NONA - OBRIGAÇÕES DO CONTRATADO

9.1 O Contratado deve cumprir todas as obrigações constantes deste Contrato e em seus anexos, assumindo como exclusivamente seus os riscos e



Município de Santa Bárbara d'Oeste

as despesas decorrentes da boa e perfeita execução do objeto, observando, ainda, as obrigações a seguir dispostas:

9.2 Responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com o Código de Defesa do Consumidor (Lei nº 8.078, de 1990);

9.3 Comunicar ao contratante, no prazo máximo de 24 (vinte e quatro) horas que antecede a data da entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação;

9.4 Atender às determinações regulares emitidas pelo fiscal ou gestor do contrato ou autoridade superior (art. 137, II, da Lei n.º 14.133, de 2021) e prestar todo esclarecimento ou informação por eles solicitados;

9.5 Reparar, corrigir ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os serviços nos quais se verificarem vícios ou incorreções resultantes da execução;

9.6 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, o valor correspondente aos danos sofridos;

9.7 O contratado deverá entregar ao setor responsável pela fiscalização do contrato, junto com a Nota Fiscal para fins de pagamento, os seguintes documentos:

- 1) Prova de regularidade relativa à Seguridade Social;
- 2) Certidão conjunta relativa aos tributos federais e à Dívida Ativa da União;
- 3) Certidões que comprovem a regularidade perante a Fazenda Estadual ou Distrital do domicílio ou sede do contratado;
- 4) Certidão de Regularidade do FGTS – CRF; e
- 5) Certidão Negativa de Débitos Trabalhistas – CNDT;

9.8 Responsabilizar-se pelo cumprimento de todas as obrigações trabalhistas, previdenciárias, fiscais, comerciais e as demais previstas em legislação específica, cuja inadimplência não transfere a responsabilidade ao contratante e não poderá onerar o objeto do contrato;

9.9 Comunicar ao Fiscal do contrato, no prazo de 24 (vinte e quatro) horas, qualquer ocorrência anormal ou acidente que se verifique no local da execução do objeto contratual.



9.10 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.

9.11 Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições exigidas para habilitação na licitação;

9.12 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, da Lei n.º 14.133, de 2021);

9.13 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, da Lei n.º 14.133, de 2021);

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

9.15 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.

9.16 Cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança do contratante;

9.17 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.

9.18 **Orientar e treinar seus empregados** sobre os deveres previstos na Lei nº 13.709, de 14 de agosto de 2018, adotando medidas eficazes para proteção de dados pessoais a que tenha acesso por força da execução deste contrato.

9.19 Conduzir os trabalhos com estrita observância às normas da legislação pertinente, cumprindo as determinações do Município, nas melhores condições de segurança, higiene e disciplina.



9.20 Submeter previamente, por escrito, ao contratante, para análise e aprovação, quaisquer mudanças nos métodos executivos que fujam às especificações do Termo de Referência.

9.21 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.

9.22 A Contratada obriga-se a atuar no presente contrato em conformidade com a Legislação vigente sobre Proteção de Dados (Lei Federal 13.709 de 2018).

9.23 A **CONTRATADA em situação de recuperação judicial/extrajudicial** deverá apresentar certidão negativa de feitos sobre falência, expedida pelo distribuidor da sede do licitante, conforme Art. 69, Inciso II da Lei 14.133/21.

9.24 Manter ao longo da vigência do Contrato junto ao MSBO, todas as informações necessárias ao fiel cumprimento da mesma, em especial, qualquer alteração relacionada ao seu contrato social, endereço, telefone e e-mail, devendo o MSBO ser informado das eventuais alterações ocorridas, no prazo máximo de 05 (cinco) dias, contados da efetiva alteração.

9.25 A Contratada deverá observar, com rigor, os termos do Decreto Municipal nº 7.468/23 e Anexo Único (Anexo VIII), sob pena de não pagamento dos valores devidos.

9.26 Cumprir todas as demais exigências e especificações referentes à prestação dos serviços constantes do Termo de Referência- Anexo I.

CLÁUSULA DÉCIMA– GARANTIA DE EXECUÇÃO

10.1 Não haverá exigência de garantia contratual da execução.

CLÁUSULA DÉCIMA PRIMEIRA– INFRAÇÕES E SANÇÕES ADMINISTRATIVAS

11.1 Comete infração administrativa, nos termos da Lei nº 14.133, de 2021, o Contratado que:

- a) der causa à inexecução parcial do contrato;



- b) der causa à inexecução parcial do contrato que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo;
- c) der causa à inexecução total do contrato;
- d) ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;
- e) apresentar documentação falsa ou prestar declaração falsa durante a execução do contrato;
- f) praticar ato fraudulento na execução do contrato;
- g) comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;
- h) praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.

11.2 Serão aplicadas ao Contratado que incorrer nas infrações acima descritas as seguintes sanções;

- a) **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 nº 14.133, de 2021);
- b) **Impedimento de licitar e contratar**, quando praticadas as condutas descritas nas alíneas “b”, “c” e “d” do subitem acima deste Contrato, sempre que não se justificar a imposição de penalidade mais grave (art. 156, § 4º, da Lei nº 14.133, de 2021);
- c) **Declaração de inidoneidade para licitar e contratar**, quando praticadas as condutas descritas nas alíneas “e”, “f”, “g” e “h” do subitem acima deste Contrato, bem como nas alíneas “b”, “c” e “d”, que justifiquem a imposição de penalidade mais grave (art. 156, §5º, da Lei nº 14.133, de 2021).

d) **Multa:**

1. Moratória de 0,1% (zero vírgula um por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 10 (dez) dias;
2. Moratória de 0,5% (zero vírgula cinco por cento) por dia de atraso injustificado sobre o valor total do contrato, até o máximo de 1% (um por



cento), pela inobservância do prazo fixado para apresentação, suplementação ou reposição da garantia.

i.O atraso superior a 10 (dez) dias injustificado, autoriza a Administração a promover a extinção do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõe o inciso I do art. 137 da Lei n. 14.133, de 2021.

11.3 A aplicação das sanções previstas neste Contrato não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao Contratante (art. 156, §9º, da Lei nº 14.133, de 2021)

11.3.1 Todas as sanções previstas neste Contrato poderão ser aplicadas cumulativamente com a multa (art. 156, §7º, da Lei nº 14.133, de 2021).

11.3.2 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, da Lei nº 14.133, de 2021).

11.3.3 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, da Lei nº 14.133, de 2021).

11.3.4 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.

11.4 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.

11.5 Na aplicação das sanções serão considerados (art. 156, §1º, da Lei nº 14.133, de 2021):

- a) a natureza e a gravidade da infração cometida;
- b) as peculiaridades do caso concreto;
- c) as circunstâncias agravantes ou atenuantes;



- d) os danos que dela provierem para o Contratante;
- e) a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

11.6 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).

11.7 A personalidade jurídica do Contratado poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste Contrato ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o Contratado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia (art. 160, da Lei nº 14.133, de 2021).

11.8 O Contratante deverá, no prazo máximo de 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ela aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e no Cadastro Nacional de Empresas Punidas (Cnep), instituídos no âmbito do Poder Executivo Federal. (Art. 161, da Lei nº 14.133, de 2021).

11.9 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.

11.10 Os débitos do Contratado para com a Administração Contratante, resultantes de multa administrativa e/ou indenizações, não inscritos em dívida ativa, poderão ser compensados, total ou parcialmente, com os créditos devidos pelo referido órgão decorrentes deste mesmo contrato ou de outros contratos administrativos que o Contratado possua com o mesmo órgão ora Contratante, na forma da Instrução Normativa SEGES/ME nº 26, de 13 de abril de 2022.

CLÁUSULA DÉCIMA SEGUNDA – DOTAÇÃO ORÇAMENTÁRIA

12.1 As despesas decorrentes da presente licitação deverão onerar a Unidade Orçamentária: 02.01.02– Planejamento Estratégico; 02.02.01 – Educação



Infantil; 02.02.02 – Ensino Fundamental; 02.0.3.01 – Saúde Geral- Natureza de Despesa: 3.3.90.40.00 – Outros Serviços da Tecnologia da Informação e Comunicação- PJ - Vínculo 01 – Próprio, suplementadas, se necessário.

CLÁUSULA DÉCIMA TERCEIRA – DOS CASOS OMISSOS

13.1 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 QUARTA – ALTERAÇÕES

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

14.2 O Contratado é obrigado 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.

14.3 As alterações contratuais deverão ser promovidas mediante celebração de termo aditivo, submetido à prévia aprovação da consultoria jurídica do Contratante, salvo nos casos de justificada necessidade de antecipação de seus efeitos, hipótese em que a formalização do aditivo deverá ocorrer no prazo máximo de 1 (um) mês (art. 132 da Lei nº 14.133, de 2021).

14.4 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 QUINTA – PUBLICAÇÃO

15.1 Incumbirá ao Contratante divulgar o presente instrumento no Portal Nacional de Contratações Públicas (PNCP), na forma prevista no art. 94 da Lei 14.133, de 2021, bem como no respectivo sítio oficial na Internet, em atenção ao art. 91, *caput*, da Lei n.º 14.133, de 2021, e ao art. 8º, §2º, da Lei n. 12.527, de 2011, c/c art. 7º, §3º, inciso V, do Decreto n. 7.724, de 2012.

CLÁUSULA DÉCIMA SEXTA– FORO



Município de Santa Bárbara d'Oeste

16.1 Fica eleito o Foro da Comarca de Santa Bárbara d'Oeste para dirimir os litígios que decorrerem da execução deste Termo de Contrato que não puderem ser compostos pela conciliação, conforme art. 92, §1º, da Lei nº 14.133/21.

Santa Bárbara d'Oeste, ____ de _____ de 2026.

MONICA MOSNA
Secretária Municipal de Administração

TÂNIA MARA DA SILVA
Secretária Municipal de Educação

MARCUS PENSUTI
Secretário Municipal de Saúde

RAFAEL PIOVEZAN
Prefeito Municipal

CONTRATADO



**ANEXO IV - TERMO DE CIÊNCIA E DE NOTIFICAÇÃO (CONTRATOS)
(REDAÇÃO DADA PELA RESOLUÇÃO Nº 11/2021)**

**CONTRATANTE:
CONTRATADO:
LICITAÇÃO:
CONTRATO Nº
OBJETO:**

Pelo presente TERMO, nós, abaixo identificados:

1. Estamos CIENTES de que:

- a) O ajuste acima referido, seus aditamentos, bem como o acompanhamento de sua execução contratual, estarão sujeitos a análise e julgamento pelo Tribunal de Contas do Estado de São Paulo, cujo trâmite processual ocorrerá pelo sistema eletrônico;
- b) Poderemos ter acesso ao processo, tendo vista e extraindo cópias das manifestações de interesse, Despachos e Decisões, mediante regular cadastramento no Sistema de Processo Eletrônico, em consonância com o estabelecido na Resolução nº 01/2011 do TCESP;
- c) Além de disponíveis no processo eletrônico, todos os Despachos e Decisões que vierem a ser tomados, relativamente ao aludido processo, serão publicados no Diário Oficial do Estado, Caderno do Poder Legislativo, parte do Tribunal de Contas do Estado de São Paulo, em conformidade com o artigo 90 da Lei Complementar nº 709, de 14 de janeiro de 1993, iniciando-se, a partir de então, a contagem dos prazos processuais, conforme regras do Código de Processo Civil;
- d) As informações pessoais dos responsáveis pelo Contratante e interessados estão cadastradas no módulo eletrônico do “Cadastro Corporativo TCESP – CadTCESP”, nos termos previstos no Artigo 2º das Instruções nº01/2020, conforme “Declaração(ões) de Atualização Cadastral” anexa(s);
- e) É de exclusiva responsabilidade do Contratado manter seus dados sempre atualizados.

2. Damo-nos por NOTIFICADOS para:



Município de Santa Bárbara d'Oeste

- a) O acompanhamento dos atos do processo até seu julgamento final e consequente publicação;
- b) Se for o caso e de nosso interesse, nos prazos e nas formas legais e regimentais, exercer o direito de defesa, interpor recursos e o que mais couber.

Santa Bárbara d'Oeste,

AUTORIDADE MÁXIMA DO ÓRGÃO/ENTIDADE:

Nome:

Cargo:

CPF:

RESPONSÁVEIS PELA HOMOLOGAÇÃO DO CERTAME OU RATIFICAÇÃO DA LICITAÇÃO:

Nome:

Cargo:

CPF:

RESPONSÁVEIS QUE ASSINARAM O AJUSTE:

Pelo CONTRATANTE:

Nome:

Cargo:

CPF:

Pelo CONTRATANTE:

Nome:

Cargo:

CPF:

Pela CONTRATADA:

Nome:

Cargo:

CPF:

ORDENADOR DE DESPESAS DA CONTRATANTE:

Nome:

Cargo:

CPF:



Município de Santa Bárbara d'Oeste

GESTOR(ES) DO CONTRATO:

Nome:

Cargo:

CPF:

DEMAIS RESPONSÁVEIS (*):

Tipo de ato sob sua responsabilidade: _____

Nome: _____

Cargo: _____

CPF: _____

Assinatura: _____

(*) - O Termo de Ciência e Notificação e/ou Cadastro do(s) Responsável(is) deve identificar as pessoas físicas que tenham concorrido para a prática do ato jurídico, na condição de ordenador da despesa; de partes Contratantes; de responsáveis por ações de acompanhamento, monitoramento e avaliação; de responsáveis por processos licitatórios; de responsáveis por prestações de contas; de responsáveis com atribuições previstas em atos legais ou administrativos e de interessados relacionados a processos de competência deste Tribunal. Na hipótese de prestações de contas, caso o signatário do parecer conclusivo seja distinto daqueles já arrolados como subscritores do Termo de Ciência e Notificação, será ele objeto de notificação específica. *(inciso acrescido pela Resolução nº 11/2021).*



ANEXO V- MODELO DECLARAÇÃO DE FATOS IMPEDITIVOS

AO

MUNICÍPIO DE SANTA BÁRBARA D'OESTE

PREGÃO ELETRÔNICO Nº ____/____.

A empresa, com sede no endereço
....., nº.....,
C.N.P.J. nº....., **DECLARA, sob as penas da Lei:**

- a) Que 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;
- b) Que 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 artigo 7º, XXXIII, da Constituição;
- c) Que 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;
- d) Que 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.

Se microempresa e empresa de pequeno porte:

- e) Que cumpre os requisitos estabelecidos no artigo 3º da Lei Complementar nº 123, de 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 n.º 14.133, de 2021.

Local e data:

Assinatura do Responsável pela Empresa
(Nome Legível/ Cargo/ Carimbo do CNPJ)



ANEXO VI- CADASTRO DE REPRESENTANTE

Dados do Representante

CONTRATADA

Caso seja representado por procuração, enviar cópia autenticada.

Nome Completo:	
Cargo:	
CPF:	
RG:	
Data de Nascimento:	
Endereço residencial completo:	
E-mail institucional:	
E-mail Pessoal:	
Telefones:	
Possui Certificado Digital e-CPF ou e-CNPJ?	<input type="checkbox"/> Sim <input type="checkbox"/> Não
Se positivo, informar a certificadora:	
Qual o tipo do certificado?	<input type="checkbox"/> A1 (instalado no computador) <input type="checkbox"/> A3 – token <input type="checkbox"/> A3 – cartão <input type="checkbox"/> A3 – nuvem



ANEXO VII- LC-02 - DECLARAÇÃO DE DOCUMENTOS À DISPOSIÇÃO DO TCE – SP

CONTRATANTE: Município De Santa Bárbara D'Oeste

CNPJ Nº: 46.422.408/0001-52

CONTRATADA:

CNPJ Nº:

CONTRATO nº (de origem):

DATA DA ASSINATURA:

VIGÊNCIA:

OBJETO:

VALOR :

Declaro(amos), na qualidade de responsável(is) pela entidade supra epigrafada, sob as penas da Lei, que os demais documentos originais, atinentes à correspondente licitação, encontram-se no respectivo processo administrativo arquivado na origem à disposição do Tribunal de Contas do Estado de São Paulo e serão remetidos quando requisitados.

LOCAL e DATA:

RESPONSÁVEL:

(nome, cargo, e-mail e assinatura)



ANEXO VIII

DECRETO Nº 7.468 DE 25 DE AGOSTO DE 2.023

“Dispõe sobre os procedimentos referente à retenção do Imposto sobre a Renda prevista na Instrução Normativa da Receita Federal do Brasil nº 1.234/2012 e alterações nos pagamentos efetuados a pessoas físicas e jurídicas pelo fornecimento de bens e prestação de serviços pelos órgãos públicos do Município de Santa Bárbara d'Oeste”.

RAFAEL PIOVEZAN, Prefeito de Santa Bárbara d'Oeste, usando das atribuições que lhe são conferidas por lei e do que consta no Memorando nº 5.727/2023,

CONSIDERANDO o disposto no inciso I do art. 158 da Constituição da República;

CONSIDERANDO a decisão proferida pelo Supremo Tribunal Federal no julgamento do Recurso Extraordinário com Repercussão Geral nº 1.293.453 e na Ação Cível Originária nº 2897;

CONSIDERANDO o disposto na legislação tributária federal atinente a retenção de tributos, em especial o disposto no art. 64 da Lei nº 9.430/1996 e, também, na Instrução Normativa da Receita Federal do Brasil nº 1.234/2012, alterada pela Instrução Normativa da Receita Federal do Brasil nº 2145/2023;

CONSIDERANDO a necessidade de instrumentalizar e orientar os procedimentos de retenção, recolhimento e transferência dos valores retidos para o ente público municipal, conforme na Instrução Normativa acima mencionada e dar integral cumprimento às correspondentes obrigações acessórias de prestação de informações à Receita Federal do Brasil,

D E C R E T A:

Art. 1º Os órgãos públicos do Município de Santa Bárbara d'Oeste, ao efetuarem a retenção do Imposto de Renda (IR) no pagamento para pessoa física ou jurídica com base na Instrução Normativa RFB nº 1.234/2012 e suas alterações, para fins de atendimento das obrigações acessórias de prestação de informações à Receita Federal do Brasil, observarão as disposições contida neste Decreto.



Município de Santa Bárbara d'Oeste

Art. 2º As retenções efetuadas sobre qualquer forma de pagamento, decorrentes de pagamentos diretos, contratos vigentes ou futuros, bem como sobre pagamentos antecipados por conta de fornecimento de bens ou de prestação de serviços para entrega futura, consideradas como antecipação do devido imposto pelos contribuintes e passíveis de dedução, compensação ou restituição na forma da legislação específica, deverão ser destacadas no corpo do documento fiscal pelo recebedor, observando-se os percentuais estabelecidos no ANEXO ÚNICO deste Decreto.

Art. 3º Os prestadores de serviços e fornecedores de bens que tiverem retenção de valores nas condições especificadas neste Decreto deverão emitir os documentos fiscais em observância às regras de retenção de Imposto de Renda vigentes.

Parágrafo único. A inobservância das regras de retenção constantes no “caput” deste artigo ensejará a recusa do recebimento dos receptivos documentos fiscais, com a notificação para a devida correção como condição de pagamento.

Art. 4º Os fornecedores e prestadores de serviços cujos pagamentos não estejam sujeitos à retenção do IR na fonte deverão apresentar a declaração especificada nos Anexos II, III e IV da Instrução Normativa mencionada.

Art. 5º As retenções referidas no presente Decreto e efetuadas pelos diferentes órgãos públicos municipais terão seu valor transferido ao Município de Santa Bárbara d'Oeste.

Art. 6º Todos órgãos da Prefeitura Municipal deverão orientar seus servidores, prestadores de serviços e fornecedores de bens quanto ao cumprimento da Instrução Normativa referida no presente Decreto, bem como sobre o procedimento de recusa do recebimento de documentos fiscais que não atendam as respectivas regras.

Art. 7º Este decreto entra em vigor na data de sua publicação.

Santa Bárbara d'Oeste, 25 de agosto de 2.023.

RAFAEL PIOVEZAN
Prefeito Municipal



ANEXO ÚNICO - TABELA DE RETENÇÃO

(Índices constantes no ANEXO I DA I.N. RFB Nº 1234, DE 11 DE JANEIRO DE 2012)

NATUREZA DO BEM FORNECIDO OU DO SERVIÇO PRESTADO	ALÍQUOTA IR
<ul style="list-style-type: none">Alimentação;Energia elétrica;Serviços prestados com emprego de materiais;Construção Civil por empreitada com emprego de materiais;Serviços hospitalares de que trata o art. 30 da IN RFB 1234/2012;Serviços de auxílio diagnóstico e terapia, patologia clínica, imagenologia, anatomia patológica e citopatologia, medicina nuclear e análises e patologias clínicas de que trata o art. 31 da IN RFB 1234/2012;Transporte de cargas, exceto os relacionados no código 8767 da IN RFB 1234/2012;Produtos farmacêuticos, de perfumaria, de toucador ou de higiene pessoal adquiridos de produtor, importador, distribuidor ou varejista, exceto os relacionados no código 8767 da IN RFB 1234/2012; eMercadorias e bens em geral.	1,20%
<ul style="list-style-type: none">Gasolina, inclusive de aviação, óleo diesel, gás liquefeito de petróleo (GLP), combustíveis derivados de petróleo ou de gás natural, querosene de aviação (QAV), e demais produtos derivados de petróleo, adquiridos de refinarias de petróleo, de demais produtores, de importadores, de distribuidor ou varejista, pelos órgãos da administração pública de que trata o caput do art. 19 da IN RFB 1234/2012;Álcool etílico hidratado, inclusive para fins carburantes, adquirido diretamente de produtor, importador ou distribuidor de que trata o art. 20 da IN RFB 1234/2012;Biodiesel adquirido de produtor ou importador, de que trata o art. 21 da IN RFB 1234/2012;	0,24%
<ul style="list-style-type: none">Gasolina, exceto gasolina de aviação, óleo diesel, gás liquefeito de petróleo (GLP), derivados de petróleo ou de gás natural e querosene de aviação adquiridos de distribuidores e comerciantes varejistas;Álcool etílico hidratado nacional, inclusive para fins carburantes adquirido de comerciante varejista;Biodiesel adquirido de distribuidores e comerciantes varejistas;Biodiesel adquirido de produtor detentor regular do selo "Combustível Social", fabricado a partir de mamona ou fruto, caroço ou amêndoa de palma produzidos nas regiões norte e nordeste e no	0,24%



Município de Santa Bárbara d'Oeste

semiárido, por agricultor familiar enquadrado no Programa Nacional de Fortalecimento da Agricultura Familiar (Pronaf).	
<ul style="list-style-type: none">• Transporte internacional de cargas efetuado por empresas nacionais;• Estaleiros navais brasileiros nas atividades de construção, conservação, modernização, conversão e reparo de embarcações pré-registradas ou registradas no Registro Especial Brasileiro (REB), instituído pela Lei nº 9.432, de 8 de janeiro de 1997;• Produtos farmacêuticos, de perfumaria, de toucador e de higiene pessoal a que se refere o § 1º do art. 22, adquiridos de distribuidores e de comerciantes varejistas;• Produtos a que se refere o § 2º do art. 22 da IN RFB 1234/2012;• Produtos de que tratam as alíneas "c" a "k" do inciso I do art. 5º da IN RFB 1234/2012;• Outros produtos ou serviços beneficiados com isenção, não incidência ou alíquotas zero da Cofins e da Contribuição para o PIS/Pasep, observado o disposto no § 5º do art. 2º da IN RFB 1234/2012;	1,20%
<ul style="list-style-type: none">• Passagens aéreas, rodoviárias e demais serviços de transporte de passageiros, inclusive, tarifa de embarque, exceto as relacionadas no código 8850 da IN RFB 1234/2012;	2,40%
<ul style="list-style-type: none">• Transporte internacional de passageiros efetuado por empresas nacionais.	2,40%
<ul style="list-style-type: none">• Serviços prestados por associações profissionais ou assemelhadas e cooperativas.	0%
<ul style="list-style-type: none">• Serviços prestados por bancos comerciais, bancos de investimento, bancos de desenvolvimento, caixas econômicas, sociedades de crédito, financiamento e investimento, sociedades de crédito imobiliário, e câmbio, distribuidoras de títulos e valores mobiliários, empresas de arrendamento mercantil, cooperativas de crédito, empresas de seguros privados e de capitalização e entidades abertas de previdência complementar;• Seguro saúde.	2,40%
<ul style="list-style-type: none">• Serviços de abastecimento de água;• Telefone;• Correio e telégrafos;• Vigilância;• Limpeza;• Locação de mão de obra;• Intermediação de negócios;• Administração, locação ou cessão de bens imóveis, móveis e direitos de qualquer natureza;• Factoring;• Plano de saúde humano, veterinário ou odontológico com valores fixos por servidor, por empregado ou por animal;• Demais serviços.	4,80%