CÂMARA MUNICIPAL DE
SANTO ANDRÉ

CONTRATO Nº 28/2023

CONTRATO DE AQUISIÇÃO DE MICROCOMPUTADORES COM GARANTIA TÉCNICA DO FABRICANTE E DE LICENCIAMENTO DE SOLUÇÃO DE PROTEÇÃO E ANTIVÍRUS, QUE CELEBRAM ENTRE SI A CÂMARA MUNICIPAL DE SANTO ANDRÉ E A EMPRESA CENTERTEC NEGÓCIOS, SOLUÇÕES E TECNOLOGIA LTDA.

PREÂMBULO

Aos quinze dias do mês de dezembro de 2023, a **CÂMARA MUNICIPAL DE SANTO ANDRÉ**, inscrita no **CNPJ sob nº 43.307.008/0001-08**, situada na Praça IV Centenário, 2, Centro, Santo André – SP, CEP 09040-905, doravante denominada "CONTRATANTE", neste ato representada por seu Presidente, Vereador Carlos Roberto Ferreira, portador da Cédula de Identidade RG nº 08.388.787-8 emitida pela Secretaria de Segurança Pública do Estado de São Paulo (SSP-SP) e do CPF/MF nº 029.194.068-41, e a empresa **CENTERTEC NEGÓCIOS, SOLUÇÕES E TECNOLOGIA LTDA**, inscrita no **CNPJ sob nº 01.157.868/0001-62**, com sede na Rua Alegre, nº 726, bairro Barcelona, São Caetano do Sul/SP, CEP 09.550-250, doravante denominada "CONTRATADA", representada pelo Sr. Valter Mateus da Silva, portador da Cédula de Identidade RG nº 16.906.843-2 emitida pela Secretaria de Segurança Pública do Estado de São Paulo (SSP-SP), e do CPF/MF nº 072.583.798-51, perante as testemunhas ao final firmadas, assinam o presente contrato, cuja celebração foi autorizada pelo despacho de fls. 990 e 991 do Processo Acessório Licitatório "PLP – 13/2023" vinculado ao **Processo Administrativo Principal CM nº 7299/2023**, que se regerá pela Lei Federal 10.520/02 e subsidiariamente pela Lei Federal 8.666/93, atendidas as cláusulas e condições que se enunciam a seguir:

FUNDAMENTO DO CONTRATO

Este contrato decorre da autorização do Senhor Presidente da Câmara Municipal de Santo André ao homologar a licitação na modalidade **PREGÃO**, do tipo **MENOR PREÇO POR LOTE**, aberta sob nº 12/2023, consoante se verifica nos autos do Processo Administrativo Principal nº 7299/2023.

I - OBJETO DO CONTRATO

1. É objeto deste contrato a **aquisição de microcomputadores com garantia técnica do fabricante e de licenciamento de solução de proteção e antivírus**, conforme especificações e condições contidas no Anexo I do Edital que antecedeu a presente contratação.

2. Nos termos do inciso XI do Art. 55 da Lei Federal nº 8.666/93, fazem parte integrante do presente contrato o Edital, seus Anexos e a proposta vencedora.

II - FORMA DE EXECUÇÃO

1. O objeto deste ajuste será executado de acordo com as normas, especificações e demais elementos técnicos fornecidos pela CONTRATANTE e em conformidade com a proposta apresentada pela CONTRATADA, os quais ficam fazendo parte integrante deste contrato, independentemente de transcrições.

III - EXIGÊNCIAS A SEREM OBSERVADAS - Na execução, a CONTRATADA deverá observar e cumprir as exigências seguintes:

1. Assumir integral responsabilidade pela boa e eficiente execução do objeto, de acordo com o estabelecido no detalhamento dos itens a serem entregues constantes do Anexo I - Termo de Referência, assim como pelos danos decorrentes da realização de ditos trabalhos.

2. Assumir inteira responsabilidade pela entrega que efetuar, de acordo com as especificações constantes no Anexo I - Termo de Referência, bem como da respectiva proposta, obedecendo ao Código de Defesa do Consumidor e à legislação pertinente vigente quanto às condições dos itens entregues.

IV - RESPONSABILIDADES

1. A CONTRATADA será única responsável pelos encargos sociais, trabalhistas, previdenciários, fiscais e comerciais resultantes da execução do contrato, bem como por todas as despesas necessárias incluindo transporte, mão de obra e demais despesas indiretas.

V - PRAZOS

1. Prazo de Vigência do Contrato: O prazo de vigência do contrato será de 12 (doze) meses a partir de sua assinatura.

2. Prazo de Garantia do Objeto: A contar da data do Recebimento Definitivo dos itens, conforme abaixo:

a. Item 1: 36 (trinta e seis) meses *on site*;
b. Item 2: 36 (trinta e seis) meses *on site*;
c. Item 3: 36 (trinta e seis) meses *on site*;
d. Item 4: Não se aplica;
e. Item 5: Não se aplica;
f. Item 6: 36 (trinta e seis) meses.

2.1. Manutenção e Assistência Técnica dos Equipamentos – Deverão ser atendidas as condições previstas no item 7 do Anexo I - Termo de Referência.

2.2. Relativamente ao disposto aplica-se, subsidiariamente, no que couber a Lei nº 8.078/1990 - Código de Defesa do Consumidor.

3. Prazo de Entrega

3.1. O prazo de entrega será de 30 (trinta) dias úteis contados a partir da assinatura contratual.

VI - DO LOCAL E DAS CONDIÇÕES DE ENTREGA

1. A entrega dos itens deverá ser efetuada na Diretoria de Apoio Tecnológico, com o acompanhamento da Comissão de Recebimentos, no endereço da Câmara Municipal de Santo André (SP), situada na Praça IV Centenário, nº 2, Centro - 09040-905, de 2ª a 6ª feira, das 10 às 13 horas e das 14 às 18 horas e, em quantidade a ser definida posteriormente, na Avenida Portugal, nº 141, salas 82 e 84, Centro - CEP 09040-010, com vistas a atender os departamentos lá alocados.

2. Os itens deverão ser entregues em embalagens originais do fabricante devidamente lacradas, os quais serão conferidos e, se achados irregulares, devolvidos à CONTRATADA, a qual terá o prazo de 05 (cinco) dias para substituí-los.

3. A CONTRATADA ficará obrigada a trocar, às suas expensas, os itens que vierem a ser recusados, sendo que o ato de recebimento não importará aceitação.

4. O prazo para substituição de itens fora da especificação ou com eventuais defeitos será de, no máximo, 10 (dez) dias corridos, a contar da data do recebimento.

VII - DA FISCALIZAÇÃO E RECEBIMENTO DO OBJETO

1. A CONTRATADA designa o Sr. Valter Mateus da Silva, a quem outorga poderes legais para representá-la na execução do contrato e servirá, ainda, de elemento permanente de ligação com os Fiscais da CONTRATANTE, devendo atendê-los em horário comercial, de segunda a sexta-feira, sem ônus qualquer adicional.

2. A CONTRATANTE designa os(as) Diretor de Tecnologia da Informação, em conjunto com o(a) Gerência de Tecnologia da Informação e o Chefe do Núcleo de Suporte ao Usuário - *Hardware* / *Software*, como seu(s) Fiscal(ais) para representá-la na execução do presente contrato, garantindo a qualidade e a excelência do objeto contratado, e atuação durante toda a sua vigência, devendo se manifestar sempre sobre o atendimento pleno e demais condições que envolvam suas entregas, relatando as ocorrências em processo próprio de acompanhamento.

3. A CONTRATANTE exercerá a mais ampla e completa fiscalização dos serviços contratados através da Comissão de Recebimentos e de seus Fiscais. A fiscalização em nenhuma hipótese eximirá, nem reduzirá as responsabilidades legais e contratuais da CONTRATADA, seja quanto aos danos materiais e pessoais que forem causados a terceiros, seja por atos próprios da mesma, seja por atitudes de seus operários e prepostos.

4. A Fiscalização comunicará a CONTRATADA, por escrito, preferencialmente via e-mail, as deficiências porventura verificadas na execução dos serviços, para a imediata correção, sem prejuízo das sanções cabíveis.

5. A Comissão de Recebimentos será composta pelos Fiscais designados no item 2 e pelo(a) Chefe de Núcleo de Patrimônio, cabendo a estes, em conjunto, dar recebimento provisório e o definitivo, permitindo a verificação da entrega, as possíveis substituições ou trocas que, porventura, forem necessárias, até seu recebimento definitivo em conformidade com as especificações do Anexo I deste Edital.

6. O acompanhamento, o controle, a fiscalização e a avaliação por parte do Fiscal do Contrato não exclui a responsabilidade da CONTRATADA e nem confere à CONTRATANTE responsabilidade solidária, inclusive perante terceiros, por quaisquer irregularidades ou danos na execução do objeto contratado.

VIII - DAS CONDIÇÕES DE RECEBIMENTO DO OBJETO

1. Recebimento Provisório - Todos os itens serão recebidos provisoriamente pela Comissão de Recebimentos, após a entrega, para verificação da conformidade com as especificações, o que ocorrerá em prazo não superior a 05 (cinco) dias úteis após a data da entrega.

1.1. Sendo constatada qualquer irregularidade, não se dará o recebimento definitivo, ficando a CONTRATADA obrigada a atender às determinações da Comissão de Recebimento no prazo máximo de 10 (dez) dias, após o qual será efetuado novo exame dos materiais.

1.2. Na 2ª oportunidade, os itens deverão apresentar perfeitas condições de serem recebidos definitivamente, sendo que, se não estiverem em ordem, a CONTRATADA sofrerá aplicação da multa cominada para o atraso diário na conclusão, a contar da data da 1ª vistoria, nos termos do Ato nº 4, de 22 de março de 2005.

2. Recebimento Definitivo - Decorrido o prazo e inexistindo falhas ou incorreções, a Comissão de Recebimento lavrará o "Termo de Recebimento Definitivo", depois de reexaminados os itens e desde que estejam em perfeitas condições, mediante requerimento da CONTRATADA, de acordo com o disposto no art. 73, II, "b" da Lei Federal nº 8.666/93.

IX - PREÇOS E PAGAMENTOS

1. A CONTRATANTE pagará à CONTRATADA, após o Recebimento Definitivo de cada entrega, o respectivo preço constante da proposta apresentada, em conformidade com as especificações técnicas contidas neste Edital e seus Anexos.

2. No preço acham-se computados e diluídos todos os ônus decorrentes de despesas diretas e indiretas (mão de obra, equipamentos, acessórios, encargos sociais e quaisquer outras despesas

necessárias), mesmo que não tenham sido apontadas expressamente pela CONTRATANTE, desde que tenham relação com os o objeto deste Edital.

3. O pagamento será efetuado em até 05 (cinco) dias úteis pela Diretoria de Orçamento e Finanças, após o Recebimento Definitivo firmado pela Comissão de Recebimentos, por meio de depósito em conta corrente, através de ordem bancária, após a apresentação da respectiva Nota Fiscal eletrônica/fatura, devidamente discriminada e atestada por servidor(a) designado(a) pela CONTRATANTE.

4. O não pagamento da Nota Fiscal eletrônica/fatura, apresentada nas condições previstas, ensejará a incidência da necessária compensação financeira a ser procedida nos termos da Lei Civil.

5. Nenhum pagamento será efetuado à CONTRATADA, enquanto pendente de liquidação de qualquer obrigação financeira que lhe for imposta, em virtude de penalidade ou inadimplência, a qual poderá ser compensada com o pagamento pendente sem que isso gere direito a acréscimos de qualquer natureza.

6. Sustação dos Pagamentos - Nenhum pagamento será feito à CONTRATADA, caso haja penalização monetária, antes que ocorra a respectiva quitação ou que se releve a conduta sancionatória aplicada.

7. Reajuste - Os preços serão fixos e irreajustáveis pelo período contratual original.

X - DO VALOR DO CONTRATO

1. A CONTRATANTE pagará à CONTRATADA pela execução do objeto contratual, o respectivo preço constante da proposta comercial, perfazendo o valor total de R$ 2.662.245,00 (dois milhões seiscentos e sessenta e dois mil duzentos e quarenta e cinco reais), distribuído da seguinte forma:

1.1. Lote 1: R$ 2.513.624,00 (dois milhões, quinhentos e treze mil, seiscentos e vinte e quatro reais);

1.2. Lote 3: R$ 148.621,00 (cento e quarenta e oito mil, seiscentos e vinte e um reais).

XI - DA DOTAÇÃO ORÇAMENTÁRIA

1. A despesa com este Contrato, no corrente exercício, no montante de R$ 2.662.245,00 (dois milhões seiscentos e sessenta e dois mil duzentos e quarenta e cinco reais), correrá à conta da **Nota de Empenho nº 749/2023**, no valor de **R$ 2.513.624,00** (dois milhões quinhentos e treze mil seiscentos e vinte e quatro reais), devidamente apropriada no elemento de despesa **4.4.90.52 - EQUIPAMENTOS E MATERIAL PERMANENTE**, vincula à atividade 1002 AQUISIÇÃO DE VEÍCULOS E EQUIPAMENTOS da vigente Lei Orçamentária Anual e da **Nota de Empenho nº 750/2023**, no valor de **R$ 148.621,00** (cento e quarenta e oito mil seiscentos e vinte e um reais), devidamente apropriada no elemento de despesa **3.3.90.40 - SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO – PJ**, vincula à atividade 2002 MANUTENÇÃO DAS ATIVIDADES LEGISLATIVAS da vigente Lei Orçamentária Anual, ambas de **12/12/2023**.

XII - GARANTIA CONTRATUAL

1. A CONTRATADA forneceu à CONTRATANTE garantia no valor de R$ 133.112,25 (cento e trinta e três mil cento e doze reais e vinte e cinco centavos), correspondente a 5% (cinco por cento) do valor contratual, na modalidade seguro-garantia, conforme o inciso II do § 1º do art. 56 da Lei Federal 8.666/93.

2. A garantia prestada será restituída após o cumprimento integral de todas as obrigações contratuais, após requerimento da CONTRATADA, inclusive períodos de garantia.

XIII - PENALIDADES

1. A CONTRATADA deverá observar rigorosamente as condições estabelecidas, sujeitando-se às penalidades constantes nos Arts. 86 e 87 da Lei Federal 8.666/93 nos casos de retardamento, de falha na execução do Contrato, de inexecução parcial ou de inexecução total do objeto.

2. As penalidades e os procedimentos relativos à aplicação de multas e outras sanções decorrentes da inexecução total ou parcial do contrato, no âmbito da Câmara Municipal de Santo André estão previstos no Anexo II - Ato nº 4, de 22 de março de 2005, do presente ajuste.

XIV - RESCISÃO

1. Haverá rescisão contratual na ocorrência de qualquer dos motivos elencados no Art. 78, na forma estabelecida no Art. 79, com as consequências previstas no Art. 80, todos da Lei Federal n.º 8.666/93, sem prejuízo das sanções enumeradas no Art. 87.

XV - DISPOSIÇÕES GERAIS

1. ACRÉSCIMOS OU SUPRESSÕES - A CONTRATADA ficará obrigada a aceitar, nas mesmas condições contratuais, acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato, obedecido ao disposto no § 1º do Art. 65 da Lei Federal nº 8.666/93.

2. MANUTENÇÃO DAS CONDIÇÕES HABILITATÓRIAS - A CONTRATADA obriga-se a manter, durante toda a execução contratual, em compatibilidade com as obrigações por ela assumidas, as condições habilitatórias e de qualificação exigidas na respectiva licitação, conforme previsão do inciso XIII do Art. 55 da Lei nº 8666, de 21 de junho de 1993.

3. FORO - Fica eleito o Foro da Comarca de Santo André, com exclusão de qualquer outro, por mais privilegiado que seja para dirimir qualquer questão oriunda da execução deste contrato.

4. PUBLICIDADE - A Administração efetivará a publicação resumida deste instrumento de contrato na imprensa oficial, nos termos do parágrafo único do Art. 61 da Lei nº 8.666/93.

5. TRATAMENTO DOS DADOS - As Partes obrigam-se a realizar o tratamento de dados pessoais em obediências às disposições legais vigentes, nos moldes da Lei 13.709/18 (LGPD), com vistas a dar efetiva proteção aos dados coletados de pessoas naturais que possam identificá-las ou torná-las identificáveis.

E, para firmeza e validade do que aqui ficou estipulado, foi lavrado o presente contrato, em 02 (duas) vias de igual teor, que, depois de lido e achado conforme, é assinado pelas partes contratantes e pelas testemunhas abaixo.

Câmara Municipal de Santo André (SP), 15 de dezembro de 2023.
470º ano da fundação da cidade.

_____	_____
CARLOS ROBERTO FERREIRA (CARLOS FERREIRA)	**VALTER MATEUS DA SILVA**
pela CONTRATANTE	**pela CONTRATADA**

Testemunha 01:	**Testemunha 02:**
Nome: _____	Nome: _____
CPF: _____	CPF: _____
Ass.: _____	Ass.: _____

ANEXO I - TERMO DE REFERÊNCIA

1. Objeto

Aquisição de microcomputadores com garantia técnica do fabricante, devidamente descritos e caracterizados nas especificações técnicas de cada item presente neste documento, bem como aquisição de licenciamento de solução de proteção e antivírus conforme especificações deste Termo de Referência.

Justificativas

1.1. Microcomputadores - Itens 1, 2 e 3.

Os computadores são parte do projeto de modernização do parque tecnológico da Câmara Municipal de Santo André que tem o intuito de melhoria na mobilidade, ergonomia, otimização de espaço, implementação do parque de máquinas utilizadas nas dependências do Legislativo ou de forma remota, em vista dos constantes avanços na área de informática. A aquisição objetiva assim um melhor desempenho na realização das atividades desenvolvidas pelos usuários, proporcionando flexibilidade e agilidade na rotina de trabalho, possibilitando, inclusive, acesso as rotinas em teletrabalho. Também os equipamentos portáteis podem ser transportados para reuniões, apresentações, visitas, possibilitando um melhor funcionamento das atividades da administração.

1.2. Das licenças - Item 6.

As atividades desenvolvidas pela Câmara Municipal de Santo André têm, entre suas finalidades, oferecer atendimento a todos os munícipes com disponibilização de uma estrutura adequada para isso, buscando, em conjunto, devolver aos moradores uma contrapartida social em forma de atendimento.

A solução de antivírus é necessária, pois a Câmara Municipal de Santo André possui parque de recursos tecnológicos que requer formas adequadas de proteção, em várias camadas, implementando a segurança nas estações de trabalho, servidores e notebooks. Entre as soluções oferecidas pelo mercado e com base em configurações mínimas definidas para uma proteção robusta, o corpo técnico precisa de uma solução que atenda as necessidades de proteção desta Edilidade.

1.3. Da qualificação técnica/operacional

A exigência de atestado de qualificação técnica para fins de habilitação justifica-se com vistas à comprovação de aptidão para fornecimento dos quantitativos, sendo alternativa de comprovar a capacidade técnico-operacional da licitante em fornecer e executar os serviços com características similares. Tal comprovação resguarda a Administração para maior garantia do cumprimento da obrigação a ser assumida pela vencedora do certame, sendo este aspecto primordial para que atenda de forma satisfatória a entrega dos itens e serviços solicitados.

2. Da Meta Física

Esta contratação tem por objetivo a modernização e reestruturação tecnológica que proporcionem segurança, durabilidade e economicidade nas manutenções. Os softwares adquiridos serão instalados nos respectivos notebooks.

3. Destinação prevista para os Computadores

Sequência	Local	Tipo
1	AJL	Tipo 1
2	AJL	Tipo 1
3	AJL	Tipo 1
4	AJL	Tipo 1
5	AJL	Tipo 1
6	AJL	Tipo 1
7	AJL	Tipo 1
8	ATP	Tipo 1
9	ATP	Tipo 1
10	ATP	Tipo 1
11	CBT	Tipo 1
12	CBT	Tipo 1
13	CBT	Tipo 1
14	CCA	Tipo 1
15	CCA	Tipo 1
16	CCA	Tipo 1
17	CCE	Tipo 1
18	CCE	Tipo 1
19	CCE	Tipo 1
20	CCE	Tipo 1
21	CCE	Tipo 1
22	CONTROLADORIA	Tipo 1
23	CONTROLADORIA	Tipo 1
24	CONTROLADORIA	Tipo 1
25	DA	Tipo 1
26	DA	Tipo 1
27	DAL	Tipo 1
28	DAL	Tipo 1
29	DAL	Tipo 1
30	DAL	Tipo 1
31	DAL	Tipo 1
32	DG	Tipo 1
33	DG	Tipo 1
34	DG	Tipo 1
35	DTI - Rede	Tipo 2
36	DTI - Rede	Tipo 1

Sequência	Local	Tipo
69	GAB. 05	Tipo 1
70	GAB. 05	Tipo 1
71	GAB. 06	Tipo 2
72	GAB. 06	Tipo 1
73	GAB. 06	Tipo 1
74	GAB. 06	Tipo 1
75	GAB. 07	Tipo 2
76	GAB. 07	Tipo 1
77	GAB. 07	Tipo 1
78	GAB. 07	Tipo 1
79	GAB. 08	Tipo 2
80	GAB. 08	Tipo 1
81	GAB. 08	Tipo 1
82	GAB. 08	Tipo 1
83	GAB. 09	Tipo 2
84	GAB. 09	Tipo 1
85	GAB. 09	Tipo 1
86	GAB. 09	Tipo 1
87	GAB. 10	Tipo 2
88	GAB. 10	Tipo 1
89	GAB. 10	Tipo 1
90	GAB. 10	Tipo 1
91	GAB. 11	Tipo 2
92	GAB. 11	Tipo 1
93	GAB. 11	Tipo 1
94	GAB. 11	Tipo 1
95	GAB. 12	Tipo 2
96	GAB. 12	Tipo 1
97	GAB. 12	Tipo 1
98	GAB. 12	Tipo 1
99	GAB. 13	Tipo 2
100	GAB. 13	Tipo 1
101	GAB. 13	Tipo 1
102	GAB. 13	Tipo 1
103	GAB. 14	Tipo 2
104	GAB. 14	Tipo 1

Sequência	Local	Tipo
137	GCI - GERENTE	Tipo 3
138	GCM	Tipo 1
139	GCM	Tipo 1
140	GCM	Tipo 1
141	GCM	Tipo 1
142	GCM	Tipo 1
143	GCM	Tipo 1
144	GCM	Tipo 1
145	GCM	Tipo 1
146	GCM	Tipo 1
147	GCM	Tipo 1
148	GIS	Tipo 1
149	GIS	Tipo 1
150	GOF	Tipo 1
151	GOF	Tipo 1
152	GOF	Tipo 1
153	GOF	Tipo 1
154	GOF	Tipo 1
155	GOF	Tipo 1
156	GOF	Tipo 1
157	GOF	Tipo 1
158	GOF	Tipo 1
159	GOF	Tipo 1
160	GRH	Tipo 1
161	GRH	Tipo 1
162	GUARDA	Tipo 1
163	NAL	Tipo 1
164	NAL	Tipo 1
165	NAP	Tipo 1
166	NAP	Tipo 1
167	NAP	Tipo 1
168	NAP	Tipo 1
169	NAP	Tipo 1
170	NAP	Tipo 1
171	NAP	Tipo 1
172	NCF	Tipo 1

Sequência	Local	Tipo
37	DTI - Desenv	Tipo 3
38	DTI - Desenv	Tipo 2
39	DTI - Desenv	Tipo 2
40	DTI - Desenv	Tipo 3
41	DTI - Suporte	Tipo 1
42	DTI - Suporte	Tipo 2
43	DTI - Suporte	Tipo 2
44	DTI - Suporte	Tipo 2
45	DTI - Suporte	Tipo 2
46	DTI - DPO	Tipo 1
47	DTI - DPO	Tipo 2
49	DTI - Cidadania	Tipo 1
50	DTI - DIRETOR	Tipo 1
51	DTI - Apoio	Tipo 1
52	ESCOLA	Tipo 1
53	ESCOLA	Tipo 1
54	ESCOLA	Tipo 1
59	GAB. 03	Tipo 2
60	GAB. 03	Tipo 1
61	GAB. 03	Tipo 1
62	GAB. 03	Tipo 1
63	GAB. 04	Tipo 2
64	GAB. 04	Tipo 1
65	GAB. 04	Tipo 1
66	GAB. 04	Tipo 1
67	GAB. 05	Tipo 2
68	GAB. 05	Tipo 1

Sequência	Local	Tipo
105	GAB. 14	Tipo 1
106	GAB. 14	Tipo 1
107	GAB. 15	Tipo 2
108	GAB. 15	Tipo 1
109	GAB. 15	Tipo 1
110	GAB. 15	Tipo 1
111	GAB. 16	Tipo 2
112	GAB. 16	Tipo 1
113	GAB. 16	Tipo 1
114	GAB. 16	Tipo 1
115	GAB. 17	Tipo 2
117	GAB. 17	Tipo 1
118	GAB. 17	Tipo 1
119	GAB. 18	Tipo 2
120	GAB. 18	Tipo 1
121	GAB. 18	Tipo 1
122	GAB. 18	Tipo 1
127	GAB. 20	Tipo 2
128	GAB. 20	Tipo 1
129	GAB. 20	Tipo 1
130	GAB. 20	Tipo 1
131	GAB. 21	Tipo 2
132	GAB. 21	Tipo 1
133	GAB. 21	Tipo 1
134	GAB. 21	Tipo 1
135	GCI	Tipo 3
136	GCI	Tipo 3

Sequência	Local	Tipo
173	NCF	Tipo 1
174	NCF	Tipo 1
175	NFT	Tipo 1
176	NFT	Tipo 1
177	NMI	Tipo 1
178	NMI	Tipo 1
179	NSO	Tipo 1
180	OUVIDORIA	Tipo 1
181	PLENARIO	Tipo 1
182	PLENARIO	Tipo 1
183	PLENARIO	Tipo 1
185	PRESIDÊNCIA	Tipo 1
186	PRESIDÊNCIA	Tipo 1
187	PRESIDÊNCIA	Tipo 1
188	PRESIDÊNCIA	Tipo 1
189	PRESIDÊNCIA	Tipo 1
190	PROTOCOLO	Tipo 1
195	TAQUIGRAFIA	Tipo 1
196	TAQUIGRAFIA	Tipo 1
197	PLANEJAMENTO	Tipo 1
198	PLANEJAMENTO	Tipo 1
199	DIRETOR ADM	Tipo 1
200	DIRETOR FINANC	Tipo 1
201	PROCURADORIA	Tipo 1
202	PROCURADORIA	Tipo 1

4. Especificações Técnicas Mínimas

4.1. Microcomputador Portátil - Tipo I

4.1.1. Processador

4.1.1.1. 01 (um) processador, padrão de arquitetura do processador x 86 de 32 bits com suporte à extensão 64 bits;

4.1.1.2. Deverá ser da última geração disponibilizada pelo fabricante do equipamento;

4.1.1.3. Processador com índice mínimo de 10.000 (dez mil) pontos tendo como referência a base de dados *Passmark CPU Mark* disponível no site: https://www.cpubenchmark.net/cpu_list.php

4.1.1.4. Deverá ter frequência mínima real (CLOCK) de 2.4 GHZ e cache de 8 MB;

4.1.1.5. Deverá conter no mínimo 4 (quatro) núcleos de processamento real;

4.1.1.6. Deverá possuir capacidade de execução simultânea de no mínimo 8 (oito) “threads”;

4.1.1.7. O processador deverá ter litografia de 14 (quatorze) nanômetros;

4.1.1.8. O processador deverá possuir recurso compatível com a tecnologia Speed Shif ou outra para selecionar mais rapidamente sua melhor frequência de operação e sua melhor tensão para desempenho ótimo e máxima eficiência de energia;
4.1.1.9. Deverá suportar no mínimo as memórias DDR4-3200 e LPDDR4x-4267;
4.1.1.10. Deverá implementar tecnologia de monitoramento térmico;
4.1.1.11. O processador deve suportar expansão com a utilização da porta Thunderbolt 4 para ajustar dinamicamente a largura de banda de dados e vídeo dependendo do dispositivo e/ou aplicação.

4.1.2. Memória Ram
4.1.2.1. Deverá ser fornecido com, no mínimo, 8 GBytes de memória RAM;
4.1.2.2. Padrão DDR4-3200 ou superior.

4.1.3. BIOS e Segurança
4.1.3.1. O BIOS deverá ser do tipo Flash Memory, utilizando memória não volátil e eletricamente reprogramável;
4.1.3.2. A inicialização do notebook deverá ser realizada na sequência definida pelo usuário, via dispositivos pela porta USB e/ou CDROM e/ou disco rígido, bem como pela placa de rede através do recurso WOL (Wake on LAN) compatível com o padrão PXE (Pré-boot Execution Enviroment);
4.1.3.3. Deverá possuir recursos de controle de permissão através de senhas, uma para inicializar o notebook, para acessar o HD e outra para acesso e alterações das configurações do BIOS;
4.1.3.4. Deverá possuir opção para bloqueio de visualização pela webcam;
4.1.3.5. Deverá possuir integrado ao hardware do notebook, subsistema de segurança TPM (Trusted Plataform Module).

4.1.4. Portas de Comunicação
4.1.4.1. 02 (duas) portas USB, sendo pelo menos 01 (uma) 3.1;
4.1.4.2. 01 (uma) porta para monitor de vídeo padrão DB15 VGA, caso o equipamento não possua porta de vídeo DB15 VGA nativa, deverá ser fornecido 01 (um) adaptador da saída digital disponível para VGA, trafegando imagem e som;
4.1.4.3. 01 (uma) porta HDMI 1.4b;
4.1.4.4. 01 (uma) porta da interface de rede padrão RJ45;
4.1.4.5. 01 (uma) porta de entrada áudio e 01 (uma) porta de saída de áudio ou 01 (uma) porta combo para microfone ou fone de ouvido;
4.1.4.6. 01 (um) conector USB-C.

4.1.5. Interface de Rede
4.1.5.1. 01 (uma) interface de rede;
4.1.5.2. Conector RJ45;
4.1.5.3. Interface de rede padrão Gigabit Ethernet;
4.1.5.4. Deverá operar automaticamente nas velocidades de comunicação de 100Mbps ou 1000Mbps;
4.1.5.5. Deverá suportar Wake-on-LAN.

4.1.6. Interface Wireless
4.1.6.1. 01 (uma) interface Wireless;
4.1.6.2. Deverá estar integrada a system board ou instalada no slot M.2;
4.1.6.3. Compatibilidade funcional e operacional com o padrão IEEE 802.11ax.

4.1.7. Interface Bluetooth
4.1.7.1. Deverá possuir interface para comunicação wireless padrão Bluetooth acima de 5 integrado;
4.1.7.2. A interface deverá estar integrada a system board ou a placa wireless.

4.1.8. Controladora de Vídeo
4.1.8.1. Padrão de barramento da controladora de vídeo do tipo on-board, PCI Express ou superior;
4.1.8.2. Frequência de 1.2GHz;
4.1.8.3. Suportar resolução gráfica 4096x2160 para a tela nativa e monitores externos;
4.1.8.4. Suportar a ligação de mais 1 monitor independente sem a necessidade de adição de placas ou acessórios.

4.1.9. Controladora de Disco
4.1.9.1. 02 (duas) controladoras SATA ou M.2.

4.1.10. Armazenamento
4.1.10.1. Deverá ser fornecido com 01 (uma) unidade de 256Gb;
4.1.10.2. Tipo interno ao gabinete;
4.1.10.3. Disco padrão SATA ou M.2;
4.1.10.4. Interface PCIe 3.0x4.

4.1.11. Kit de Áudio
4.1.11.1. Deverá ser fornecido 01 (um) Kit de Áudio composto por 01 (uma) Controladora de som e 01 (um) Headset USB-A mono aural com controle de volume, botão mute e cancelamento de ruído e proteção contra picos de som;
4.1.11.2. A controladora de som deverá ser onboard, contendo 01 (uma) saída amplificada para canais estéreos e 01 (uma) entrada para microfone ou combo de áudio (microfone/fone de ouvido em uma única saída);
4.1.11.3. Os alto-falantes deverão estar integrados ao gabinete do notebook com amplificador de sinal e potência de 1.5W por canal.

4.1.12. Webcam
4.1.12.1. 01 (uma) Webcam;
4.1.12.2. Resolução de 720p.

4.1.13. Teclado
4.1.13.1. Integrado;
4.1.13.2. Compatibilidade com o padrão ABNT Variant 2;
4.1.13.3. Teclado alfanumérico com 12 teclas de função e teclas combinadas para acesso rápido;

4.1.13.4. Possuir teclado numérico lateral.
4.1.13.5. Acompanhar teclado externo:
4.1.13.6. Dimensões (CxLxA) 400 x 120 x 20mm;
4.1.13.7. Possuir teclado numérico com 10 teclas;
4.1.13.8. Sem fio;
4.1.13.9. Ambos resistentes ao derramamento de líquidos;
4.1.13.10. Acompanhar pilhas com autonomia de 12 meses.

4.1.14. Mouse
4.1.14.1. Tipo Touchpad ou TrackPoint integrado ao gabinete;
4.1.14.2. Acompanhar um mouse externo;
4.1.14.3. Ambidestro;
4.1.14.4. Óptico com 03 botões;
4.1.14.5. Sem fio e compartilhando o mesmo receptor do teclado;
4.1.14.6. Dimensões (CxLxA) 110 x 60 x 40mm;
4.1.14.7. Acompanhar pilhas com autonomia de 12 meses.

4.1.15. Tela
4.1.15.1. Formato padrão 16:9;
4.1.15.2. Tamanho da tela de vídeo de 15 polegadas com superfície com tratamento antirreflexo;
4.1.15.3. Suportar resolução gráfica de 1920 x 1080 pixels;
4.1.15.4. Ângulo de visão 90º;
4.1.15.5. Brilho de 250cd;
4.1.15.6. Contraste de 500:1.

4.1.16. Fonte De Alimentação
4.1.16.1. A fonte deverá operar com tensão de entrada de 100 a 240VAC;
4.1.16.2. Frequência de operação de 50Hz a 60Hz;
4.1.16.3. Potência entre 60W e 80W.

4.1.17. Bateria Principal
4.1.17.1. A bateria deverá ser do tipo Íons de Lítio ou Polímero de Lítio de no mínimo 35Wh;
4.1.17.2. O tempo de recarga da bateria para 80% de carga deverá ser, no máximo, de 1 (uma) hora;
4.1.17.3. A autonomia deve ser de, no mínimo, 5 horas.

4.1.18. Gabinete
4.1.18.1. Gabinete monobloco com todos os conectores das portas de comunicação solicitadas;
4.1.18.2. O gabinete deverá ter estrutura robusta, revestido com composto de carbono, liga de magnésio, alumínio, titânio, polímero, fibra de vidro ou a mesclagem deles, para proteção contra impactos, com acabamento de alta resistência para maior durabilidade;
4.1.18.3. Botão liga/desliga, hibernação e deverá possuir dispositivo de proteção para prevenir o desligamento acidental do mesmo;
4.1.18.4. Deverá possuir 01 (uma) fenda para fixação e acompanhar o cabo ou trava antifurto que permita prender o notebook em objetos ou móveis fixos.

4.1.19. Dimensões

4.1.19.1. O peso do notebook deverá ser no máximo de 1,70 kg inclusos o disco rígido e a bateria principal;

4.1.19.2. A espessura (altura) do notebook deverá ser no máximo de 230 mm com a bateria instalada.

4.1.20. Sistema Operacional e Drivers

4.1.20.1. Deverá ser entregue com 01 (uma) licença do sistema operacional corporativo MS-Windows 11 Professional 64bits, em idioma português/Brasil. O recovery do sistema operacional ofertado deverá ser disponibilizado em uma partição do disco rígido do equipamento ou em mídias óticas;

4.1.20.2. O notebook e todos os seus periféricos deverão ser compatíveis com o sistema operacional oferecido;

4.1.20.3. O notebook deve estar certificado no HCL (Hardware Compatibility List) da Microsoft para o sistema operacional ofertado, que deve ser comprovado através de certificado obtido através do link: https://sysdev.microsoft.com/en-US/Hardware/lpl/

4.1.20.4. Deverá indicar em sua proposta comercial, link do fabricante onde possam ser baixados atualizações, firmwares, manuais, documentos, drivers e softwares e, ainda, consultadas especificações e status da garantia, bastando inserir o número de série do equipamento, sem qualquer ônus adicional à Câmara Municipal.

4.1.21. Mochila

4.1.21.1. Para notebooks de até 15,6” em nylon;

4.1.21.2. Possuir alça de transporte para mão e costas;

4.1.21.3. Cor com graduação escura;

4.1.21.4. Possuir compartimento específico para acomodar o notebook;

4.1.21.5. Possuir bolsos para acessórios com zíper;

4.1.21.6. Possuir porta externa e cabo interno para ligação de power bank, tornando o carregamento mais simples.

4.1.22. Qualidade do Equipamento

4.1.22.1. Deverá possuir identificação impressa com o nome do fabricante, modelo e número de série. Estas identificações não poderão ser feitas com etiquetas de fácil remoção ou danificação.

4.1.23. Assistência Técnica

4.1.23.1. Garantia prestada no local da CONTRATANTE (“on-site”) para o notebook ofertado, por 36 meses, com atendimento no próximo dia útil a abertura do chamado.

4.1.24. Certificações e Comprovações

4.1.24.1. O modelo ofertado deve estar em conformidade com o padrão RoHS (Restriction of Hazardous Substances) ou com a certificação de Rotulagem Ambiental da ABNT, isto é, ser construído com substâncias que não agridem o meio ambiente tais como: cádmio (Cd),

mercúrio (Hg), cromo hexavalente (Cr(VI)), bifenilos polibromados (PBBs), éteres difenilpolibromados (PBDEs) e chumbo (Pb);

4.1.24.2. A interface Wireless ofertada deve possuir homologação junto à ANATEL comprovada através de certificado;

4.1.24.3. Comprovação de que a licitante está autorizada a comercializar o equipamento oferecido;

4.1.24.4. Comprovação de que o equipamento pertence à linha corporativa e está em linha normal de fabricação;

4.1.24.5. Comprovação de que a assistência técnica será prestada pelo fabricante ou autorizada por ele indicada;

4.1.24.6. O modelo do equipamento ofertado deverá possuir Certificado ou Relatório de Avaliação de Conformidade emitido por um órgão credenciado pelo INMETRO;

4.1.24.7. O modelo ofertado deve estar em conformidade com a certificação Energy Star;

4.1.24.8. Para comprovação das certificações acima, será dispensado à apresentação das mesmas, quando constar essas informações no catálogo do produto;

4.1.24.9. Deverá apresentar o(s) documento(s) que comprove(m) o registro INPI da marca (Marca Registrada) do equipamento oferecido;

4.1.24.10. A empresa vencedora será responsável pela instalação, configuração e migração dos dados (se houver), do antigo equipamento para o novo;

4.1.24.11. A(s) empresa(s) participante(s) deverá(ão) apresentar catálogos com as características dos equipamentos ofertados, se necessário, dos acessórios que componham o solicitado, fornecendo os elementos que, de forma inequívoca, identifiquem e constatem as configurações cotadas sob pena de desclassificação. Constar na proposta comercial a marca e o modelo, que deverão ser identificados no material fornecido como comprovação. Catálogos ou outros documentos genéricos e/ou de família de produtos, onde não constem o modelo ou código oferecido serão desconsiderados.

4.1.25. <u>Monitor</u>

4.1.25.1. Deverá ser fornecido 01 (um) monitor para cada microcomputador portátil;

4.1.25.2. Tela LED com área de visão de 21,5 polegadas e com tratamento antirreflexo;

4.1.25.3. Resolução suportada nas interfaces digitais de 1920 x 1080;

4.1.25.4. Possuir ajuste de altura e inclinação;

4.1.25.5. Possuir interface digital nativa 01 (uma) HDMI ou DP e 01 (uma) analógica;

4.1.25.6. Possuir 01 (uma) fenda para fixação de cabo ou trava antifurto;

4.1.25.7. Brilho de 250cd/m2;

4.1.25.8. Ângulo de visão 160o H x V 160o;

4.1.25.9. Possuir contraste típico mínimo de 3000:1;

4.1.25.10. Fonte interna bivolt automática;

4.1.25.11. Possuir furação tipo vesa 100x100;

4.1.25.12. Possuir o mínimo de suporte de cor de 16,7 milhões de cores;

4.1.25.13. Possuir a mesma graduação de cores e ser do mesmo fabricante do equipamento;

4.1.25.14. Possuir certificação RoHS, EPEAT e Energy Star;

4.1.25.15. Acompanhar cabo de sinal digital e cabo de força;

4.1.25.16. Garantia de 03 anos.

4.2. Microcomputador Portátil - Tipo II

4.2.1. Processador

4.2.1.1. 01 (um) processador, padrão de arquitetura do processador x86 de 32 bits com suporte à extensão 64 bits;

4.2.1.2. Deverá ser da última geração disponibilizada pelo fabricante do equipamento do notebook;

4.2.1.3. Processador com índice mínimo de 10.000 (dez mil) pontos tendo como referência a base de dados *Passmark CPU Mark* disponível no site: https://www.cpubenchmark.net/cpu_list.php

4.2.1.4. Deverá ter frequência mínima real (CLOCK) de 2.8 GHZ e cache de 12 MB;

4.2.1.5. Deverá conter no mínimo 4 (quatro) núcleos de processamento real;

4.2.1.6. Deverá possuir capacidade de execução simultânea de, no mínimo, 8 (oito) “threads”;

4.2.1.7. Deverá suportar as memórias DDR4-3200 e LPDDR4x-4267;

4.2.1.8. O processador deverá ter litografia de 10 (dez) nanômetros;

4.2.1.9. O processador deverá possuir recurso compatível com a tecnologia Speed Shif ou outra para selecionar mais rapidamente sua melhor frequência de operação e sua melhor tensão para desempenho ótimo e máxima eficiência de energia;

4.2.1.10. Deverá implementar tecnologia de monitoramento térmico;

4.2.1.11. O processador deve suportar expansão com a utilização da porta Thunderbolt 4 para ajustar dinamicamente a largura de banda de dados e vídeo dependendo do dispositivo e/ou aplicação;

4.2.1.12. Possuir tecnologia para Virtualização.

4.2.2. Memória Ram

4.2.2.1. Deverá ser fornecido com, no mínimo, 16GBytes de memória RAM;

4.2.2.2. Padrão DDR4-3200 ou superior.

4.2.3. BIOS e Segurança

4.2.3.1. O BIOS deverá ser do tipo Flash Memory, utilizando memória não volátil e eletricamente reprogramável;

4.2.3.2. A inicialização do notebook deverá ser realizada na sequência definida pelo usuário, via dispositivos pela porta USB e/ou CDROM e/ou disco rígido, bem como pela placa de rede através do recurso WOL (Wake on LAN) compatível com o padrão PXE (Pré-boot Execution Enviroment);

4.2.3.3. Deverá possuir recursos de controle de permissão através de senhas, uma para inicializar o notebook, para acessar o HD e outra para acesso e alterações das configurações do BIOS;

4.2.3.4. Deverá possuir leitor de digital e bloqueio de visualização pela webcam;

4.2.3.5. Deverá possuir, integrado ao hardware do notebook, subsistema de segurança TPM (Trusted Plataform Module) compatível com a norma TPM Specification Version 2.0 especificadas pelo TCG (Trusted Computing Group).

4.2.4. Portas de Comunicação

4.2.4.1. 02 (duas) portas USB, sendo 01 (uma) 3.2;

4.2.4.2. 01 (uma) porta HDMI 1.4b;

4.2.4.3. 01 (uma) porta da interface de rede padrão RJ45;

4.2.4.4. 01 (uma) porta de entrada áudio e 01 (uma) porta de saída de áudio ou 01 (uma) porta combo para microfone ou fone de ouvido;
4.2.4.5. 01 (um) porta Thunderbolt 4 com adaptador para DP + HDMI + passagem de energia.

4.2.5. Interface De Rede
4.2.5.1. 01 (uma) interface de rede;
4.2.5.2. Conector RJ45;
4.2.5.3. Interface de rede padrão Gigabit Ethernet;
4.2.5.4. Deverá operar automaticamente nas velocidades de comunicação de 100Mbps ou 1000Mbps;
4.2.5.5. Deverá suportar Wake-on-LAN.

4.2.6. Interface Wireless
4.2.6.1. 01 (uma) interface Wireless;
4.2.6.2. Deverá estar integrada a system board ou instalada no slot M.2;
4.2.6.3. Compatibilidade funcional e operacional com o padrão IEEE 802.11ax.

4.2.7. Interface Bluetooth
4.2.7.1. Deverá possuir, para comunicação wireless, padrão Bluetooth 5.1 integrado;
4.2.7.2. A interface deverá estar integrada a system board ou em slot M.2.

4.2.8. Controladora de Vídeo
4.2.8.1. Padrão de barramento da controladora de vídeo do tipo on-board, PCI Express ou superior;
4.2.8.2. Frequência de 1.3GHz;
4.2.8.3. Suportar resolução gráfica 4096x2160 para a tela nativa e monitores externos;
4.2.8.4. Suportar a ligação de até mais 2 monitores independentes.

4.2.9. Controladora De Disco
4.2.9.1. 01 (uma) controladora M.2.

4.2.10. Armazenamento
4.2.10.1. Deverá ser fornecido com 01 (uma) unidade de 256Gb;
4.2.10.2. Tipo interno ao gabinete;
4.2.10.3. Disco padrão M.2;
4.2.10.4. Interface PCIe 3.0x4.

4.2.11. Kit De Áudio
4.2.11.1. Deverá ser fornecido 01 (um) Kit de Áudio composto por 01 (uma) Controladora de som, 02 (dois) alto-falantes internos e 01 (um) Headset USB-A mono aural com controle de volume, botão mute, gerenciamento de chamada e cancelamento de ruído e proteção contra picos de som;

4.2.11.2. A controladora de som deverá ser onboard, contendo 01 (uma) saída amplificada para canais estéreos e 01 (uma) entrada para microfone ou combo de áudio (microfone/fone de ouvido em uma única saída);
4.2.11.3. Os alto-falantes deverão estar integrados ao gabinete do notebook com amplificador de sinal e potência de 2W por canal.

4.2.12. Webcam
4.2.12.1. 01 (uma) Webcam integrada ao gabinete do notebook;
4.2.12.2. Resolução de 720p.

4.2.13. Teclado
4.2.13.1. Integrado: Compatibilidade com o padrão ABNT Variant 2;
4.2.13.2. Teclado alfanumérico com 12 teclas de função e teclas combinadas para acesso rápido;
4.2.13.3. A impressão sobre as teclas deverá ser do tipo permanente, não podendo apresentar desgastes por abrasão ou por uso prolongado.
4.2.13.4. Acompanhar teclado externo:
4.2.13.5. Dimensões (CxLxA) 400 x 120 x 20mm;
4.2.13.6. Possuir teclado numérico com 10 teclas;
4.2.13.7. Sem fio;
4.2.13.8. Ambos resistentes ao derramamento de líquidos;
4.2.13.9. Acompanhar pilhas com autonomia de 12 meses.

4.2.14. Mouse
4.2.14.1. Tipo Touchpad ou TrackPoint integrado ao gabinete;
4.2.14.2. Acompanhar um mouse externo;
4.2.14.3. Ambidestro;
4.2.14.4. Óptico com 3 botões;
4.2.14.5. Sem fio e compartilhando o mesmo receptor do teclado;
4.2.14.6. Dimensões (CxLxA) 110 x 60 x 40mm;
4.2.14.7. Acompanhar pilhas com autonomia de 12 meses.

4.2.15. Tela
4.2.15.1. Formato padrão 16:9;
4.2.15.2. Tamanho da tela de vídeo de 14 polegadas com superfície com tratamento antirreflexo;
4.2.15.3. Suportar resolução gráfica de 1920 x 1080 pixels;
4.2.15.4. Ângulo de visão 90º;
4.2.15.5. Brilho de 200cd;
4.2.15.6. Contraste de 500:1.

4.2.16. Fonte de Alimentação
4.2.16.1. A fonte deverá operar com tensão de entrada de 100 a 240VAC;
4.2.16.2. Frequência de operação de 50Hz a 60Hz;
4.2.16.3. Potência entre 60W e 80W;
4.2.16.4. Conector USB-C 3 pinos.

4.2.17. Bateria Principal

4.2.17.1. A bateria deverá ser do tipo Íons de Lítio ou Polímero de Lítio de, no mínimo, 45Wh;

4.2.17.2. O tempo de recarga da bateria para 80% de carga deverá ser de, no máximo, 1 (uma) hora;

4.2.17.3. A autonomia deve ser, no mínimo, de 8 horas.

4.2.18. Gabinete

4.2.18.1. Gabinete monobloco com todos os conectores das portas de comunicação solicitada;

4.2.18.2. O gabinete deverá ter estrutura robusta, revestido com composto de carbono, liga de magnésio, alumínio, titânio, polímero, fibra de vidro ou a mesclagem deles, para proteção contra impactos, com acabamento de alta resistência para maior durabilidade;

4.2.18.3. Botão liga/desliga, hibernação e deverá possuir dispositivo de proteção para prevenir o desligamento acidental do mesmo;

4.2.18.4. Deverá possuir 01 (uma) fenda para fixação e acompanhar o cabo ou trava antifurto que permita prender o notebook em objetos ou móveis fixos;

4.2.18.5. Possuir certificação de que foi submetido a pelo menos 3 testes dentre esses: temperatura, pressão, imersão, choque, acústica, vibração e umidade.

4.2.19. Dimensões

4.2.19.1. O peso do notebook deverá ser de, no máximo, 1,60 kg inclusos o disco rígido e a bateria principal;

4.2.19.2. A espessura (altura) do notebook deverá ser no máximo de 200 mm com a bateria instalada.

4.2.20. Sistema Operacional e Drivers

4.2.20.1. Deverá ser entregue com 01 (uma) licença do sistema operacional corporativo MS-Windows Professional 64bits na versão mais recente em idioma português/Brasil. O recovery do sistema operacional ofertado deverá ser disponibilizado em uma partição do disco rígido do equipamento ou em mídias óticas;

4.2.20.2. O notebook e todos os seus periféricos deverão ser compatíveis com o sistema operacional oferecido;

4.2.20.3. O notebook deve estar certificado no HCL (Hardware Compatibility List) da Microsoft para o sistema operacional ofertado, que deve ser comprovado através de certificado obtido através do link: https://sysdev.microsoft.com/en-US/Hardware/lpl/

4.2.20.4. Deverá indicar em sua proposta comercial, link do fabricante onde possam ser baixados atualizações, firmwares, manuais, documentos, drivers e softwares e, ainda, consultadas especificações e status da garantia, bastando inserir o número de série do equipamento, sem qualquer ônus adicional à Câmara Municipal.

4.2.21. Mochila

4.2.21.1. Para notebooks de até 15,6";

4.2.21.2. Possuir alça de transporte para mão e costas;

4.2.21.3. Cor com graduação escura;

4.2.21.4. Possuir compartimento específico para acomodar o notebook;

4.2.21.5. Possuir bolsos para acessórios com zíper em nylon;
4.2.21.6. Possuir porta externa e cabo interno para ligação de power bank, tornando o carregamento mais simples.

4.2.22. Qualidade do Equipamento
4.2.22.1. Deverá possuir identificação impressa com o nome do fabricante, modelo e número de série. Estas identificações não poderão ser feitas com etiquetas de fácil remoção ou danificação.

4.2.23. Assistência Técnica
4.2.23.1. Garantia prestada no local da CONTRATANTE ("on-site") para o notebook ofertado, por 36 meses, com atendimento no próximo dia útil a abertura do chamado.

4.2.24. Certificações e Comprovações
4.2.24.1. O modelo do equipamento ofertado deverá estar registrado no EPEAT (Electronic Product Environmental Assessment Tool) da Agência de Proteção Ambiental na categoria Gold, no site: http://www.epeat.net ou a certificação de Rotulagem Ambiental da ABNT, comprovando que o equipamento atinge as exigências para controle do impacto ambiental em seu processo de fabricação;
4.2.24.2. O modelo ofertado deve estar em conformidade com o padrão RoHS (Restriction of Hazardous Substances) ou com a certificação de Rotulagem Ambiental da ABNT, isto é, ser construído com substâncias que não agridem o meio ambiente tais como: cádmio (Cd), mercúrio (Hg), cromo hexavalente (Cr(VI)), bifenilos polibromados (PBBs), éteres difenilpolibromados (PBDEs) e chumbo (Pb);
4.2.24.3. A interface Wireless ofertada deve possuir homologação junto à ANATEL comprovada através de certificado;
4.2.24.4. Comprovação de que a licitante está autorizada a comercializar o equipamento oferecido;
4.2.24.5. Comprovação de que o equipamento pertence a linha corporativa e está em linha normal de fabricação;
4.2.24.6. Comprovação de que a assistência técnica será prestada pelo fabricante ou autorizada por ele indicada;
4.2.24.7. O modelo do equipamento ofertado deverá possuir Certificado ou Relatório de Avaliação de Conformidade emitido por um órgão credenciado pelo INMETRO;
4.2.24.8. O modelo ofertado deve estar em conformidade com a certificação Energy Star e TCO;
4.2.24.9. Para comprovação das certificações acima, será dispensada a apresentação das mesmas, quando constar essas informações no catálogo do produto;
4.2.24.10. Deverá apresentar o(s) documento(s) que comprove(m) o registro INPI da marca (Marca Registrada) do equipamento oferecido;
4.2.24.11. A empresa vencedora será responsável pela instalação, configuração e migração dos dados (se houver), do antigo equipamento para o novo;
4.2.24.12. A(s) empresa(s) participante(s) deverá(ão) apresentar catálogos com as características dos equipamentos ofertados, se necessário, dos acessórios que componham o solicitado, fornecendo os elementos que, de forma inequívoca, identifiquem e constatem as configurações cotadas sob pena de desclassificação. Constar na proposta comercial a

marca e o modelo, que deverão ser identificados no material fornecido como comprovação. Catálogos ou outros documentos genéricos e/ou de família de produtos onde não constem o modelo ou código oferecido serão desconsiderados.

4.2.25. Monitor
4.2.25.1. Deverá ser fornecido 01 (um) monitor para cada microcomputador portátil;
4.2.25.2. Tela LED entre 24 e 25 polegadas com tratamento antirreflexo;
4.2.25.3. Resolução suportada nas interfaces digitais de 1920 x 1080;
4.2.25.4. Possuir ajuste de altura, inclinação, giro e rotação;
4.2.25.5. Possuir interfaces digitais nativas, 01 (uma) Display Port e 02 (duas) HDMI;
4.2.25.6. Possuir 01 (uma) fenda para fixação de cabo ou trava antifurto;
4.2.25.7. Taxa de atualização de no mínimo 60Hz;
4.2.25.8. Possuir acessório com ângulo para ajuste ao ambiente;
4.2.25.9. Acompanhar controle externo de acesso rápido das configurações;
4.2.25.10. Brilho de 320cd/m2;
4.2.25.11. Possuir tecnologia Flicker-free;
4.2.25.12. Possuir contraste típico mínimo de 1000:1;
4.2.25.13. Fonte interna bivolt automática;
4.2.25.14. Possuir furação tipo vesa 100x100;
4.2.25.15. Possuir o mínimo de suporte de cor de 16,7 milhões de cores;
4.2.25.16. Acompanhar capa de proteção, cabo de sinal e cabo de força.

4.3. Microcomputador - Tipo III

4.3.1. Processador
4.3.1.1. Processador com índice de 20.000 (vinte mil) pontos tendo como referência a base de dados *Passmark CPU Mark* disponível no site: http://www.cpubenchmark.net/
4.3.1.2. Deverá ter frequência mínima real (CLOCK) de 2.1 GHZ e cache em 16 MB;
4.3.1.3. Deverá conter no mínimo 8 (oito) núcleos de processamento real;
4.3.1.4. Deverá possuir capacidade de execução simultânea de 16 (dezesseis) “threads”;
4.3.1.5. O processador deverá ter litografia de 14 (quatorze) nanômetros.

4.3.2. Memória Principal
4.3.2.1. Devera possuir 32 (trinta e dois) gigabytes de memória instalada;
4.3.2.2. Instalados de forma a utilizar a tecnologia dual-channel;
4.3.2.3. Possuir tecnologia DDR-4 com frequência de 3200MHz.

4.3.3. BIOS
4.3.3.1. O equipamento deverá possuir BIOS que deverá ser do mesmo fabricante do equipamento ou que tenha direitos de copyright sobre esse BIOS. Deverá possuir livre direito de edição sobre a mesma, garantindo assim adaptabilidade do conjunto adquirido. Não serão aceitas soluções em regime de OEM, customizações ou apenas cessão de direitos limitados;
4.3.3.2. Possibilitar que a senha de acesso ao BIOS seja ativada e desativada via SETUP;

4.3.3.3. Deverá o equipamento dispor de software para diagnóstico de problemas com as seguintes características: A fim de permitir o teste do equipamento em 2 modos, sendo básico e avançado (teste de stress), com independência do sistema operacional instalado, o software de diagnóstico deve ser capaz de ser executado (inicializado) a partir da UEFI (Unified Extensible Firmware Interface) ou do Firmware do equipamento através do acionamento de tecla função (F1...F12);

4.3.3.4. O software de diagnóstico deverá ser capaz de informar, através de tela gráfica o fabricante, modelo do equipamento; número de série e realizar testes dos componentes: processador; placa de vídeo; memória RAM; disco rígido; portas de comunicação. Deverá verificar testar e emitir relatório, através de tela gráfica que mostre o andamento do teste, dos seguintes componentes: Processador; Memória; Disco (ou memória de armazenamento);

4.3.3.5. Possibilitar que a senha de acesso ao BIOS seja ativada e desativada via SETUP;

4.3.3.6. Chip de segurança TPM versão 2.0 integrado para criptografia, gerenciamento e o fabricante deverá constar no site: http://www.trustedcomputinggroup.org/members

4.3.4. Placa Mãe

4.3.4.1. Ser de fabricação própria e exclusiva para o modelo ofertado. Não ser produzida em regime de OEM ou personalizada;

4.3.4.2. Possuir 3 (três) slots PCI e (PCI Express), sendo uma delas obrigatoriamente no padrão 4.0 x16 e 1 (um) slots M.2 livre;

4.3.4.3. Deve possuir 4 (quatro) slots e suportar expansão até 128 GB de memória, sendo obrigatoriamente 2 (dois) disponíveis para expansão;

4.3.4.4. O chipset deve pertencer à geração mais recente disponibilizada pelo fabricante sendo compatível com o processador ofertado.

4.3.5. Armazenamento

4.3.5.1. 01 (uma) unidade de disco flash interna do tipo SSD de 256Gb no padrão M.2 NVMe e 01 (uma) unidade de disco rígido SATA de 1TB com 7.200 RPM;

4.3.5.2. A controladora de discos deverá ser integrada à placa mãe, com taxa de transferência mínima de 6.0 Gb/s.

4.3.6. Controladora de Rede

4.3.6.1. Possuir capacidade de comunicação de 100 e 1000 Mbps, com reconhecimento automático da velocidade da rede;

4.3.6.2. Possuir conector do tipo RJ-45 fêmea;

4.3.6.3. Deverá suportar Wake-on-LAN.

4.3.7. Controladora Wireless

4.3.7.1. Deverá estar integrada ao equipamento;

4.3.7.2. Compatibilidade funcional e operacional com os padrões IEEE 802.11ax Dual Band;

4.3.7.3. Integrar Bluetooth 5.1.

4.3.8. Controladora de Vídeo

4.3.8.1. Suportar a Resolução de 3840x2160@ 1200Hz;

4.3.8.2. Possuir 04 (quatro) DisplayPort ou mDP 1.4;
4.3.8.3. Possuir Memória de 6GB GDDR6 com 128bit;
4.3.8.4. Possibilitar a ligação de até 04 (quatro) monitores simultaneamente com a resolução acima;
4.3.8.5. Interface PCI-e 3.0 x16 single slot;
4.3.8.6. Compatível com OpenGl 4.6 e DirectX 12.0;
4.3.8.7. Acompanhar dois cabos mDP x HDMI 2.0.

4.3.9. Controladora de Áudio
4.3.9.1. Deverá ser integrada à placa mãe;
4.3.9.2. Ser HD;
4.3.9.3. Possuir conectores frontais para Headphone e microfone, sendo aceita interface tipo combo e conectores traseiros 3,5mm para I/O e mic.

4.3.10. Gabinete
4.3.10.1. Deve suportar a configuração completa de acessórios e componentes do equipamento;
4.3.10.2. Deve ser do tipo desktop torre;
4.3.10.3. Deve possuir sensor para alerta de abertura de gabinete e slot para instalação de trava de segurança;
4.3.10.4. Possuir 06 (seis) conectores USB, sendo 04 deles no padrão 3.2 e localizados na parte frontal, todos fazendo parte do projeto sem a utilização de hubs, placas ou adaptadores;
4.3.10.5. Possuir porta combo para fone e microfone com conector 3,5mm na parte frontal, e 01 (uma) porta de saída de áudio na parte traseira;
4.3.10.6. Acompanhar Teclado e Mouse com fio e interface USB do mesmo fabricante;
4.3.10.7. Deverá possuir fonte de alimentação com tensão de entrada 110/220 VAC automática, com potência mínima de 500W e eficiência energética de 90% com certificação 80Plus.

4.3.11. Sistema Operacional e Outros
4.3.11.1. Deverá acompanhar licença OEM do Microsoft Windows 11 Pro especifico para o equipamento e no idioma Português (Brasil) com opção de downgrade para versão anterior;
4.3.11.2. Todos os drivers necessários para o pleno funcionamento do equipamento deverão estar inclusos e disponíveis via website do fabricante;
4.3.11.3. Deverá indicar em sua proposta comercial, link do fabricante onde possam ser baixados atualizações, firmwares, manuais, documentos, drivers e softwares e ainda consultado especificações e status da garantia, bastando inserir o número de série do equipamento, sem qualquer ônus adicional à Câmara Municipal de Santo André.

4.3.12. Assistência Técnica
4.3.12.1. Garantia prestada no local da CONTRATANTE (“on-site”) para o microcomputador ofertado, por 36 meses, com atendimento no próximo dia útil a abertura do chamado.

4.3.13. Certificações e Comprovações - Computador
4.3.13.1. Comprovação de que o fabricante dos equipamentos ofertados possui banco de dados disponibilizado na Internet que permita obter a configuração de hardware e software,

periféricos internos e drivers de instalação atualizados e disponíveis para download a partir do n.º de série dos mesmos;

4.3.13.2. Nenhum dos equipamentos fornecidos poderá conter substâncias perigosas como mercúrio (Hg), chumbo (Pb), cromo hexavalente (Cr(VI)), cádmio (Cd), bifenil polibromados (PBBs), éteres difenil-polibromados (PBDEs), em concentração acima da recomendada na diretiva RoHS (Restriction of Certain Hazardous Substances);

4.3.13.3. A interface Wireless ofertada deve possuir homologação junto à ANATEL comprovada através de certificado;

4.3.13.4. Todos os equipamentos a serem entregues deverão ser idênticos, ou seja, todos os componentes externos e internos de mesmos modelos e marcas dos utilizados nos equipamentos enviados para avaliação e/ou homologação. Caso o componente não mais se encontre disponível no mercado, admitem-se substitutos com qualidade e características idênticas ou superiores, mediante nova homologação;

4.3.13.5. A(s) empresa(s) participante(s) deverá(ão) apresentar catálogos com as características dos equipamentos ofertados, se necessário, dos acessórios que componham o solicitado, fornecendo os elementos que, de forma inequívoca, identifiquem e constatem as configurações cotadas sob pena de desclassificação. Constar na proposta comercial a marca e o modelo, que deverão ser identificados no material fornecido como comprovação. Catálogos ou outros documentos genéricos e/ou de família de produtos onde não constem o modelo ou código oferecido serão desconsiderados;

4.3.13.6. O Microcomputador deverá atender as normas EPEAT Silver e ENERGY STAR;

4.3.13.7. Comprovação de Inmetro;

4.3.13.8. A fonte deve possuir a certificação 80 Plus Platinum;

4.3.13.9. Para comprovação das certificações acima, será dispensada a apresentação das mesmas, quando constar essas informações no catálogo do produto.

4.3.14. <u>Monitor</u>

4.3.14.1. Deverão ser fornecidos 02 (dois) monitores para cada microcomputador;

4.3.14.2. Tela IPS 27 polegadas com tratamento antirreflexo;

4.3.14.3. Resolução de 2560 x 1440;

4.3.14.4. Possuir ajuste de altura, inclinação, giro e rotação;

4.3.14.5. Possuir interfaces nativas, 02 (duas) Display Port, 01 (uma) HDMI e 03 (três) USB 3.1;

4.3.14.6. Possuir 01 (uma) fenda para fixação de cabo ou trava antifurto;

4.3.14.7. Ângulo de visão de 170 x 170 (H/V);

4.3.14.8. Possuir áudio estéreo;

4.3.14.9. Brilho de 350cd/m2;

4.3.14.10. Tempo de resposta 4ms;

4.3.14.11. Possuir contraste típico mínimo de 1000:1;

4.3.14.12. Fonte interna bivolt automática;

4.3.14.13. Possuir a mesma graduação de cores e ser do mesmo fabricante do equipamento;

4.3.14.14. Possuir furação tipo vesa 100x100;

4.3.14.15. Possuir o mínimo de suporte de cor de 16,7 milhões de cores;

4.3.14.16. Acompanhar cabo de sinal e cabo de força.

4.4. Softwares

4.4.1. Antivírus

4.4.1.1. Características Gerais

- A solução deverá ter vigência mínima de 12 (doze) meses com possibilidade de eventual prorrogação nos termos da lei;
- A console de Administração deverá estar alocada em ambiente da CONTRATANTE.

4.4.1.2. A Console de Administração da Solução deverá ser compatível com os seguintes Sistemas Operacionais:

- Microsoft Windows Server 2008 (Todas edições);
- Microsoft Windows Server 2008 x64 SP1 (Todas edições);
- Microsoft Windows Server 2008 R2 (Todas edições);
- Microsoft Windows Server 2012 (Todas edições);
- Microsoft Windows Server 2012 R2 (Todas edições);
- Microsoft Windows Server 2016 x64;
- Microsoft Windows Server 2019 x64 (Todas as edições);
- Microsoft Windows Small Business Server 2008 (Todas edições);
- Microsoft Windows Small Business Server 2011 (Todas edições);
- Microsoft Windows XP Professional SP2 ou superior;
- Microsoft Windows XP Professional x64 SP2 ou superior;
- Microsoft Windows Vista Business / Enterprise / Ultimate SP1 ou posterior;
- Microsoft Windows Vista Business / Enterprise / Ultimate SP1 x64 ou posterior;
- Microsoft Windows 7 SP1 Professional / Enterprise/Ultimate x32/x64;
- Microsoft Windows 7 SP1 Professional / Enterprise/Ultimate x32/x64;
- Microsoft Windows 8 SP1 Professional / Enterprise x32/x64;
- Microsoft Windows 8 Professional / Enterprise x64;
- Microsoft Windows 8.1 Professional / Enterprise x32;
- Microsoft Windows 8.1 Professional / Enterprise x64;
- Microsoft Windows 10 todas edições x32;
- Microsoft Windows 10 todas edições x64.

Deverá ser compatível com as seguintes plataformas virtuais:

- Vmware: Workstation 12.x Pro, vSphere 5.5, vSphere 6.x;
- Microsoft Hyper-V: 2008, 2008 R2, 2008 R2 SP1, 2012, 2012 R2, 2016;
- Microsoft VirtualPC 6.0.156.0;
- Parallels Desktop 7 e 11;
- Oracle VM VirtualBox 4.0.4-70112 (Somente logon como convidado).

4.4.1.3. Características Gerais da Console de Gerenciamento

- A console deve ser acessada via WEB (HTTPS) ou MMC;
- Console deve ser baseada no modelo cliente/servidor;
- Compatibilidade com Windows Failover Clustering ou outra solução de alta disponibilidade;

- Deve permitir a atribuição de perfis para os administradores da Solução de Antivírus;
- Deve permitir incluir usuários do AD para logarem na console de Administração;
- Console deve ser totalmente integrada com suas funções e módulos caso haja a necessidade no futuro de adicionar novas tecnologias tais como, criptografia, Patch management e MDM;
- As licenças deverão ser perpétuas, ou seja, expirado a validade da mesma o produto deverá permanecer funcional para a proteção contra códigos maliciosos utilizando as definições até o momento da expiração da licença;
- Capacidade de remover remotamente e automaticamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores;
- Capacidade de instalar remotamente a solução de antivírus nas estações e servidores Windows, através de compartilhamento administrativo, login script e/ou GPO de Active Directory;
- Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria;
- Deve armazenar histórico das alterações feitas em políticas;
- Deve permitir voltar para uma configuração antiga da política de acordo com o histórico de alterações efetuadas pelo administrador apenas selecionando a data em que a política foi alterada;
- Deve ter a capacidade de comparar a política atual com a anterior, informando quais configurações foram alteradas;
- A solução de gerencia deve permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas;
- Através da solução de gerência, deve ser possível verificar qual licença está aplicada para determinado computador;
- Capacidade de instalar remotamente a solução de segurança em smartphones e tablets de sistema iOS e Android;
- Capacidade de instalar remotamente qualquer “app” em smartphones e tablets de sistema iOS;
- A solução de gerência centralizada deve permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle;
- Deverá ter a capacidade de criar regras para limitar o tráfego de comunicação cliente/servidor por sub-rede com os seguintes parâmetros: KB/s e horário;
- Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux e Mac) protegidos pela solução antivírus;
- Capacidade de gerenciar smartphones e tablets (Android e iOS) protegidos pela solução de segurança;
- Capacidade de instalar atualizações em computadores de teste antes de instalar nos demais computadores da rede;
- Capacidade de gerar pacotes customizados (auto executáveis) contendo a licença e configurações do produto;
- Capacidade de atualizar os pacotes de instalação com as últimas vacinas;
- Capacidade de fazer distribuição remota de qualquer software, ou seja, deve ser capaz de remotamente enviar qualquer software pela estrutura de gerenciamento de antivírus para que seja instalado nas máquinas clientes;
- A comunicação entre o cliente e o servidor de administração deve ser criptografada;
- Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes;

- Deve permitir a realocação de máquinas novas na rede para um determinado grupo sem ter um agente ou endpoint instalado utilizando os seguintes parâmetros:
  - ✓ Nome do computador;
  - ✓ Nome do domínio;
  - ✓ Range de IP;
  - ✓ Sistema Operacional;
  - ✓ Máquina virtual.
- Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas;
- Deve permitir, por meio da console de gerenciamento, extrair um artefato em quarentena de um cliente sem a necessidade de um servidor ou console de quarentena adicional;
- Capacidade de monitorar diferentes subnets de rede a fim de encontrar máquinas novas para serem adicionadas à proteção;
- Capacidade de monitorar grupos de trabalhos já existentes e quaisquer grupos de trabalho que forem criados na rede, a fim de encontrar máquinas novas para serem adicionadas a proteção;
- Capacidade de, assim que detectar máquinas novas no Active Directory, subnets ou grupos de trabalho, automaticamente importar a máquina para a estrutura de proteção da console e verificar se possui o antivírus instalado. Caso não possuir, deve instalar o antivírus automaticamente;
- Capacidade de agrupamento de máquina por características comuns entre as mesmas, por exemplo: agrupar todas as máquinas que não tenham o antivírus instalado, agrupar todas as máquinas que não receberam atualização nos últimos 2 dias, etc.;
- Capacidade de definir políticas de configurações diferentes por grupos de estações, permitindo que sejam criados subgrupos e com função de herança de políticas entre grupos e subgrupos;
- Deve fornecer as seguintes informações dos computadores:
  - ✓ Se o antivírus está instalado;
  - ✓ Se o antivírus está iniciado;
  - ✓ Se o antivírus está atualizado;
  - ✓ Minutos/horas desde a última conexão da máquina com o servidor administrativo;
  - ✓ Minutos/horas desde a última atualização de vacinas;
  - ✓ Data e horário da última verificação executada na máquina;
  - ✓ Versão do antivírus instalado na máquina;
  - ✓ Se é necessário reiniciar o computador para aplicar mudanças;
  - ✓ Data e horário de quando a máquina foi ligada;
  - ✓ Quantidade de vírus encontrados (contador) na máquina;
  - ✓ Nome do computador;
  - ✓ Domínio ou grupo de trabalho do computador;
  - ✓ Data e horário da última atualização de vacinas;
  - ✓ Sistema operacional com Service Pack;
  - ✓ Quantidade de processadores;
  - ✓ Quantidade de memória RAM;
  - ✓ Usuário(s) logado(s) naquele momento, com informações de contato (caso disponíveis no Active Directory);
  - ✓ Endereço IP;

- ✓ Aplicativos instalados, inclusive aplicativos de terceiros, com histórico de instalação, contendo data e hora que o software foi instalado ou removido;
- ✓ Atualizações do Windows Updates instaladas;
- ✓ Informação completa de hardware contendo: processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de áudio, adaptadores de rede, monitores, drives de CD/DVD;
- ✓ Vulnerabilidades de aplicativos instalados na máquina;

- Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterá-las;
- Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como:
  - ✓ Alteração de Gateway Padrão;
  - ✓ Alteração de sub-rede;
  - ✓ Alteração de domínio;
  - ✓ Alteração de servidor DHCP;
  - ✓ Alteração de servidor DNS;
  - ✓ Alteração de servidor WINS;
  - ✓ Alteração de sub-rede;
  - ✓ Resolução de Nome;
  - ✓ Disponibilidade de endereço de conexão SSL;
- Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet;
- Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes;
- Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus;
- Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos;
- Capacidade de eleger qualquer computador cliente como repositório de vacinas e de pacotes de instalação, sem que seja necessária a instalação de um servidor administrativo completo, onde outras máquinas clientes irão atualizar-se e receber pacotes de instalação, a fim de otimizar tráfego da rede;
- Capacidade de fazer deste repositório de vacinas um gateway para conexão com o servidor de administração, para que outras máquinas que não consigam conectar-se diretamente ao servidor possam usar este gateway para receber e enviar informações ao servidor administrativo;
- Capacidade de exportar relatórios para os seguintes tipos de arquivos: PDF, HTML e XML;
- Capacidade de gerar traps SNMP para monitoramento de eventos;
- Capacidade de enviar e-mails para contas específicas em caso de algum evento;
- Listar em um único local, todos os computadores não gerenciados na rede;
- Deve encontrar computadores na rede através de no mínimo três formas: Domínio, Active Directory e sub-redes;
- Deve possuir compatibilidade com Microsoft NAP, quando instalado em um Windows 2008 Server;
- Deve possuir compatibilidade com Cisco Network Admission Control (NAC);

- Capacidade de baixar novas versões do antivírus direto pela console de gerenciamento, sem a necessidade de importá-los manualmente;
- Capacidade de ligar máquinas via Wake on Lan para realização de tarefas (varredura, atualização, instalação, etc), inclusive de máquinas que estejam em subnets diferentes do servidor;
- Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado intervalo de tempo);
- Deve através de opções de optimizações fazer com que o computador gerenciado conceda recursos à outras aplicações, mantendo o antivírus ativo porém sem comprometer o desempenho do computador;
- Deve permitir a configuração de senha no endpoint e configurar quando que será necessário a utilizá-la, (ex: Solicitar senha quando alguma tarefa de scan for criada localmente no endpoint);
- Permitir fazer uma verificação rápida ou detalhada de um dispositivo removível assim que conectado no computador, podendo configurar a capacidade máxima em GB da verificação;
- Deve ser capaz de configurar quais eventos serão armazenados localmente, nos eventos do Windows ou ainda se serão mostrados na tela para o colaborador, sejam estes eventos informativos, de alertas ou de erros;
- Capacidade de realizar atualização incremental de vacinas nos computadores clientes;
- Deve armazenar localmente e enviar ao servidor de gerência a ocorrência de vírus com os seguintes dados, no mínimo:
  - ✓ Nome do vírus;
  - ✓ Nome do arquivo infectado;
  - ✓ Data e hora da detecção;
  - ✓ Nome da máquina ou endereço IP;
  - ✓ Ação realizada.
- Capacidade de reportar vulnerabilidades de softwares presentes nos computadores;
- Capacidade de listar updates nas máquinas com o respectivo link para download;
- Deve criar um backup de todos os arquivos deletados em computadores para que possa ser restaurado através de comando na Console de administração;
- Deve ter uma quarentena na própria console de gerenciamento, permitindo baixar um artefato ou enviar direto para análise do fabricante;
- Capacidade de realizar inventário de hardware de todas as máquinas clientes;
- Capacidade de realizar inventário de aplicativos de todas as máquinas clientes;
- Capacidade de diferenciar máquinas virtuais de máquinas físicas.

4.4.1.4. Microsoft Windows - Deverá possuir compatibilidade para os seguintes sistemas operacionais:

- Microsoft Windows 7 Professional/Enterprise/Ultimate x86 / x64 e posterior;
- Microsoft Windows 8 Professional/Enterprise x86 / x64;
- Microsoft Windows 8.1 Pro / Enterprise x86 / x64;
- Microsoft Windows 10 Pro / Enterprise x86 / x64;
- Microsoft Windows Server 2012 R2 Standard x64;
- Microsoft Windows Server 2012 Foundation x64;
- Microsoft Windows Server 2012 Standard x64;

- Microsoft Small Business Server 2011 Standard x64;
- Microsoft Windows Server 2008 R2 Standard/Enterprise x64 SP1;
- Microsoft Windows Server 2008 Standard/Enterprise x86/x64 SP2;
- Microsoft Windows Server 2016 x64;
- Microsoft Windows Server 2019 x64;
- Windows Server 2008 Standard/Enterprise/Datacenter SP1 e posterior, sendo 32 bits;
- Windows Server 2008 Core Standard/Enterprise/Datacenter SP1 e posterior, sendo 32 bits;
- Microsoft Windows Server 2008 Standard / Enterprise / DataCenter (SP1 ou posterior);
- Microsoft Windows Server 2008 Core Standard / Enterprise / DataCenter (SP1 ou posterior).
- Microsoft Windows Server 2008 R2 Standard / Enterprise / DataCenter (SP1 ou posterior);
- Microsoft Windows Server 2008 R2 Core Standard / Enterprise / DataCenter (SP1 ou posterior);
- Microsoft Windows Storage Server 2008 R2;
- Microsoft Windows Storage Server 2008 SP2 Standard Edition;
- Microsoft Windows Storage Server SP2 Workgroup Edition;
- Microsoft Windows Hyper-V Server 2008 R2 SP1 e posterior;
- Microsoft Windows Server 2012 Essentials / Standard / Foundation / Datacenter;
- Microsoft Windows Server 2012 R2 Essentials / Standard / Foundation / Datacenter;
- Microsoft Windows Server 2012 Core Essentials / Standard / Foundation / Datacenter;
- Microsoft Windows Server 2012 R2 Core Essentials / Standard / Foundation / Datacenter;
- Microsoft Windows Storage Server 2012 (Todas edições);
- Microsoft Windows Storage Server 2012 R2 (Todas edições);
- Microsoft Windows Hyper-V Server 2012;
- Microsoft Windows Hyper-V Server 2012 R2;
- Windows Server 2016 Essentials/Standard/Datacenter/Core;
- Windows Storage Server 2016;
- Windows Hyper-V Server 2016.

4.4.2. Características Gerais para Microsoft Windows

- Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
- Antivírus de Web (módulo para verificação de sites e downloads contra vírus);
- Antivírus de E-mail (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos);
- Antivírus de Mensagens Instantâneas (módulo para verificação de mensagens instantâneas, como ICQ, MSN, IRC, etc);
- O Endpoint deve possuir opção para rastreamento por linha de comando, parametrizável, com opção de limpeza;
- Firewall com IDS;
- Autoproteção (contra-ataques aos serviços/processos do antivírus);
- Controle de dispositivos externos;
- Controle de acesso a sites por categoria, ex: Bloquear conteúdo adulto, sites de jogos, etc.;
- Controle de acesso a sites por horário;

- Controle de acesso a sites por usuários;
- Controle de acesso a websites por dados, ex: bloquear websites com
- Conteúdo de vídeo e áudio;
- Controle de execução de aplicativos;
- Controle de vulnerabilidades do Windows e dos aplicativos instalados;
- Capacidade de escolher quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
- As vacinas devem ser atualizadas pelo fabricante e disponibilizadas aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa);
- Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;
- Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: “Win32.Trojan. banker”) para que qualquer objeto detectado com o veredicto escolhido seja ignorado;
- Capacidade de adicionar aplicativos a uma lista de “aplicativos confiáveis”, onde as atividades de rede, atividades de disco e acesso ao registro do Windows não serão monitoradas;
- Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);
- Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
- Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;
- Ter a capacidade de fazer detecções por comportamento, identificando ameaças avançadas sem a necessidade de assinaturas;
- Capacidade de verificar somente arquivos novos e alterados;
- Capacidade de verificar objetos usando heurística;
- Capacidade de agendar uma pausa na verificação;
- Deve permitir a filtragem de conteúdo de URL avançada efetuando a classificação dos sites em categorias;
- Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;
- O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
- Perguntar o que fazer, ou;
- Bloquear acesso ao objeto;
- Apagar o objeto ou tentar desinfetá-lo (de acordo com a configuração pré-estabelecida pelo administrador).
- Caso positivo de desinfecção, restaurar o objeto para uso;
- Caso negativo de desinfecção, mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);
- Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente,
- O antivírus deve realizar um backup do objeto;

- Capacidade de verificar e-mails recebidos e enviados nos protocolos POP3, IMAP, NNTP, SMTP e MAPI, assim como conexões criptografadas (SSL) para POP3 e IMAP (SSL);
- Capacidade de verificar tráfego de ICQ, MSN, AIM e IRC contra vírus e links phishings;
- Capacidade de verificar links inseridos em e-mails contra phishings;
- Capacidade de verificar tráfego nos browsers: Internet Explorer, Firefox e Opera;
- Capacidade de verificação de corpo e anexos de e-mails usando heurística;
- O antivírus de e-mail, ao encontrar um objeto potencialmente perigoso, deve:
- Perguntar o que fazer, ou;
- Bloquear o e-mail;
- Apagar o objeto ou tentar desinfetá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
- Caso positivo de desinfecção:
- Restaurar o e-mail para o usuário;
- Caso negativo de desinfecção:
- Mover para quarentena ou apagar o objeto (de acordo com a configuração pré- estabelecida pelo administrador);
- Caso o e-mail conter código que parece ser, mas não é definitivamente malicioso, o mesmo deve ser mantido em quarentena;
- Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados;
- Capacidade de filtrar anexos de e-mail, apagando-os ou recomendo-os de acordo com a configuração feita pelo administrador;
- Capacidade de verificação de tráfego HTTP e qualquer script do Windows Script Host (Java Script, Visual Basic Script, etc), usando heurísticas;
- Deve ter suporte total ao protocolo Ipv6;
- Capacidade de alterar as portas monitoradas pelos módulos de Web e E- mail;
- Na verificação de tráfego web, caso encontrado código malicioso o programa deve:
- Perguntar o que fazer, ou;
- Bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio, ou;
- Permitir acesso ao objeto;
- O antivírus de web deve realizar a verificação de, no mínimo, duas maneiras diferentes, sob escolha do administrador:
- Verificação on-the-fly, onde os dados são verificados enquanto são recebidos em tempo real, ou;
- Verificação de buffer, onde os dados são recebidos e armazenados para posterior verificação;
- Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus de web;
- Deve possuir módulo que analise as ações de cada aplicação em execução no computador, gravando as ações executadas e comparando-as com sequências características de atividades perigosas. Tais registros de sequências devem ser atualizados juntamente com as vacinas;
- Deve possuir módulo que analise cada macro de VBA executada, procurando por sinais de atividade maliciosa;
- Deve possuir módulo que analise qualquer tentativa de edição, exclusão ou gravação do registro, de forma que seja possível escolher chaves específicas para serem monitoradas e/ou bloqueadas;

- Deve possuir módulo de bloqueio de Phishing, com atualizações incluídas nas vacinas, obtidas pelo Anti-Phishing Working Group (http://www.antiphishing.org/);
- Capacidade de distinguir diferentes subnets e conceder opção de ativar ou não o firewall para uma subnet específica;
- Deve possuir módulo IDS (Intrusion Detection System) para proteção contra port scans e exploração de vulnerabilidades de softwares. A base de dados de análise deve ser atualizada juntamente com as vacinas;
- O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:
- Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;
- Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.
- Deve possuir módulo que habilite ou não o funcionamento dos seguintes dispositivos externos, no mínimo:
  - ✓ Discos de armazenamento locais;
  - ✓ Armazenamento removível;
  - ✓ Impressoras;
  - ✓ CD/DVD;
  - ✓ Drives de disquete;
  - ✓ Modems;
  - ✓ Dispositivos de fita;
  - ✓ Dispositivos multifuncionais;
  - ✓ Leitores de smart card;
  - ✓ Dispositivos de sincronização via ActiveSync (Windows CE, Windows Mobile, etc);
  - ✓ Wi-Fi;
  - ✓ Adaptadores de rede externos;
  - ✓ Dispositivos MP3 ou smartphones;
  - ✓ Dispositivos Bluetooth;
  - ✓ Câmeras e Scanners.
- Capacidade de liberar acesso a um dispositivo e usuários por um período de tempo específico, sem a necessidade de desabilitar a proteção e o gerenciamento central ou de intervenção local do administrador na máquina do usuário;
- Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por usuário;
- Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por agendamento;
- Capacidade de habilitar “logging” em dispositivos removíveis tais como Pendrive, Discos externos, etc.
- Capacidade de configurar novos dispositivos por Class ID/Hardware ID;
- Capacidade de limitar a execução de aplicativos por hash MD5, nome do arquivo, versão do arquivo, nome do aplicativo, versão do aplicativo, fabricante/desenvolvedor, categoria (ex: navegadores, gerenciador de download, jogos, aplicação de acesso remoto, etc);
- Capacidade de bloquear execução de aplicativo que está em armazenamento externo;

- Capacidade de limitar o acesso dos aplicativos a recursos do sistema, como chaves do registro e pastas/arquivos do sistema, por categoria, fabricante ou nível de confiança do aplicativo;
- Capacidade de, em caso de epidemia, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web;
- Capacidade de, caso o computador cliente saia da rede corporativa, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web.
- Capacidade de voltar ao estado anterior após um ataque de malware, incluindo recuperação de arquivos criptografados.
- Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros.
- Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning).

4.4.3. Servidores Microsoft Windows - Características Gerais

- Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
- Autoproteção contra-ataques aos serviços/processos do antivírus;
- Firewall com IDS;
- Controle de vulnerabilidades do Windows e dos aplicativos instalados;
- Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
- As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;
- Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
- Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
- Gerenciamento de tarefa (criar ou excluir tarefas de verificação);
- Leitura de configurações;
- Modificação de configurações;
- Gerenciamento de Backup e Quarentena;
- Visualização de relatórios;
- Gerenciamento de relatórios;
- Gerenciamento de chaves de licença;
- Gerenciamento de permissões (adicionar/excluir permissões acima);
- O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:
- Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;
- Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.
- Capacidade de separadamente selecionar o número de processos que irão executar funções de varredura em tempo real, o número de processos que executarão a varredura sob demanda e o número máximo de processos que podem ser executados no total;

- Bloquear malwares tais como Cryptlockers mesmo quando o ataque vier de um computador sem antivírus na rede
- Capacidade de resumir automaticamente tarefas de verificação que tenham sido paradas por anormalidades (queda de energia, erros, etc);
- Capacidade de automaticamente pausar e não iniciar tarefas agendadas caso o servidor esteja em rodando com fonte ininterrupta de energia (uninterruptible Power supply - UPS);
- Em caso de erros, deve ter capacidade de criar logs e traces automaticamente, sem necessidade de outros softwares;
- Capacidade de configurar níveis de verificação diferentes para cada pasta, grupo de pastas ou arquivos do servidor;
- Capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado no servidor;
- Capacidade de criar uma lista de máquina que nunca serão bloqueadas mesmo quando infectadas;
- Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;
- Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: “Win32.Trojan. banker”) para que qualquer objeto detectado com o veredicto escolhido seja ignorado;
- Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
- Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;
- Capacidade de verificar somente arquivos novos e alterados;
- Capacidade de escolher qual tipo de objeto composto será verificado (ex: arquivos comprimidos, arquivos auto descompressores, .PST, arquivos compactados por compactadores binários, etc.);
- Capacidade de verificar objetos usando heurística;
- Capacidade de configurar diferentes ações para diferentes tipos de ameaças;
- Capacidade de agendar uma pausa na verificação;
- Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;
- O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
  - ✓ Perguntar o que fazer, ou;
  - ✓ Bloquear acesso ao objeto;
  - ✓ Apagar o objeto ou tentar desinfetá-lo (de acordo com a configuração pré- estabelecida pelo administrador);
  - ✓ Caso positivo de desinfecção:
  - ✓ Restaurar o objeto para uso;
  - ✓ Caso negativo de desinfecção:
  - ✓ Mover para quarentena ou apagar (de acordo com a configuração pré- estabelecida pelo administrador);
  - ✓ Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;

- ✓ Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;
- ✓ Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;
- ✓ Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa.
- ✓ Capacidade de voltar ao estado anterior após um ataque de malware, incluindo recuperação de arquivos criptografados.
- ✓ Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros
- ✓ Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning).

4.4.4. Compatibilidade de Criptografia

- Deverá ter compatibilidade de criptografia para os seguintes sistemas operacionais:
- Microsoft Windows 7 Ultimate SP1 ou superior x86/x64;
- Microsoft Windows 7 Enterprise SP1 ou superior x86/x64;
- Microsoft Windows 7 Professional SP1 ou superior x86/x64;
- Microsoft Windows 8 Enterprise x86/x64;
- Microsoft Windows 8 Pro x86/x64;
- Microsoft Windows 8.1 Pro x86/x64;
- Microsoft Windows 8.1 Enterprise x86/x64;
- Microsoft Windows 10 Enterprise x86/x64;
- Microsoft Windows 10 Pro x86/x64;
- Microsoft Windows Vista x86/x64 SP2 ou superior;
- Microsoft Windows XP Professional x86 SP3 ou superior.

4.4.5. Características Gerais De Criptografia

- O acesso ao recurso criptografado (arquivo, pasta ou disco) deve ser garantido mesmo em caso o usuário tenha esquecido a senha, através de procedimentos de recuperação;
- Utilizar, no mínimo, algoritmo AES com chave de 256 bits;
- Capacidade de criptografar completamente o disco rígido da máquina, adicionando um ambiente de pré-boot para autenticação do usuário;
- Capacidade de utilizar Single Sign-On para a autenticação de pré-boot;
- Permitir criar vários usuários de autenticação pré-boot;
- Capacidade de criar um usuário de autenticação pré-boot comum com uma
- Senha igual para todas as máquinas a partir da console de gerenciamento;
- Capacidade de criptografar drives removíveis de acordo com regra criada pelo administrador, com as opções:
- Criptografar somente os arquivos novos que forem copiados para o disco removível, sem modificar os arquivos já existentes;
- Criptografar todos os arquivos individualmente;
- Criptografar o dispositivo inteiro, de maneira que não seja possível listar os arquivos e pastas armazenadas;

- Criptografar o dispositivo em modo portátil, permitindo acessar os arquivos em máquinas de terceiros através de uma senha;
- Capacidade de selecionar pastas e arquivos (por tipo, ou extensão) para serem criptografados automaticamente. Nesta modalidade, os arquivos devem estar acessíveis para todas as máquinas gerenciadas pela mesma console de maneira transparente para os usuários;
- Capacidade de criar regras de exclusões para que certos arquivos ou pastas nunca sejam criptografados;
- Capacidade de selecionar aplicações que podem ou não ter acesso aos arquivos criptografados;
- Verifica compatibilidade de hardware antes de aplicar a criptografia;
- Possibilita estabelecer parâmetros para a senha de criptografia;
- Bloqueia o reuso de senhas;
- Bloqueia a senha após um número de tentativas pré-estabelecidas;
- Capacidade de permitir o usuário solicitar permissão a determinado arquivo criptografado para o administrador mediante templates customizados;
- Permite criar exclusões para não criptografar determinados “discos rígidos” através de uma busca por nome do computador ou nome do dispositivo
- Permite criptografar as seguintes pastas pré-definidas: “meus documentos”, “Favoritos”, “Desktop”, “Arquivos temporários” e “Arquivos do outlook”;
- Permite utilizar variáveis de ambiente para criptografar pastas customizadas;
- Capacidade de criptografar arquivos por grupos de extensão, tais como: Documentos do office, Document, arquivos de áudio etc.;
- Permite criar um grupo de extensões de arquivos a serem criptografados;
- Capacidade de criar regra de criptografia para arquivos gerados por aplicações;
- Permite criptografia de dispositivos móveis mesmo quando o endpoint não possuir comunicação com a console de gerenciamento.
- Capacidade de deletar arquivos de forma segura após a criptografia;
- Capacidade de criptografar somente o espaço em disco utilizado;
- Deve ter a opção de criptografar arquivos criados a partir de aplicações selecionadas pelo administrador;
- Capacidade de bloquear aplicações selecionadas pelo administrador de acessarem arquivos criptografados;
- Deve permitir criptografar somente o espaço utilizado em dispositivos removíveis tais como pendrives, HD externo, etc;
- Capacidade de criptografar discos utilizando a criptografia BitLocker da Microsoft;
- Deve ter a opção de utilização de TPM para criptografia através do BitLocker;
- Capacidade de fazer “Hardware encryption”.

4.4.6. Gerenciamento de Sistemas

- Capacidade de criar imagens de sistema operacional remotamente e distribuir essas imagens para computadores gerenciados pela solução e para computadores bare-metal;
- Deve possibilitar a utilização de servidores PXE na rede para deploy de imagens;
- Capacidade de detectar softwares de terceiros vulneráveis, criando assim um relatório de softwares vulneráveis;

- Capacidade de corrigir as vulnerabilidades de softwares, fazendo o download centralizado da correção ou atualização e aplicando essa correção ou atualização nas máquinas gerenciadas de maneira transparente para os usuários;
- Capacidade de gerenciar licenças de softwares de terceiros;
- Capacidade de registrar mudanças de hardware nas máquinas gerenciadas;
- Capacidade de gerenciar um inventário de hardware, com a possibilidade de cadastro de dispositivos (ex: router, switch, projetor, acessório, etc), informando data de compra, local onde se encontra, service tag, número de identificação e outros;
- Possibilita fazer distribuição de software de forma manual e agendada;
- Suporta modo de instalação silenciosa;
- Suporte a pacotes MSI, exe, bat, cmd e outros padrões de arquivos executáveis;
- Possibilita fazer a distribuição através de agentes de atualização;
- Utiliza tecnologia multicast para evitar tráfego na rede;
- Possibilita criar um inventário centralizado de imagens;
- Capacidade de atualizar o sistema operacional direto da imagem mantendo os dados do usuário;
- Suporte a Wake On Lan para deploy de imagens;
- Capacidade de atuar como servidor de atualização do Windows podendo fazer deploy de patches;
- Suporta modo de teste, podendo atribuir alguns computadores para receberem as atualizações de forma automática para avaliação de alterações no comportamento;
- Capacidade de gerar relatórios de vulnerabilidades e patches;
- Possibilita criar exclusões para aplicação de patch por tipo de sistema operacional, estação de trabalho e servidor ou por grupo de administração;
- Permite iniciar instalação de patch e correções de vulnerabilidades ao reiniciar ou desligar o computador;
- Permite baixar atualizações para o computador sem efetuar a instalação
- Permite o administrador instalar somente atualizações aprovadas, instalar todas as atualizações (exceto as bloqueadas) ou instalar todas as atualizações incluindo as bloqueadas;
- Capacidade de instalar correções de vulnerabilidades de acordo com a severidade;
- Permite selecionar produtos a serem atualizados pela console de gerenciamento;
- Permite selecionar categorias de atualizações para serem baixadas e instaladas, tais como: atualizações de segurança, ferramentas, drivers, etc.;
- Capacidade de adicionar caminhos específicos para procura de vulnerabilidades updates em arquivos;
- Capacidade de instalar atualizações ou correções somente em computadores definidos, em grupos definidos ou em uma porcentagem de computadores conforme selecionado pelo administrador;
- Capacidade de configurar o reinicio do computador após a aplicação das atualizações e correções de vulnerabilidades;
- Deve permitir selecionar o idioma das aplicações que serão atualizadas;
- Permitir agendar o sincronismo entre a console de gerenciamento e os sites da Microsoft para baixar atualizações recentes.

5. Da Qualificação Técnica/Operacional

5.1. Comprovação de aptidão para o fornecimento do objeto do presente Termo de Referência, estando de acordo com todas as características, exigências e especificações similares, quantidades e prazos compatíveis. A comprovação deverá ser feita por meio de atestado(s) de capacidade técnica fornecido(s) por pessoa(s) jurídica(s) de direito público ou privado, competentes para tanto;

5.2. Somente serão considerados válidos atestados com timbre da entidade expedidora e com identificação do nome completo, telefone e e-mail. O atestado deverá ser datado e assinado por pessoa física identificada pelo seu nome e cargo exercido na entidade, bem como dados para eventual contato, estando as informações sujeitas à conferência pela equipe de apoio técnico ao pregoeiro. Não serão aceitos atestados emitidos por empresas ou entidades que comercializem o objeto da licitação;

5.3. O(s) quantitativo(s), quando não mencionado(s) no(s) atestado(s), deverá(ão) ser comprovado(s) por quaisquer documentos, tais como: contrato(s), nota(s) fiscal(is) ou outro(s) documento(s) equivalente(s);

5.4. Os quantitativos mínimos de prova de execução obedecerão ao percentual de 50% (cinquenta por cento), conforme definido a seguir para cada lote e, em consonância com a Súmula 24 do Tribunal de Contas do Estado de São Paulo.

5.5. Quadro

ITEM	QUANTIDADE A SER COMPROVADA
1	82
2	17
3	3
6	115

6. Da Qualificação Econômico/Financeira

6.1. Certidão Negativa de Falência e Concordata expedida pelo distribuidor da sede da Pessoa Jurídica ou de Execução Patrimonial expedida no domicílio do empresário individual ou;

6.2. Certidão Negativa de Recuperação Judicial ou Extrajudicial expedida pelo distribuidor da sede da Pessoa Jurídica.

6.3. Nas hipóteses em que a certidão encaminhada for positiva, deve a Licitante apresentar comprovante da homologação/deferimento pelo juízo competente do plano de recuperação judicial/extrajudicial vigente.

6.3.1. Para o caso de empresas em recuperação judicial: Deve apresentar declaração, em papel timbrado, de estar ciente de que, no momento da assinatura contratual, a mesma deverá apresentar cópia do ato de nomeação do Administrador Judicial ou, se o Administrador for Pessoa Jurídica, o nome do profissional responsável pela condução do processo e, ainda, declaração, relatório ou documento equivalente do juízo ou do Administrador, de que a Licitante está cumprindo o plano de recuperação judicial.

6.3.2. Para o caso de empresas em recuperação extrajudicial: Deve apresentar declaração, em papel timbrado, de estar ciente de que, no momento da assinatura contratual, a mesma deverá apresentar comprovação documental do cumprimento das obrigações do plano de recuperação extrajudicial.

6.4. Apresentação do último balanço patrimonial e o demonstrativo de resultado do exercício, já exigíveis na forma da lei, que comprovem a boa situação financeira da Licitante. Não sendo esta obrigada a publicar seu balanço, deverá apresentar fotocópia legível de página do Diário Geral, onde tenha sido transcrito o balanço patrimonial, ativo/passivo e a demonstração de resultado do exercício. Estes documentos deverão conter os respectivos termos de abertura e encerramento, registrados na Junta Comercial ou Cartório de Registro Civil de Pessoas Jurídicas. Esta exigência também se aplica às Licitantes que optam pela Tributação Simplificada do Imposto de Renda Pessoa Jurídica ("Lucro Presumido" ou "microempresa").

6.5. No caso de Sociedade Anônima, observadas as exceções legais, apresentar as publicações na Imprensa Oficial do Balanço e Demonstrações Contábeis, e da Ata de Aprovação devidamente arquivada na Junta Comercial.

6.6. A boa situação econômico-financeira da Licitante também deverá ser comprovada e demonstrada, em folha anexa ao Balanço apresentado, no caso de não demonstrados no próprio livro, através dos índices contábeis constantes do Anexo XI do Edital.

6.6.1. Quando esses índices não estiverem informados no próprio balanço, o memorial de cálculo relativo aos índices de LG, LC e de SG devem ser apresentados obrigatoriamente em folha timbrada da Licitante e devem conter assinatura do(s) responsável(is), além do Contador/Técnico Contábil com seu número de registro.

6.6.2. A Licitante que apresentar resultado menor do que 01 (um), em qualquer dos índices fixados no Anexo XI, deverá comprovar, para a respectiva habilitação, o patrimônio líquido positivo correspondente a 10% (dez por cento) do valor estimado do Lote ofertado.

7. Garantia e Assistência Técnica dos Equipamentos

7.1. Da Garantia dos Equipamentos (para todos os equipamentos dos Itens 1,2 e 3)

7.1.1. O prazo de garantia mínimo será de 36 (trinta e seis) meses no local de instalação (on site) a partir da entrega.

7.2. Da Manutenção dos Equipamentos:

7.2.1. O tempo de chegada do técnico ao local de instalação deverá ser no máximo de 24 (vinte e quatro) horas a partir do chamado dentro do período de disponibilidade (das 08 às 11 horas e das 13 às 18 horas de segunda a sexta-feira);

7.2.2. Em caso de retirada para reparo em laboratório, é obrigatória a instalação de equipamento substituto equivalente;

7.2.3. O período total entre o chamado e a devolução do equipamento devidamente reparado não poderá ultrapassar 15 (quinze) dias;

7.2.4. O serviço de manutenção deverá ser executado pela CONTRATADA ou por empresa designada por ela ou pela Fabricante na Câmara Municipal de Santo André;

7.2.5. Na eventual necessidade de substituição de peças, elas serão de inteira responsabilidade da CONTRATADA, sem ônus para a CONTRATANTE.

8. DOS PRAZOS

8.1. Prazo de Vigência do Contrato: O prazo de vigência do contrato será de 12 (doze) meses a partir da assinatura do contrato;

8.2. Prazo de Garantia do Objeto: a contar da data de recebimento definitivo dos itens, conforme abaixo:
   a. Item 1: 36 (trinta e seis) meses, on site;
   b. Item 2: 36 (trinta e seis) meses, on site;
   c. Item 3: 36 (trinta e seis) meses, on site;
   d. Item 4: não se aplica;
   e. Item 5: não se aplica;
   f. Item 6: durante 36 meses.

8.3. Relativamente ao disposto aplica-se, subsidiariamente, no que couber a Lei no 8.078/1990 - Código de Defesa do Consumidor;

8.4. Prazo de Entrega

8.4.1. O Prazo de entrega será de 30 (trinta) dias úteis, contados a partir da assinatura do contrato;

8.4.2. A entrega dos equipamentos deverá ser efetuada na Diretoria de Apoio Tecnológico, com o acompanhamento da Comissão de Recebimentos, no endereço da Câmara Municipal de Santo André (SP), situada na Praça IV Centenário, nº 2, Centro - 09040-905, de 2ª a 6ª feira, das 10 às 13 horas e das 14 às 18 horas e, em quantidade a ser definida posteriormente, na Avenida Portugal, nº 141, salas 82 e 84, Centro - CEP 09040-010, visando atender os departamentos alocados nesse endereço;

8.4.3. O objeto deste contrato deverá ser entregue de acordo com as normas, especificações e demais elementos técnicos fornecidos pela CONTRATANTE e em conformidade com a proposta apresentada pela CONTRATADA, os quais farão parte integrante do contrato, independentemente de transcrições;

8.4.4. A CONTRATADA assumirá inteira responsabilidade pela entrega que efetuar, de acordo com as especificações constantes no presente Termo de Referência, bem como da respectiva proposta, obedecendo ao Código de Defesa do Consumidor quanto às condições dos produtos entregues;

8.4.5. Os materiais deverão ser entregues em embalagens originais do fabricante devidamente lacradas, os quais serão conferidos e, se achados irregulares, devolvidos à empresa, que terá o prazo de 5 (cinco) dias para substituí-los;

8.4.6. A CONTRATADA ficará obrigada a trocar, às suas expensas, os materiais que vierem a ser recusados, sendo que o ato de recebimento não importará aceitação;

8.4.7. O prazo para substituição de itens fora da especificação ou com eventuais defeitos será de, no máximo, 10 (dez) dias corridos, a contar da data do recebimento, conforme item 9.

9. Da Comissão de Recebimento e Fiscalização dos Serviços

9.1. A CONTRATANTE exercerá a mais ampla e completa fiscalização dos serviços contratados através da Comissão de Recebimentos e de seus fiscais. A fiscalização em nenhuma hipótese eximirá nem reduzirá as responsabilidades legais e contratuais da CONTRATADA, seja quanto aos danos materiais e pessoais que forem causados a terceiros, seja por atos próprios da mesma, seja por atitudes de seus operários e prepostos;

9.2. A Fiscalização será desempenhada pelo(a) Diretor de Tecnologia da Informação, em conjunto com o(a) Gerência de Tecnologia da Informação e o Chefe do Núcleo de Suporte ao Usuário - Hardware/Software, e terá atuação durante toda a vigência do contrato, bem como durante toda a garantia, devendo se manifestar sempre sobre o atendimento pleno desta última e demais condições que envolvam a sua entrega e garantia, relatando as ocorrências em processo próprio de acompanhamento;

9.3. A Fiscalização comunicará a empresa, por escrito, preferencialmente via e-mail, as deficiências porventura verificadas na execução dos serviços, para a imediata correção, sem prejuízo das sanções cabíveis;

9.4. A Comissão de Recebimentos será composta pelos fiscais designados no item 9.2 e pelo(a) Chefe de Núcleo de Patrimônio, cabendo a estes, em conjunto, dar recebimento provisório e o definitivo, permitindo a verificação da entrega, as possíveis substituições ou trocas que, porventura, forem necessárias, até seu recebimento definitivo em conformidade com as especificações do Edital.

10. Das Condições de Recebimento do Objeto

10.1. Recebimento Provisório - Todos os equipamentos serão recebidos provisoriamente pela Comissão de Recebimentos, após a entrega para verificação da conformidade com as especificações, o que ocorrerá em prazo não superior a 5 (cinco) dias úteis, após a data da entrega.

a. Sendo constatada qualquer irregularidade, não se dará o recebimento definitivo, ficando a CONTRATADA obrigada a atender às determinações da Comissão de Recebimento de Materiais no prazo máximo de 10 (dez) dias, após o qual será efetuado novo exame dos materiais;

b. Na segunda oportunidade, os materiais deverão apresentar perfeitas condições de serem recebidos definitivamente, sendo que, se não estiverem em ordem, a CONTRATADA sofrerá aplicação da multa cominada para o atraso diário na conclusão, a contar da data da primeira vistoria, nos termos do Ato nº 4, de 22 de março de 2005.

10.2. Recebimento Definitivo - Decorrido o prazo e inexistindo falhas ou incorreções, a Comissão de Recebimento de Materiais lavrará o "Termo de Recebimento Definitivo", depois de reexaminados os materiais e desde que estejam em perfeitas condições, mediante requerimento da CONTRATADA, de acordo com o disposto no art. 73, II "b" da Lei Federal nº 8.666/93.

11. Dos Pagamentos

11.1. A CONTRATANTE pagará à CONTRATADA, após o recebimento definitivo de cada entrega, o respectivo preço constante da proposta apresentada pela empresa em conformidade com as especificações técnicas contidas no respectivo ato convocatório;

11.2. No preço acham-se computados e diluídos todos os ônus decorrentes de despesas diretas e indiretas (mão-de-obra, equipamentos, acessórios, encargos sociais e quaisquer outras

despesas necessárias), mesmo que não tenham sido apontadas expressamente pela CONTRATANTE, desde que tenham relação com os serviços a serem executados;

11.3. O pagamento será efetuado até 5 (cinco) dias úteis pela Diretoria de Orçamento e Finanças, após o recebimento definitivo firmado pela Comissão de Recebimentos, por meio de depósito em conta corrente, através de ordem bancária, após a apresentação da respectiva nota fiscal/fatura, devidamente discriminada e atestada por servidor(a) designado(a) pela CONTRATANTE;

11.4. O não pagamento da fatura, apresentada nas condições previstas, ensejará a incidência da necessária compensação financeira, a ser procedida nos termos da Lei Civil;

11.5. Nenhum pagamento será efetuado à CONTRATADA enquanto pendente de liquidação qualquer obrigação financeira que lhe for imposta, em virtude de penalidade ou inadimplência, a qual poderá ser compensada com o pagamento pendente, sem que isso gere direito a acréscimos de qualquer natureza;

Sustação dos Pagamentos - Nenhum pagamento será feito à CONTRATADA, caso haja penalização monetária, antes que ocorra a respectiva quitação ou que se releve a conduta sancionatória aplicada.

TRIBUNAL DE CONTAS DO ESTADO DE SÃO PAULO

ANEXO II - TERMO DE CIÊNCIA E DE NOTIFICAÇÃO
(Contratos)

CONTRATANTE: CÂMARA MUNICIPAL DE SANTO ANDRÉ
CONTRATADA: CENTERTEC NEGÓCIOS, SOLUÇÕES E TECNOLOGIA LTDA
CONTRATO Nº (DE ORIGEM): 28/2023 - Processo CMSA 7299/2023 – Pregão 12/2023.
OBJETO: Aquisição de microcomputadores com garantia técnica do fabricante e de licenciamento de solução de proteção e antivírus.
ADVOGADO(S) / Nº OAB: (*) _____

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 à 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 pela CONTRATANTE estão cadastradas no módulo eletrônico do "Cadastro Corporativo TCESP - CadTCESP", nos termos previstos no Artigo 2º das Instruções nº 01/2020, conforme "Declaração(ões) de Atualização Cadastral" anexa (s);
e) é de exclusiva responsabilidade da CONTRATADA manter seus dados sempre atualizados.

2. Damo-nos por NOTIFICADOS para:
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.

Santo André (SP), 15 de dezembro de 2023.

Autoridade Máxima do Órgão/Entidade:
Nome: Carlos Roberto Ferreira
Cargo: Presidente da Câmara Municipal de Santo André
CPF: 029.194.068-41

Responsável pela Ratificação da Dispensa/Inexigibilidade de Licitação:
Nome: Carlos Roberto Ferreira
Cargo: Presidente da Câmara Municipal de Santo André
CPF: 029.194.068-41

Assinatura: _____

Ordenador de Despesas da CONTRATANTE:
Nome: Carlos Roberto Ferreira
Cargo: Presidente da Câmara Municipal de Santo André
CPF: 029.194.068-41

Assinatura: _____

Responsáveis que assinaram o Ajuste:
Pela CONTRATANTE:
Nome: Carlos Roberto Ferreira
Cargo: Presidente da Câmara Municipal de Santo André
CPF: 029.194.068-41

Assinatura: _____

Pela CONTRATADA:
Nome: Valter Mateus da Silva
Cargo: Sócio administrador
CPF: 072.583.798-51

Assinatura: _____

(*) Facultativo. Indicar quando já constituído, informando, inclusive, o endereço eletrônico.