

TERMO DE REFERÊNCIA (TR)

HISTÓRICO DE REVISÕES

<u>DATA</u>	<u>VERSÃO</u>	<u>DESCRIÇÃO</u>	<u>AUTOR</u>
01/04/2026	1.0	Elaboração do termo de referência	Abel Jose Maria Neto
22/04/2026	2.0	Revisão do termo de referência	Felipe Augusto Alencar Maia

Vila Velha –ES, 24 de abril de 2026.

TERMO DE REFERÊNCIA

Lei nº 14.133, de 1º de abril de 2021

Prefeitura Municipal de Vila Velha

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

Processo Administrativo:	21893/2026
Modalidade / Forma:	Pregão Eletrônico / Menor Preço Global
Base Legal:	Lei Federal nº 14.133/2021
Órgão Requisitante:	Secretaria Municipal de Tecnologia e Inovação – SEMTI
Órgãos Participantes:	SEMTI; SEMAP; SEMED; SEMEL; SEMMA; SEMPDEC; SEMTUR; PGM; SEMAD; SEMAS; FMASVV; SEMCOM; SEMCONT; SEMCULT; SEMDEC; SEMDU; SEMOPE; SEMPLA; SEMPMU; SEMRI; SEMDEST; SEMSA; SEMGAP; SEMSU e SEMFI
Vigência estimada:	12 (doze) meses, prorrogável nos termos do art. 107 da Lei nº 14.133/2021
Responsável pela elaboração:	Abel José Maria Neto – Secretário de Tecnologia e Inovação
Observação:	Este Termo de Referência segue modelo adotado pela Portaria Conjunta SEMAD/PGM/ SEMCONT nº 04/2024

1.1. Constitui objeto da pretensa contratação, o Registro de Preços visando futuras e eventuais aquisições de **DESKTOPS, NOTEBOOKS, WORKSTATIONS, MONITORES e TABLETS**, observado o detalhamento do objeto.

1.2. Os bens objeto desta contratação são caracterizados como comuns.

1.3. O prazo de vigência da contratação é de 12 (doze) meses, contados da assinatura do contrato, na forma do artigo 105, da Lei nº 14.133 de 2021.

2. DA CONTEXTUALIZAÇÃO E JUSTIFICATIVA DA NECESSIDADE DA CONTRATAÇÃO

2.1. Com a evolução contínua das Tecnologias da Informação e Comunicação (TIC), a informática tornou-se ferramenta essencial para a execução dos serviços no âmbito das organizações públicas e privadas, contribuindo para que a maioria dos seus processos seja executada por meio de equipamentos tecnológicos que assumiram tamanha importância que se tornaram absolutamente indispensáveis.

2.2. Diante da imperiosa necessidade de provisão de equipamentos para sustentar a continuidade de suas atividades, as organizações, com a frequência necessária providencia aquisições para renovação de seus parques tecnológicos com fins de que cada vez mais suas operações sejam executadas de forma mais célere e eficaz.

2.3. Os equipamentos computacionais, tais como desktops, workstations, monitores e tablets, desempenham, portanto, papel fundamental no funcionamento eficiente e na prestação de serviços dos órgãos públicos municipais. Assim, a presente aquisição é pautada pela nova Lei de Licitações nº 14.133/2021 e visa atender às demandas crescentes por equipamentos atualizados e modernos, visando garantir a continuidade operacional dos serviços públicos de forma econômica e eficaz.

2.4. A modernização constante dos parques tecnológicos é essencial para acompanhar as demandas dos serviços públicos, garantir a segurança das informações e oferecer um ambiente de trabalho adequado aos servidores municipais. Considerando a obsolescência natural dos equipamentos de informática e a necessidade de adaptação às novas exigências de softwares e sistemas, torna-se imprescindível a atualização periódica desses recursos.

2.5. Nesse contexto, a aquisição de equipamentos com ampla cobertura de garantia se mostra como a estratégia mais adequada para minimizar interrupções nos serviços públicos, além de proporcionar maior segurança e confiabilidade no funcionamento dos sistemas de informação. A garantia integral dos equipamentos também contribui para a redução de custos a longo prazo, evitando gastos excessivos com manutenção e reparos emergenciais.

2.6. Ao centralizar a aquisição de bens de informática, o presente processo está em conformidade com as diretrizes de racionalização do gasto público, promovendo a otimização dos recursos disponíveis e a melhoria da gestão dos parques tecnológicos municipais. Além disso, a padronização dos equipamentos facilita a interoperabilidade entre os diferentes órgãos públicos, promovendo a integração e a eficiência na prestação de serviços.

2.7. Por fim, a definição das especificações técnicas dos equipamentos considera as necessidades operacionais dos servidores municipais, garantindo que os recursos adquiridos atendam plenamente às demandas da PMVV. Dessa forma, a presente aquisição visa proporcionar um ambiente de trabalho moderno, seguro e eficiente, contribuindo para a melhoria do atendimento ao cidadão e aperfeiçoamento das atividades administrativas dos órgãos públicos municipais.

2.8.FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

a) A Fundamentação da Contratação e de seus quantitativos encontra-se pormenorizada em Tópico específico dos Estudos Técnicos Preliminares, apêndice deste Termo de Referência.

b) O objeto da contratação está previsto no Plano de Contratações Anual 2026, conforme detalhamento a seguir:

I) ID PCA no PNCP: 27165554000103-0-000001/2026

II) Data de publicação no PNCP: 23 de junho de 2025

III) Id do item no PCA: 766

IV) Classe/Grupo: Soluções de TIC – Material de TIC

V) Identificador da Futura Contratação: PCW00766.2026-13

3.REQUISITOS DA CONTRATAÇÃO

3.1. MODALIDADE E TIPO DA LICITAÇÃO

3.1.1.O tipo e critério de julgamento da licitação é o menor preço global, para a seleção da proposta mais vantajosa, utilizado para compras e serviços de modo geral e para contratação de bens e serviços de informática, nos termos da justificativa já apresentada.

3.1.2.De acordo com o Art. 4º do Decreto Municipal nº 94/2005, esta licitação deve ser realizada na modalidade de Pregão, preferencialmente na sua forma eletrônica.

3.1.3.A fundamentação pauta-se na premissa de que a presente contratação de serviços se baseia em padrões de desempenho e qualidade claramente definidos no Termo de Referência, havendo diversos fornecedores capazes de prestá-los, caracterizando-se, assim, como “serviço comum”, conforme estatui o §1º, do Art. 2º, ainda do Decreto nº 94/2005.

3.2.JUSTIFICATIVA PARA PROCESSAMENTO DO CERTAME PELO SISTEMA DE REGISTRO DE PREÇOS

O processamento da licitação pelo Sistema de Registro de Preços justifica-se:

- a. Pela imprevisibilidade de se estimar com exatidão, o quantitativo a ser utilizado no período de validade da Ata de Registro de Preços, especialmente pela expansão dos serviços digitais, que demandará a aquisição de novos equipamentos;
- b. Por ser adequado para situações em que a aquisição integral e imediata não é viável, mas há demanda, permitindo que a administração faça pedidos dos itens durante a execução, evitando a necessidade de um novo processo licitatório;
- c. Pela possibilidade de a Ata de Registro de Preços ultrapassar o exercício financeiro corrente, viabilizando o atendimento para demandas imprevisíveis e do exercício posterior;
- d. Pelo fato de não haver necessidade de reserva orçamentária, logo, não bloqueando recursos desnecessariamente e, pela possibilidade de atendimento de múltiplos órgãos que compõem a estrutura do Município com um único procedimento, caracterizando, desta forma, ganho com economia de escala.

3.3.PARCELAMENTO OU NÃO DA CONTRATAÇÃO

3.3.1. Considerando as características específicas da presente contratação e visando à eficiência na gestão contratual, optou-se pela contratação em lote único integrado.

3.3.2. A adoção em lote único facilita a gestão contratual e permite uma melhor adequação às necessidades da Secretaria.

3.3.3. A fragmentação desta solução entre múltiplos fornecedores criaria "zonas cinzentas" de responsabilidade técnica, especialmente no que tange à garantia on-site.

3.3.4. Ademais, a contratação em lote único proporciona economia de escala e eficiência administrativa, mediante:

- Padronização Tecnológica: Garantia de compatibilidade técnica integral entre as fontes de alimentação das workstations/computadores e a senoidal dos Nobreaks fornecidos;
- Logística Reversa e Manutenção: Ponto único de contato para suporte técnico e garantia do parque tecnológico, reduzindo o tempo médio de reparo (MTTR);
- Redução de Custos de Gestão: Otimização da fiscalização contratual com um único interlocutor para a entrega e instalação de todos os grupos de serviço, gerando valores unitários mais competitivos em observância ao princípio da vantajosidade.

3.4. DA SUBCONTRATAÇÃO E CONSÓRCIO

3.4.1. Não é admitida a subcontratação do objeto contratual.

3.4.2. O contrato oferece maior detalhamento das regras que serão aplicadas em relação à subcontratação.

3.4.3. Fica vedada a participação de consórcios, prevista no art. 15 da Lei nº 14.133/2021, considerando a necessidade de responsabilidade unificada pela cadeia integrada de atendimento, bem como a complexidade técnica do objeto, que demanda gestor único dos serviços e dos níveis de serviço acordados.

3.5. GARANTIA DA CONTRATAÇÃO

3.5.1. Será exigida a garantia da contratação de que tratam os arts. 96 e seguintes da Lei nº 14.133, de 2021, no percentual de 5% do valor contratual, conforme regras previstas no contrato

3.5.2. No caso de seguro-garantia sua apresentação deverá ocorrer, no máximo, até a data de assinatura do contrato.

3.6. JUSTIFICATIVA PARA NÃO APLICAÇÃO DE COTAS DE RESERVA

3.6.1. Não serão reservadas cotas destinadas às micro e pequenas empresas (ME/EPP) por apresentar riscos ao alcance dos objetivos dessa contratação centralizada, principalmente no que se refere à obtenção de ganho de escala. A divisão do fornecimento em cotas pode reduzir o ganho de escala e impactar negativamente a economicidade no preço final.

3.6.2. Além disso, a escolha de uma empresa capaz de executar a distribuição de um volume expressivo de equipamentos é essencial. Sem os parâmetros adequados que assegurem a existência de fornecedores aptos a atender a demanda, a inclusão de itens exclusivos ou com cotas para ME/EPP pode resultar em uma licitação ineficaz, gerando risco de itens desertos e/ou fracassados por ausência de fornecedores capacitados.

3.7. RESULTADOS E BENEFÍCIOS A SEREM ALCANÇADOS

3.7.1. A presente contratação tem como finalidade assegurar a melhoria da infraestrutura tecnológica da Administração, contribuindo diretamente para o

desempenho eficiente das atividades institucionais. Nesse sentido, espera-se alcançar os seguintes resultados e benefícios:

- Aumento da eficiência operacional, com equipamentos mais modernos, capazes de executar sistemas e tarefas com maior rapidez e estabilidade;
- Redução de falhas e indisponibilidades, decorrente da substituição de equipamentos obsoletos ou com alto índice de manutenção;
- Melhoria na produtividade e experiência dos servidores, proporcionando melhores condições de trabalho e redução do tempo de resposta nas atividades administrativas;
- Maior segurança da informação, com equipamentos compatíveis com requisitos atualizados de segurança, reduzindo riscos de vulnerabilidades e perda de dados;
- Padronização do parque tecnológico, facilitando a gestão, manutenção, suporte técnico e eventual reposição de equipamentos;
- Otimização de custos a médio e longo prazo, equipamentos com garantia apresentam redução de despesas com manutenção corretiva e aumento da vida útil dos equipamentos;
- Aprimoramento na prestação dos serviços públicos, refletindo diretamente na qualidade do atendimento ao cidadão;
- Conformidade com diretrizes de governança e transformação digital, promovendo modernização administrativa e alinhamento com boas práticas de gestão pública.

4.DESCRICÃO DA SOLUÇÃO COMO UM TODO

4.1. A definição dos quantitativos previstos observou o cenário atual, o planejamento dos órgãos do Município e as demandas tecnológicas, visando atender adequadamente as necessidades da PMVV, para o período de vigência da futura Ata de Registro de Preços.

4.1.2. Desta feita, as quantidades previstas abarcam o planejamento de modernização e expansão do quantitativo de equipamentos do Município, pelo período de 12 (doze) meses, podendo ser prorrogado por igual período, conforme art. 84, da Lei nº 14.133/2021.

4.2. BENS E/OU SERVIÇOS QUE COMPÕEM A SOLUÇÃO DE TIC:

LOTE ÚNICO					
ITEM	DESCRIÇÃO DO BEM OU SERVIÇO (ESPECIFICAÇÃO MÍNIMAS)	UNIDADE DE MEDIDA	QTD	VALOR UNITÁRIO	VALOR TOTAL ESTIMADO
01	MICROCOMPUTADOR TIPO I Descrição completa vide ANEXO I.	UNIDADE	756	14.355,00	10.852.380,00
	MICROCOMPUTADOR TIPO II Descrição completa vide ANEXO I.	UNIDADE	1639	12.660,00	20.749.740,00
03	NOTEBOOK Descrição completa vide ANEXO I.	UNIDADE	243	11.382,50	2.765.947,50
04	WORKSTATION Descrição completa vide ANEXO I.	UNIDADE	120	35.171,00	4.220.520,00
05	MONITOR 21,5" Descrição completa vide ANEXO I.	UNIDADE	556	1.894,50	1.053.342,00
06	MONITOR 23,8" Descrição completa vide ANEXO I.	UNIDADE	751	2.288,00	1.718.288,00
07	TABLET Descrição completa vide ANEXO I.	UNIDADE	431	2.965,50	1.278.130,50

Valor total da contratação: R\$ 42.638.348,00 (quarenta e dois milhões, seiscentos e trinta e oito mil, trezentos e quarenta e oito reais).



PREFEITURA DE
VILA VELHA

SECRETARIA DE TECNOLOGIA E INOVAÇÃO

4.3.ESCOPO DO FORNECIMENTO

4.3.1.As especificações técnicas para os itens estão descritas no Anexo I do presente Termo de Referência.

MICROCOMPUTADOR TIPO I																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																														
Computador Desktop – Processador com 06 núcleos e 12 threads; Memória 16GBx1 ou 8GBx2/DIMM DDR5/5200Mhz; SSD 256GB do tipo M.2 PCIe NVMe; Interface de rede Gigabit Ethernet e Wireless (802.11ax); Teclado alfanumérico ABNT II com 107 teclas; Mouse tipo óptico; Sistema Operacional: Microsoft Windows 11 profissional 64 bits OEM/pré-instalado; monitor 21,5” Resolução de 1920 x 1080 pixels; portas DisplayPort ou HDMI e VGA. Garantia e suporte técnico on-site de, no mínimo, 60 (sessenta) meses; Nobreak - Potência nominal mínima de 600 VA; bivolt;4 (quatro) tomadas de saída; chave liga/desliga; proteção contra descarga total da bateria; Garantia mínima de 12 (doze) meses.																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																														
ITEM	SEMTI	SEMAP	SEMED	SEMEL	SEMMA	SEMPDEC	SEMTUR	PGM	SEMAD	SEMAS	FMSVV	SEMTI	SEMTUR	SEMCONT - FMCC	SEMCULT	SEMDEC	SEMTUR	SEMOPE	SEMTUR	SEMPMU	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR	SEMTUR





PREFEITURA DE
VILA VELHA

SECRETARIA DE TECNOLOGIA E INOVAÇÃO

WORKSTATION

Workstation - Processador com 20 núcleos e 28 threads; Memória 64GB/ UDIMM DDR5-ECC/4400Mhz; Disco 1: 1TB do tipo SSD M.2 PCIe NVMe. Disco 2: 2TB do tipo SATA III, 7200RMP; Placa de vídeo dedicada 12GB GDDR6; Teclado alfanumérico ABNT II com 107 teclas; Mouse tipo óptico; monitor 23.8" Resolução de 1920 x 1080 pixels; portas DisplayPort ou HDMI e VGA; Sistema Operacional: Microsoft Windows 11 professional 64 bits OEM/pré-instalado. Garantia e suporte técnico on-site de, no mínimo, 60 (sessenta) meses. Nobreak - Potência nominal mínima de 600 VA; bivolt; 4 (quatro) tomadas de saída; chave liga/desliga; proteção contra descarga total da bateria; Garantia mínima de 12 (doze) meses.

ITEM	SEMTI	SEMAP	SEMED	SEMEL	SEMMA	SEMPDEC	SEMTUR	PGM	SEMAD	SEMAS	FMSVV	SEMTI	SEMCOM	SEMCONT - FMCC	SEMCULT	SEMDEC	SEMDU	SEMOPE	SEMPLA	SEMPMU	SEMRI	SEMDEST	SEMSA	SEMGAP	SEMSU	QTD	VL.MÉDIO UNITÁRIO	VALOR TOTAL
4	47	0	6	0	5	0	0	0	3	3	7	5	2	0	1	0	20	10	1	0	0	6	1	2	1	120	35.171,00	4.220.520,00

MONITOR 21.5"

Monitor de 21,5" polegadas; Resolução de 1920 x 1080 pixels; portas DisplayPort ou HDMI e VGA. Garantia e suporte técnico on-site de, no mínimo, 60 (sessenta) meses. Mouse tipo óptico; monitor 23.8" Resolução de 1920 x 1080 pixels; portas DisplayPort ou HDMI e VGA; Sistema Operacional: Microsoft Windows 11 professional 64 bits OEM/pré-instalado. Garantia e suporte técnico on-site de, no mínimo, 60 (sessenta) meses.

ITEM	SEMTI	SEMAP	SEMED	SEMEL	SEMMA	SEMPDEC	SEMTUR	PGM	SEMAD	SEMAS	FMSVV	SEMTI	SEMCOM	SEMCONT - FMCC	SEMCULT	SEMDEC	SEMDU	SEMOPE	SEMPLA	SEMPMU	SEMRI	SEMDEST	SEMSA	SEMGAP	SEMSU	QTD	VL.MÉDIO UNITÁRIO	VALOR TOTAL
5	250	0	0	5	0	0	0	10	20	25	75	0	0	0	5	0	0	20	1	0	0	5	100	0	40	556	1.894,50	1.053.342,00



PREFEITURA DE
VILA VELHA

SECRETARIA DE TECNOLOGIA E INOVAÇÃO

MONITOR 23.8"

Monitor de 23,8" polegadas; Resolução de 1920 x 1080 pixels; portas DisplayPort ou HDMI e VGA. Garantia e suporte técnico on-site de, no mínimo, 60 (sessenta) meses.VGA; Sistema Operacional: Microsoft Windows 11 professional 64 bits OEM/pré-instalado. Garantia e suporte técnico on-site de, no mínimo, 60 (sessenta) meses.

ITEM	SEMTI	SEMAP	SEMED	SEMEL	SEMMA	SEMPDEC	SEMTUR	PGM	SEMAD	SEMAS	FMSVV	SEMFI	SEMCOM	SEMCONT - FMCC	SEMCULT	SEMDEC	SEMDU	SEMOPE	SEMPLA	SEMPMU	SEMRI	SEMDEST	SEMSA	SEMGAP	SEMSU	QTD	VL.MÉDIO UNITÁRIO	VALOR TOTAL
6	230	0	0	3	10	0	6	0	5	25	75	20	2	5	1	0	200	20	1	3	0	35	100	0	10	751	2.288,00	1.718.288,00

TABLET

Tablet: Tablet com processador octa-core mínimo de 2,0 GHz; memória RAM mínima de 3GB; armazenamento interno mínimo de 128GB (flash/eMMC), com expansão via microSD até 1TB; tela mínima de 10" com resolução mínima de 1920x1080 (LCD ou OLED); conectividade Wi-Fi 802.11 b/g/n/ac, Bluetooth 5.0 ou superior, 4G compatível com frequências nacionais e GPS integrado; áudio com alto-falante, microfone e saída P2 (3,5 mm); câmeras frontal (mín. 5MP) e traseira (mín. 8MP); bateria mínima de 7000 mAh; sensores de acelerômetro e luz ambiente; sistema operacional Android 12 ou superior em português. Garantia e suporte técnico de, no mínimo, 12 (doze) meses. Descrição completa vide anexo I.

ITEM	SEMTI	SEMAP	SEMED	SEMEL	SEMMA	SEMPDEC	SEMTUR	PGM	SEMAD	SEMAS	FMSVV	SEMFI	SEMCOM	SEMCONT - FMCC	SEMCULT	SEMDEC	SEMDU	SEMOPE	SEMPLA	SEMPMU	SEMRI	SEMDEST	SEMSA	SEMGAP	SEMSU	QTD	VL.MÉDIO UNITÁRIO	VALOR TOTAL
7	180	0	0	1	30	0	4	0	5	30	60	20	0	2	5	0	50	4	1	1	0	33	0	0	5	431	2.965,50	1.278.130,50

4.3.2.As secretarias partícipes atestarão este Termo de Referência por meio de suas assinaturas, declarando ciência e concordância com as disposições nele contidas.

5. OBRIGAÇÕES DAS PARTES

5.1.OBRIGAÇÕES DA CONTRATANTE

5.1.1.Além das obrigações decorrentes da observância da Lei nº14.133/2021, são obrigações da CONTRATANTE:

- a. Acompanhar, fiscalizar, conferir e avaliar o objeto da contratação através de fiscais devidamente designados;
- b. Cumprir com os compromissos financeiros assumidos com a CONTRATADA e realizar o pagamento devido no prazo e forma estabelecidos neste Termo de Referência e seus anexos
- c. Prestar informações e esclarecimentos que venham a ser solicitados ao Município;
- d. Atestar notas fiscais correspondentes após o recebimento dos itens comprados;
- e. Receber e fiscalizar os serviços/produtos entregues, verificando a sua correspondência com as especificações prescritas no Edital, atestando sua conformidade;
- f. Designar formalmente um servidor da unidade gestora para acompanhar e fiscalizar a execução da autorização de fornecimento ou instrumentos equivalentes;
- g. Notificar formalmente quaisquer irregularidades encontradas na entrega dos itens para que sejam tomadas as devidas providências de substituição ou correção;
- h. Proporcionar todas as condições necessárias para que a CONTRATADA possa cumprir as obrigações assumidas;
- i. Informar, previamente, o local de execução do objeto;
- j. Aplicar as sanções administrativas pertinentes, em caso de inadimplemento das obrigações contratuais;
- k. Fazer, na forma definida na Legislação em vigor, retenção de encargos sociais/previdenciários e outros, sob sua responsabilidade, aplicáveis no caso.

5.2.OBRIGAÇÕES DA CONTRATADA

5.2.1.Além das obrigações resultantes da observância da Lei nº 14.133/2021, são obrigações a CONTRATADA:

- a. Assumir integral responsabilidade pela boa e eficiente execução dos serviços, que deverão ser efetuados de acordo com o estabelecido no Edital, Termo de

Referência e seus anexos, normas da Associação Brasileira de Normas Técnicas e a legislação em vigor;

- b. Efetuar a entrega do objeto desta licitação em perfeitas condições, conforme especificações, prazo e local constantes neste Termo de Referência, acompanhado da respectiva “Nota Fiscal/Fatura”, na qual, constarão as indicações referentes a: marca, procedência e demais descrições dos serviços contratados;
- c. Executar fielmente o contrato, comunicando imediatamente e, com antecedência, o representante legal da CONTRATANTE, na hipótese de ocorrência de qualquer fato impeditivo de seu cumprimento;
- d. Assumir total responsabilidade por danos causados ao CONTRATANTE ou a terceiros, decorrentes da execução dos serviços, isentando o CONTRATANTE de todas as reclamações que possam surgir, sejam elas resultantes de atos de seus prepostos ou de quaisquer pessoas físicas ou jurídicas empregadas ou ajustadas na execução dos serviços;
- e. Acatar as orientações da CONTRATANTE, sujeitando-se à mais ampla e irrestrita fiscalização, prestando os esclarecimentos solicitados e atendendo as reclamações formuladas;
- f. Manter durante toda a execução do Contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;
- g. A eventual aceitação dos serviços por parte do CONTRATANTE não eximirá a CONTRATADA da responsabilidade de quaisquer erros, imperfeições ou vícios que eventualmente venham a se verificar posteriormente, circunstâncias em que as despesas de correção ou modificação correrão por conta exclusiva da CONTRATADA;
- h. Em caso de substituição dos profissionais responsáveis técnicos, submeter à prévia aprovação da CONTRATANTE os nomes dos novos responsáveis pelos serviços a serem prestados, que deverão atender às exigências estabelecidas para a participação no certame.

6.CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

6.1. CRITÉRIOS DE QUALIFICAÇÃO TÉCNICA PARA A HABILITAÇÃO

Para comprovação de sua qualificação técnica, a Licitante deverá apresentar os seguintes documentos:

6.2.COMPROVAÇÃO DE CAPACIDADE TÉCNICA

- a. ATESTADO(S) DE CAPACIDADE TÉCNICA emitido(s) por pessoa jurídica de direito público ou privado comprovando que a licitante forneceu, sem restrição, equipamento compatível em características e quantidades, com o objeto da licitação.
- b. A comprovação será feita por meio de apresentação de atestado (s), redigido (s) em português, devidamente assinado(s), carimbado(s), em papel timbrado da empresa ou órgão tomador do serviço.
- c. O(s) atestado(s) apresentado(s) deverá(ão) comprovar o fornecimento dos itens correspondentes às seguintes parcelas relevantes do objeto da licitação: **Microcomputador tipo I; Microcomputador tipo II; Notebook.**
- d. O(s) atestado(s) apresentado(s) deverão demonstrar fornecimento em quantidade equivalente a, no mínimo, **50% do total de unidades estimadas** para cada item relevante.

Item Relevante	Quantidade Estimada	Quantidade Mínima Exigida (50%)
Microcomputador tipo I	756 unidades	378 unidades
Microcomputador tipo II	1639 unidades	819 unidades
Notebook	243 unidades	121 unidades

- e. Em relação à compatibilidade quanto ao quantitativo, será admitida a soma de atestados para comprovar a execução de fornecimentos que atendam ao quantitativo mínimo estipulado para cada item relevante, conforme quadro acima.
- f. A exigência de atestados de capacidade técnica para as parcelas relevantes, fundamenta-se na necessidade de garantir a execução adequada do contrato, prevenindo falhas que possam comprometer a continuidade das atividades administrativas e gerar prejuízos à Administração Pública. Os itens representam uma parte substancial do objeto e possuem impacto econômico e operacional, sendo essenciais para a eficiência das operações públicas.
- g. A comprovação prévia por meio de atestados reduz os riscos de fornecimento inadequado, atrasos e inexecução, protegendo o erário público e assegurando que os equipamentos atendam às especificações técnicas e sejam entregues nos prazos estabelecidos. Essa exigência está alinhada ao art. 67 da Lei nº 14.133/2021, que permite restrições proporcionais às parcelas de maior relevância, garantindo o interesse público, a continuidade do serviço e a qualidade da execução contratual.

6.2.1.DOCUMENTOS COMPLEMENTARES

- a. PLANILHA indicando marca/modelo dos produtos ofertados;
- b. CATÁLOGOS e/ou MANUAIS que permitam a identificação das especificações técnicas dos equipamentos propostos.
- c. Os documentos referenciados deverão ser enviados no formato PDF, de boa resolução, sem senha ou qualquer outro tipo de proteção que impeça a visualização ou a impressão, indicando todas as funcionalidades exigidas no termo de referência.

6.3.CONDIÇÕES GERAIS DE HABILITAÇÃO

6.3.1. Para todos os itens, os equipamentos a serem ofertados deverão ser novos, sem qualquer uso anterior e em linha de fabricação.

6.3.2. A licitante deverá apresentar junto com as demais documentações, documento contendo obrigatoriamente o número do pregão eletrônico e o número do processo, além de enumerar todos os equipamentos contemplados na proposta e que atendam integralmente às exigências deste Termo de Referência. A falta da documentação acima implicará na desclassificação da empresa licitante.

6.3.3. A licitante deverá ainda, apresentar junto com as demais documentações, documento vigente, emitido pelo fabricante dos equipamentos propostos, de acordo com os itens, onde conste que ela é uma revenda autorizada dos produtos de sua fabricação.

6.3.4. A falta de qualquer documentação informada e solicitada acima, implicará na inabilitação e desclassificação da licitante para participação no certame.

7. GESTÃO DA CONTRATAÇÃO

7.1. PRAZOS PARA ENTREGA /EXECUÇÃO DOS SERVIÇOS

7.1.1. O prazo máximo para entrega fica fixado em 60 (sessenta) dias, contados a partir da data de recebimento da Autorização de Fornecimento – AF expedida pela CONTRATANTE.

7.1.2. A Fiscalização fornecerá junto com a Autorização de Fornecimento todos os elementos indispensáveis à entrega.

7.1.3. Caso a CONTRATANTE identifique que algum dos equipamentos ofertados não atendem as especificações técnicas mínimas exigidas no ANEXO I deste Termo de

Referência, a empresa licitante, inicialmente declarada como vencedora, será desclassificada, e será chamada a empresa licitante subsequentemente habilitada e classificada no pregão com melhor proposta comercial apresentada no processo licitatório realizado, onde será admitido novamente o prazo inicial para entrega.

7.2. GESTÃO E FISCALIZAÇÃO DO CONTRATO

7.2.1. A fiscalização será realizada por servidor(a) designado(a) por meio de Ato de Designação do Secretário da Pasta requisitante, nos termos do Art. 117, da Lei n.º 14.133/2021, que deverá atestar o recebimento dos materiais.

7.2.2. Caberá ao “Gestor/Fiscal do Contrato” notificar a CONTRATADA por escrito, quando necessário, sobre quaisquer irregularidades que venham a ocorrer em função da entrega dos bens e materiais adquiridos, por meio do objeto desta licitação.

7.2.3. A Fiscalização será exercida no interesse do CONTRATANTE e não exclui, nem reduz a responsabilidade da CONTRATADA, inclusive perante terceiros, por qualquer irregularidade, e, na sua ocorrência, não implica corresponsabilidade do Poder Público ou de seus agentes e prepostos.

7.2.4. O representante da Administração anotará em registro próprio todas as ocorrências relacionadas com a execução da contratação, indicando dia, mês e ano, bem como o nome dos funcionários eventualmente envolvidos, determinando o que for necessário à regularização das falhas ou defeitos observados e encaminhando os apontamentos à autoridade competente para as providências cabíveis.

7.2.5. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos (Lei nº 14.133, de 2021, art. 117, caput).

7.2.6. O fiscal técnico acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas, de modo a assegurar os melhores resultados para a Administração. (Decreto nº 11.246, de 2022, art. 22, VI).

7.2.7. O fiscal técnico anotará no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do mesmo, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados. (Lei nº 14.133, de 2021, art. 117, §1º, e Decreto nº 11.246, de 2022, art. 22, II).

7.2.8. Identificada qualquer inexatidão ou irregularidade, o fiscal técnico do contrato emitirá notificações para a correção da execução do mesmo, determinando prazo para a correção. (Decreto nº 11.246, de 2022, art. 22, III).

7.2.9. O fiscal técnico informará ao gestor do contrato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso. (Decreto nº 11.246, de 2022, art. 22, IV).

7.2.10. No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprazadas, o fiscal técnico do contrato comunicará o fato imediatamente ao gestor. (Decreto nº 11.246, de 2022, art. 22, V).

7.2.11. O fiscal técnico comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à renovação tempestiva ou à prorrogação contratual (Decreto nº 11.246, de 2022, art. 22, VII).

7.2.12. O gestor acompanhará os registros realizados pelos fiscais do contrato, de todas as ocorrências relacionadas à execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassarem a sua competência. (Decreto nº 11.246, de 2022, art. 21, II).

7.2.13. O gestor do contrato tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de eventuais sanções, a ser conduzido pela comissão de que trata o art. 158 da Lei nº 14.133, de 2021, ou pelo agente ou pelo setor com competência para tal, conforme o caso (Decreto nº 11.246, de 2022, art. 21, X).

7.2.14. O fiscal administrativo do contrato comunicará ao gestor, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à tempestiva renovação ou prorrogação contratual (Decreto nº 11.246, de 2022, art. 22, VII).

8. DA LIQUIDAÇÃO E PAGAMENTO

8.1. Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de dez dias úteis para fins de liquidação, na forma desta seção, prorrogáveis por igual período.

8.2. Para fins de liquidação, o setor competente deverá verificar se a nota fiscal ou instrumento de cobrança equivalente apresentado expressa os elementos necessários e essenciais do documento, tais como:

- a) o prazo de validade;
- b) a data da emissão;
- c) os dados do contrato e do órgão contratante;
- d) o período respectivo de execução do contrato;
- e) o valor a pagar; e
- f) eventual destaque do valor de retenções tributárias cabíveis.

8.3. Havendo erro na apresentação da nota fiscal ou instrumento de cobrança equivalente, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que a CONTRATADA providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus a CONTRATANTE.

8.4. A nota fiscal ou instrumento de cobrança equivalente deverá ser obrigatoriamente acompanhado da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 68 da Lei nº 14.133, de 2021.

8.5. A Administração deverá realizar consulta ao SICAF para:

- a) verificar a manutenção das condições de habilitação exigidas no edital;
- b) identificar possível razão que impeça a participação em licitação, no âmbito do órgão ou entidade, que implique proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas.

8.6. Constatando-se, junto ao SICAF, a situação de irregularidade da CONTRATADA, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da CONTRATANTE.

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

8.8. Persistindo a irregularidade, a CONTRATANTE deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada a CONTRATADA a ampla defesa.

8.9. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso a CONTRATADA não regularize sua situação junto ao SICAF.

8.10. O pagamento será efetuado em até 30 (trinta) dias após a aceitação do fornecimento, mediante apresentação da Nota Fiscal/Fatura devidamente atestada pelo órgão competente.

8.11. Os pagamentos só serão efetuados sob análise criteriosa e avaliação da Fiscalização, mediante apresentação dos seguintes documentos ao CONTRATANTE:

- b) Certidões negativas do INSS, FGTS, Tributos Federais, Tributos Estaduais, Tributos Municipais e Débitos Trabalhistas;
- c) É vedada a antecipação de pagamentos sem a contraprestação dos serviços/fornecimento dos produtos.

9. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

9.1. O custo estimado total da contratação é de **R\$ 42.638.348,00 (quarenta e dois milhões, seiscentos e trinta e oito mil, trezentos e quarenta e oito reais)**, conforme custos unitários apostos na tabela acima.

10. ADEQUAÇÃO ORÇAMENTÁRIA

10.1. Na licitação para Registro de Preços não haverá prévia reserva orçamentária, sendo o quantitativo do objeto pretendido indicado em termos estimativos, em função da previsão de demandas, de forma que a dotação orçamentária será indicada somente no momento da efetiva contratação dos serviços (execução da futura Ata).

10.2. As despesas decorrentes da contratação do objeto desta Licitação correrão à conta dos recursos consignados no Orçamento da CONTRATANTE, para os exercícios alcançados pelo prazo de validade da Ata de Registro de Preços, e será a cargo do Órgão Participante, cujo programa de trabalho e elemento de despesa específica constará na respectiva Nota de Empenho.

11. PENALIDADES

11.1. À CONTRATADA, em razão de eventual inadimplemento de suas obrigações, poderão ser aplicadas as sanções previstas na minuta padrão de edital, além das responsabilidades por perdas e danos, conforme disposto no Decreto Municipal nº 201/2015.

12. EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO

Felipe Augusto de Alencar Maia -Subsecretário de Infraestrutura

Abel Jose Maria Neto –Secretário de Tecnologia e Inovação

DECLARAÇÃO

Aprovo o conteúdo do Termo de Referência e Autorizo a realização da contratação conforme disposto na Lei nº 14.133/2021.

Abel Jose Maria Neto

Secretário de Tecnologia e Inovação

ANEXO I

1. DAS ESPECIFICAÇÕES TÉCNICAS DETALHADAS

- 1.1. Todas as características e especificações técnicas obrigatórias dos equipamentos ofertados deverão estar descritas em tabela específica, relacionando-as as suas especificações mínimas exigidas neste Anexo deste Termo de Referência, essa documentação será entregue junto com a documentação para habilitação e participação no certame, de forma a garantir uma rápida e melhor análise. A falta dessas documentações acima implicará na desclassificação da empresa licitante.

2. LOTE ÚNICO – ITEM 01 - MICROCOMPUTADOR TIPO I

ESPECIFICAÇÕES MÍNIMAS:

2.1. PROCESSADOR:

- 2.1.1. O modelo do processador ofertado deve ser de uma geração recente fornecido pelo fabricante, não sendo aceito modelos de processadores com o ano de lançamento inferior a janeiro de 2024 e ainda deve atender aos seguintes requisitos de desempenho e funcionalidade:
- a. Mínimo de 06 (seis) núcleos de desempenho e 12 (doze) threads de processamento;
 - b. Atender a um índice mínimo de 24.028 (vinte quatro mil e vinte e oito) pontos de desempenho, conforme a base de dados Passmark CPU Mark. Este requisito deve ser comprovado por meio de um anexo extraído do site http://www.cpubenchmark.net/cpu_list.php, datado a partir da publicação inicial deste edital.
 - c. Deve ser compatível no mínimo com memória do tipo DDR5 ou superior;
 - d. Projetado e fabricado visando uma eficiência energética superior, utilizando uma litografia máxima de 14nm para uma dissipação de calor mais eficaz.

2.2. MEMÓRIA RAM (RANDOM ACCESS MEMORY)

- 2.2.1. Deve possuir no mínimo 16 GB de memória (16GB x 1) ou (8GB x 2);
- 2.2.2. Deve ser de no mínimo padrão DDR5 com frequência de 4800 MT/s;
- 2.2.3. Deve ser compatível com a tecnologia Dual-Channel.

2.3. PLACA MÃE

- 2.3.1. Deve ser do mesmo fabricante do microcomputador ou projetada especificamente para o modelo de microcomputador ofertado, não sendo aceitas placas de livre comercialização no mercado;
- 2.3.2. Deve possuir chip de segurança TPM (Trusted Platform Module), versão 2.0, podendo ser discreto ou soldado à placa principal;

- 2.3.3. Deve suportar boot por pendrive ou disco conectado a uma porta USB;
- 2.3.4. Deve possuir suporte a expansão de memória RAM para no mínimo 64 GB;
- 2.3.5. Deve suportar a tecnologia Dual-Channel;
- 2.3.6. Deve possuir 1 slots de memória RAM livres ao final da configuração;
- 2.3.7. Deve suportar a controladora de disco padrão SATA III (6.0 Gb/s);
- 2.3.8. Deve suportar o padrão S.M.A.R.T.

2.4. BIOS

- 2.4.1. Desenvolvida pelo mesmo fabricante do microcomputador em Flash ROM ou com direito de Copyright, em conformidade com a especificação UEFI 2.7 (<http://www.uefi.org/specifications>), ou superior, e capturáveis por aplicações do tipo UCM (User Centric Management);
- 2.4.2. Para comprovação técnica que o BIOS atende e está em conformidade com as especificações exigidas na UEFI versão 2.7, ou superior, poderá ser comprovado através consulta ao site oficial: <http://www.uefi.org/members>, onde o fabricante do microcomputador ofertado deverá constar em qualquer categoria
- 2.4.3. Deverá possuir capacidade de habilitar/desabilitar as interfaces USB;
- 2.4.4. Deverá suportar senhas, configuráveis através do BIOS, do tipo:
 - a. Power-On: senha para inicialização do microcomputador;
 - b. Setup: senha para acesso e alterações de configurações;
 - c. Hard Disk: senha para inicialização e acesso ao disco de armazenamento.
- 2.4.5. Possuir solução de diagnóstico capaz de ser executado (inicializado) a partir da UEFI (Unified Extensible Firmware Interface) ou do firmware do microcomputador através do acionamento de tecla função (F1...F12). O software de diagnóstico deverá ser capaz de fazer a verificação individual e ao mesmo tempo de todos os componentes: processador, memória, unidade de armazenamento e placa mãe.

2.5. CHIPSET

- 2.5.1. Deverá ser do mesmo fabricante do processador ofertado, para melhor compatibilidade.

2.6. SLOTS E INTERFACES

- 2.6.1. O microcomputador ofertado deve possuir 01 (um) slot PCI Express livre ao final da configuração solicitada, sendo PCIe 3.0 ou superior;
- 2.6.2. Possuir, no mínimo, 05 (cinco) portas USB, sendo:
 - a. Pelo menos 02 (duas) portas USB 3.2, no padrão USB-A na parte frontal;
 - b. Pelo menos 01 (uma) porta USB 3.2, no padrão USB-C na parte frontal;
 - c. Pelo menos 02 (duas) portas USB 2.0 ou superior, no padrão USB-A na parte traseira;

- 2.6.3. O microcomputador deve possuir as seguintes saídas de vídeo:
 - a. No mínimo, 01 (uma) saída digital no padrão HDMI;
 - b. No mínimo, 01 (uma) saída digital no padrão DisplayPort.
- 2.6.4. Todas as interfaces citadas devem ser integradas ao microcomputador ofertado. Não será aceito o uso de adaptadores para atingir a quantidade de portas solicitadas.

2.7. CONTROLADORA DE DISCO RÍGIDO E ÓPTICO

- 2.7.1. Deverá possuir controladora de unidade de disco integrada a placa mãe, compatível com o padrão Serial ATA 6.0Gb/s.

2.8. ARMAZENAMENTO

- 2.8.1. Entregue com (01) uma unidade de armazenamento em estado sólido (SSD) interna, com:
 - a. Capacidade mínima de 512 GB;
 - b. Padrão de conexão M.2 Card;
 - c. Padrão de barramento PCIe NVMe;
 - d. Suporte a tecnologia S.M.A.R.T., para verificação de integridade na unidade de armazenamento.

2.9. VÍDEO

- 2.9.1. Interface com controladora de vídeo integrada com resolução mínima de 1920×1080 a 60Hz com alocação dinâmica de memória de vídeo;
- 2.9.2. Deverá suportar até 3 telas independentes no modo estendido ou espelhado;
- 2.9.3. Deverá possuir compatibilidade com a tecnologia DirectX 12;

2.10. ÁUDIO

- 2.10.1. Controladora de áudio integrada com suporte à tecnologia de Alta Definição;
- 2.10.2. Com conectores Line Out, Mic frontais integrado ao microcomputador ofertado, sendo aceito combo jack;
- 2.10.3. Deverá possuir no mínimo 01 (um) alto falante interno com potência mínima de 1 (um) Watt.

2.11. INTERFACES DE REDE

- 2.11.1. Interface de rede integrada padrão Gigabit Ethernet (IEEE 802.3) com:
 - a. Taxa de transmissão 10/100/1000 Mbps;
 - b. Deverá possuir compatibilidade com as tecnologias WoL (Wake on Lan);
 - c. Conector RJ-45 fêmea integrado à placa mãe.
- 2.11.2. Interface de rede Wireless (sem fio) padrão IEEE 802.11ax ou superior com a configuração:
 - a. Suporte as especificações IEEE 802.11ax;

- b. Suporte à tecnologia Dual Band de 2.4GHz e 5GHz;
- c. Suporte a transferência de dados mínima de 2.4 Gbps;
- d. Suporte as autenticações WPA, WPA2 e 802.1X;
- e. MU-MIMO 2x2.
- 2.11.3. Deve ser homologada e fornecida pelo mesmo fabricante do modelo de microcomputador ofertado.
- 2.11.4. Devendo possuir certificação Wifi-Alliance e homologado junto a entidade reguladora ANATEL, devendo estar vigente e serem apresentados junto a proposta.
- 2.11.5. O fabricante do microcomputador ofertado deve possuir a interface de rede homologada, a qual pode ser integrada à placa mãe ou conectada por meio de um slot padrão M.2 na placa mãe. Não serão aceitos adaptadores para atingir a quantidade de interfaces solicitadas, tampouco adaptadores externos via porta USB.

2.12. TECLADO

- 2.12.1. Teclado alfanumérico, ABNT II com 107 teclas;
- 2.12.2. Possuir bloco numérico separado das demais teclas;
- 2.12.3. Apresentar relevo nas teclas “F” e “J” do teclado alfanumérico e na tecla “5” do bloco numérico;
- 2.12.4. Possuir leds com indicação de "Numlock" e "CapsLock", e base com regulagem de inclinação;
- 2.12.5. Possuir identificação das teclas com serigrafia a quente, ou equivalente, resistente ao apagamento por uso prolongado, bem como ser resistente ao derramamento de líquidos;
- 2.12.6. Conector tipo USB, com conector compatível com o microcomputador ofertado, sem utilização de adaptador.

2.13. MOUSE

- 2.13.1. Mouse tipo óptico;
- 2.13.2. Resolução mínima de 1000 dpi;
- 2.13.3. Possuir 02 (dois) botões para seleção “click” e 01 (um) botão de rolagem “scroll”;
- 2.13.4. Possuir processo de construção para utilização ambidestra;
- 2.13.5. Conector tipo USB, com conector compatível com o microcomputador ofertado, sem utilização de adaptador.

2.14. GABINETE E FONTE DE ALIMENTAÇÃO

- 2.14.1. O gabinete deverá ser do tipo Small Form Factor (Compacto) com volume máximo de 9.500 cm³, e com índice de eficiência comprovado através de apresentação de documento emitidos pelo IT ECO Declarations, ou

equivalente, que conste compatibilidade do microcomputador ofertado com a ISO 9296, ou equivalente emitido pelo INMETRO;

- 2.14.2. O gabinete deverá possuir botão liga/desliga, luzes de indicação de atividade da unidade de disco rígido e de status ligado (power-on);
- 2.14.3. Possuir fonte de alimentação para corrente alternada com tensões de entrada de 100 a 240 VAC [±10%], 50-60Hz com ajuste automático, com potência mínima de 65 W e máxima de 360W e fator de eficiência igual ou superior a 85%; e ainda:
- 2.14.4. O modelo de fonte de alimentação ofertado deverá possuir certificação 80PLUS Bronze, comprovado através de consulta ou certificado emitido pelo site <https://www.plugloadsolutions.com/80PlusPowerSupplies.aspx>.
- 2.14.5. Possuir baixo nível de ruído conforme NBR 10.152, ISO 9296 e ISO 7779, ou equivalentes.

2.15. SISTEMA OPERACIONAL

- 2.15.1. O microcomputador deverá vir com o Microsoft Windows 11 Professional pré-instalado, em sua versão 64 bits, e em Português do Brasil;
- 2.15.2. O licenciamento do sistema operacional deverá ser fornecido pelo fabricante do microcomputador ofertado, em regime OEM, onde, por questões de segurança a chave de ativação deverá ser embarcada no próprio BIOS do microcomputador, o qual deverá ser consultada no processo ativação desta licença.

2.16. COMPATIBILIDADE

- 2.16.1. Compatibilidade com EPEAT em qualquer comprovada através de atestado e certidões que comprovem que o microcomputador ofertado é aderente ao padrão de eficiência energética EPEAT, emitido por instituo credenciado junto ao INMETRO. Será admitida como comprovação também, a indicação que o microcomputador conste em listagem e em status de "active" no site EPEAT através do link: <http://www.epeat.net>;
- 2.16.2. Apresentar certificação ou documento para o modelo de microcomputador ofertado que comprove compatibilidade com a norma IEC 60950, ou equivalente emitida pelo INMETRO;
- 2.16.3. O modelo de microcomputador ofertado deverá possuir certificação que sua fabricação está livre de 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), podendo ser comprovados através de relatório de conformidade ambiental por certificado EPEAT RoHS Criteria (<http://www.epeat.net/>);

- 2.16.4. O modelo de microcomputador ofertado deverá constar no Microsoft Windows HCL. A comprovação da compatibilidade será efetuada através de apresentação do documento Hardware Compatibility Test Report emitido especificamente para a versão do sistema operacional que o acompanha;
- 2.16.5. O fabricante do microcomputador ofertado deverá obrigatoriamente constar na lista de produtos habilitados para o padrão DMI 2.0, ou superior, como Board ou Leadership o que será conferido por meio de acesso ao site da DMTF (Distributed Management Task Force), no endereço: <http://www.dmtf.org>;
- 2.16.6. O modelo de microcomputador ofertado deve possuir certificação TCO Certified ou certificações similares nacionais, como o Rótulo Ecológico da ABNT, para garantir conformidade com os padrões de sustentabilidade e responsabilidade corporativa;
- 2.16.7. O fabricante do microcomputador ofertado deve possuir sistema de gestão ambiental com base na norma ISO 14001, devidamente comprovado através do respectivo certificado.

2.17. DIVERSOS

- 2.17.1. Todos os equipamentos (microcomputador e acessórios) a serem entregues deverão ser idênticos, conforme informados na Proposta Comercial. Caso o componente não mais se encontra disponível no mercado, admitem-se substitutos com qualidade e características idênticas ou superiores, mediante declaração técnica do fornecedor;
- 2.17.2. Componentes como teclado, mouse e demais acessórios devem ser do mesmo fabricante do microcomputador ou fabricados em regime de OEM com certificado ou declaração para os mesmos.

2.18. SISTEMA DE GERENCIAMENTO E SEGURANÇA

- 2.18.1. O microcomputador deverá possuir solução ou software do próprio fabricante que permita monitorar o sistema, realizar diagnósticos, emitir alertas e ajudar a reparar erros do sistema, ajudando assim a manter a saúde e segurança do sistema;
 - 2.18.1.1. A solução deverá funcionar tanto de forma integrada, quanto de forma isolada ("stand-alone");
 - 2.18.1.2. Todos os componentes necessários à implementação desta solução corporativa deverão pertencer à mesma família de solução corporativa, denominado neste certame como segurança de dispositivos (integrar uma única solução corporativa);

- 2.18.1.3. Todos os componentes tratados nesta descrição, deverão funcionar de forma integrada na solução. Não será aceito soluções diferentes com gestão separada;
- 2.18.1.4. A solução deverá permitir que haja troca de informações entre painel de gerenciamento e seus clientes. As informações de que trata o presente item são aqueles relevantes para a realização das ações de segurança e proteção de computadores ligados em rede, assim como monitoramento e controle.
- 2.18.1.5. A troca de informações de que trata o tópico anterior deverá permitir o recolhimento de informações sobre o estado de funcionamento da solução nas diferentes estações. As seguintes informações deverão ser contempladas, no mínimo: versão do sistema operacional, nome do host, versão do antimalware, status e informações cpu, memória, disco;
- 2.18.1.6. O acesso para ferramenta de configuração do gerenciamento em nuvem (plataforma) deverá ser com acesso seguro via https, com possibilidade de uso de duplo fator de autenticação.
- 2.18.1.7. Ter possibilidade de através de uma senha administrativa, desabilitar algumas funções do sistema de proteção local de estação ou servidor da família Windows;
- 2.18.1.8. A solução deverá permitir trabalhar obrigatoriamente na língua portuguesa do brasil e inglês;
- 2.18.1.9. A plataforma de gerenciamento em nuvem permitirá efetuar configurações e criação de políticas por grupos ou territórios em uma hierarquia do tipo árvore, selecionando qual grupo de dispositivos pertencente à que território aquela política se aplica.
- 2.18.1.10. A plataforma de gerenciamento em nuvem permitirá gerência granular de políticas, por nível hierárquico, permitindo usuário configurar políticas seguindo uma ordem de hierarquia determinada por grupos ou conjunto de computadores, sendo possível permitir a configuração de políticas como dominantes, ou seja, que não podem ser reescritas por políticas em nível hierárquico mais baixo;
- 2.18.1.11. A ferramenta deverá prover gerência de acesso para usuários de administração com vários níveis de permissão configuráveis pelo administrador principal.
- 2.18.1.12. Com relação ao sistema específico da família Microsoft Windows, o sistema deverá no mínimo ter as seguintes funcionalidades:
- 2.18.1.13. Suportar todas as funcionalidades nos sistemas Windows 10 e 11 e Windows server 2016/2019/2022
- 2.18.1.14. Verificar todos os tipos de códigos maliciosos contra os quais oferece proteção e realizar as tarefas de proteção de computadores ligados em rede em tempo real;

- 2.18.1.15. Permitir definir regras de funcionamento dos bloqueios comportamentais do antivírus, com no mínimo configuração do tipo de alerta, se o usuário será notificado para tomar uma ação, se o usuário será notificado e a ação será automática ou função silêncio onde a ação é tomada e o usuário não é notificado;
- 2.18.1.16. Permitir visualizar tempo de uso de cada aplicação e software filtrado pelo nome do usuário;
- 2.18.1.17. O console de gerenciamento web deverá prover na tela principal um dashboard com no mínimo informações sobre o percentual de máquina com número de antivírus/antimalware instalado e ameaças neutralizadas;
- 2.18.1.18. A solução deverá prover dashboard detalhado do gerenciamento do antimalware, do monitoramento e do inventário da rede com no mínimo as seguintes informações: estatísticas sobre ameaças identificadas, ameaças em quarentena, estatística de aplicação de licenças, informações quanto aos dispositivos ligados, desligados, informações sobre monitoramento de servidores, informações de monitoramento de banco de dados sqlserver, mysql, postgresql, oracle, monitoramento do serviço do Microsoft active directory e dns, informações quanto aos sistemas operacionais instalados, versão do sistema operacional, informações quanto ao número de máquinas com licença ativa do Windows bem como licenças não válidas, vencidas ou sem licença além de resumo dos 10 maiores fornecedores de software;
- 2.18.1.19. Ter painel de visualização que permita verificar através de cores e com informações básicas quais dispositivos estão com problemas, quais estão com alertas e quais estão com execução sem nenhum problema, identificando os que são ou não servidores;
- 2.18.1.20. A solução deverá prover relatórios referente as informações extraídas dos dispositivos, no mínimo deverá conter relatórios de inventário de software e hardware, relatório contendo equipamento e licença do Windows e seu status, informações da existência de algum software virtualizado instalado em algum dispositivo, relatório licença do antimalware e suas aplicações, relatório de infecções equipamento infectados, nome da infecção e nível de risco da mesma.
- 2.18.1.21. A solução deverá trazer informações sobre sistemas operacionais descontinuados, informando qual o sistema operacional bem como o equipamento que apresenta a condição;
- 2.18.1.22. Fornecer proteção, no mínimo, contra os seguintes tipos de códigos maliciosos: vírus de computador (em todas as suas variações), bombas lógicas, vermes ("worms"), cavalos de tróia ("trojan"), códigos espiões ("spyware", "keylogger", "screenlogger", etc), códigos de apoio à invasão e escalada de privilégio ("rootkit", "backdoor", etc), código e conteúdo indesejado ("dialer", "adware", "joke", etc);

- 2.18.1.23. Deverá ter a possibilidade de rastreamento manual nas estações de trabalho (programada ou não) de dispositivos móveis de armazenamento (ou não) e mídias removíveis ou quaisquer outros que permitam a transferência de arquivos para a estação de trabalho;
- 2.18.1.24. Deverá negar acesso ao arquivo infectado antes que o mesmo seja carregado em memória, aberto e/ou executado. Após negar o acesso ao arquivo infectado o antimalware deverá limpar o arquivo, e/ou apagar o arquivo infectado e enviar o arquivo infectado para uma área de segurança (quarentena);
- 2.18.1.25. Permitir detecção de ameaças em arquivos compactados nos principais algoritmos ("zip", "rar", "7zip")
- 2.18.1.26. A proteção de tempo real deverá trabalhar também com listas brancas (whitelist) permitindo adicionar um arquivo em específico ou um diretório, permitindo assim todos os arquivos de serem executados e recursivamente.
- 2.18.1.27. Permitir a execução de escaneamentos nos servidores e nas estações de trabalho (programada ou não).
- 2.18.1.28. Possuir camada de proteção contra acesso a sites fraudulentos e perigosos;
- 2.18.1.29. Possuir camada de proteção de arquivos contra sequestro de informações;
- 2.18.1.30. Possuir camada de proteção comportamental contra programas e/ou comportamentos suspeitos;
- 2.18.1.31. Ter módulo de histórico com uma lista de ações executadas pelo sistema antivírus/antimalware;
- 2.18.1.32. Permitir gerar "kit de emergência" que permitirá usuário dar boot na máquina e efetuar limpeza manual;
- 2.18.1.33. Possuir módulo de bloqueio por meio de comportamento dos processos, sistemas e programas;
- 2.18.1.34. A solução deverá proteger os arquivos através de análise comportamental, ou seja, proteger arquivos mesmo que a solução não disponha de assinatura para esse artefato, permitindo também a inclusão de arquivos na lista branca ou negra para análise comportamental de arquivos, inclusão de um arquivo somente para monitoramento bem como definir um arquivo ou aplicação que deverá ser bloqueada, permitindo configurar se tal ação será ou não notificada ao usuário, sendo que essa notificação ao usuário deverá ser em português do Brasil.
- 2.18.1.35. Além dos componentes responsáveis pelo combate a códigos maliciosos, possuir também componente responsável por implementar uma camada de proteção para acesso a internet que impeça abertura de sites com risco de acesso a conteúdos maliciosos;

- 2.18.1.36. Permitir a inclusão de arquivos na lista branca ou negra para com base em assinaturas, inclusão de um arquivo somente para monitoramento bem como definir um arquivo ou aplicação que deverá ser bloqueada, permitindo configurar se tal ação será ou não notificada ao usuário, sendo que essa notificação ao usuário deverá ser em português do Brasil, para esse item deverá permitir ativação ou não de proteção quanto pup do acrônimo em inglês possible unintended programs, ou seja, programas possivelmente indesejados como exemplos adwares e spywares;
- 2.18.1.37. A solução deverá prover proteção quanto a navegação, para essa função a solução deverá funcionar sem a necessidade de instalação de outro agente ou plugins nos navegadores;
- 2.18.1.38. Para a proteção de navegação a solução deverá permitir no mínimo proteção quanto sites maliciosos com base própria, sites com conteúdo indesejados (pup - possible unintended programs), bem como permitir a inclusão manual pelo administrador de sites na lista branca bem como na lista negra;
- 2.18.1.39. A solução deverá permitir agendamento de scan no dispositivo, podendo criar mais do que umas regras de agendamento separado entre rápido e completo, determinando dia e horário assim como a frequência;
- 2.18.1.40. A solução deverá permitir executar comandos e scripts remotos na estação, deverá permitir no mínimo acionar desinstalação de um software instalado, desinstalar ou instalar o antimalware, reiniciar dispositivo, desligar dispositivo, bloquear o dispositivo com possibilidade de desbloqueio através de uma senha específica.
- 2.18.1.41. Trazer a localização georreferenciada do dispositivo de maneira automática ou permitir configurar de maneira manual a latitude e longitude para localização do dispositivo;
- 2.18.1.42. Permitir acessar remotamente o equipamento direto do painel cloud, a solução permitirá o acesso através de solicitação ou diretamente sem solicitação de autorização;
- 2.18.1.43. Permitir configuração de tipos de alertas, para monitoramento dos dispositivos tais como: percentuais de CPU, memória e disco e tais informações deverão estar disponíveis em um painel ou dashboard específico para monitoramento;
- 2.18.1.44. O sistema deverá trazer no mínimo as seguintes informações de cada dispositivo: status do dispositivo, data em que os dados foram coletados, o número da licença do sistema operacional Windows bem como o status da licença daquele dispositivo, nome do host, versão do antivírus/antimalware, versão do sistema operacional, usuário logado no dispositivo, tempo de atividade, consumo e total de CPU, consumo e total de memória RAM, consumo e total de memória swap, consumo e volume total de disco, interfaces de rede,

serviços que estão em execução, serviços que estão parados, processos que estão mais consumindo cpu, processos que estão mais consumindo memória, informações de hardware, tais como: drivers de impressora, cd-rom, dispositivos gerais, ide, usb, som, vídeo, adaptador de rede, processador, bios, memória, placa de som, disco, memória, informações dos softwares instalados, tais como: fabricantes, software e versão;

- 2.18.1.45. O sistema deverá permitir monitoramento por meio de protocolo snmp de qualquer dispositivo conectado na rede, através da definição de qual dispositivo será o coletor dos dados e o mesmo centralizar as informações mostrando na plataforma
- 2.18.1.46. A plataforma deverá permitir ligar os dispositivos através do recurso wake-on-lan, caso o dispositivo possua este recurso e esteja ativada na bios;
- 2.18.1.47. O sistema deverá ter funcionalidade de proteção contra gravação de tela e printscreen através da inserção automática de marcas d'água ao realizar capturas de tela ou gravações de vídeo;
- 2.18.1.48. O sistema deverá ter recurso de visualização de documentos, através do endpoint, alertando o usuário caso tenha um documento obrigatório a ser visualizado, permitindo o mesmo registrar a visualização através de um token recebido por e-mail;
- 2.18.1.49. O sistema deverá ter bloqueio da função que permite o dispositivo se torne um ponto de hotspot (ponto específico em uma área física onde é possível acessar a internet, geralmente por meio de uma rede sem fio (wifi)), mantendo assim sua rede protegida evitando potenciais ameaças, garantindo um ambiente seguro e confiável.
- 2.18.1.50. O sistema deverá permitir o controle e gestão de patches do sistema operacional e outros produtos Microsoft gerenciáveis pelo Windows update;
- 2.18.1.51. O sistema deverá permitir configurar alertas através de configuração de identificação de um padrão de log no dispositivo, que pode ser configurado direto no painel em nuvem.
- 2.18.1.52. O sistema permitirá definir quais dispositivos serão centralizados de atualizações na rede. A partir do momento que for definido, os demais dispositivos da mesma rede, se atualização direto no centralizador;
- 2.18.1.53. O sistema permitirá efetuar agendamentos com objetivo de descoberta de novos dispositivos na rede. O agendamento poderá ser feito por dispositivo localizado em uma sub-rede e deverá mostrar a listagem de todos dispositivos que possuam ip na mesma;
- 2.18.1.54. O sistema terá um módulo de prevenção contra vazamento de dados (dlp – data loss prevention), que permitirá identificar através de scan se o dispositivo scaneado possui algum dado previamente cadastrado como alvo da prevenção através de expressão regular, permitindo que o sistema possa cadastrar novas informações usando a mesma sintaxe.

- 2.18.1.55. No caso de smartphones android, o sistema deverá prover as funcionalidades de:
- 2.18.1.56. Gerenciar os aplicativos que poderão ou não serem executados no dispositivo
- 2.18.1.57. Permitir bloqueio de determinados aplicativos por horário
- 2.18.1.58. Restringir seu funcionamento pela velocidade em km por hora, a fim de garantir segurança durante o uso e veículos
- 2.18.1.59. Configuração remota de redes wifi
- 2.18.1.60. Disponibilizar informações sobre monitoramento de memória, bateria, temperatura, localização
- 2.18.1.61. Disponibilizar informações sobre o dispositivo como sistema operacional, modelo dos dispositivos, versões, contas cadastradas e em uso, operadora, redes conectadas
- 2.18.1.62. No caso de dispositivo com sistema operacional Linux, o sistema deverá prover as funcionalidades de:
- 2.18.1.63. A solução deverá prover agente para monitoramento dos sistemas operacionais Linux prevendo ao menos o funcionamento nas versões centos 7 e 7, debian 8, 9 e 10, ubuntu 14, 16 e 18;
- 2.18.1.64. A solução deverá prover monitoramento dos agentes em Linux prevendo ao menos:
- 2.18.1.65. Ativar ou desativar recebimento de alerta dos dispositivos;
- 2.18.1.66. Verificar todos os tipos de códigos maliciosos contra os quais oferece proteção;
- 2.18.1.67. Permitir configuração de tipos de alertas, para monitoramento dos dispositivos tais como: percentuais de cpu, memória e disco e tais informações deverão estar disponíveis em um painel ou dashboard específico para monitoramento;
- 2.18.1.68. Trazer as seguintes informações de cada dispositivo: status do dispositivo, data em que os dados foram coletados, nome do host, versão do sistema operacional, usuário logado no dispositivo, consumo e total de cpu, consumo e total de memória ram, consumo e total de memória swap, consumo e volume total de disco e suas partições, interfaces de rede, serviços que estão em execução, serviços que estão parados, processos que estão mais consumindo cpu, processos que estão mais consumindo memória, histórico de comandos executados, localização do dispositivo em mapa georreferenciado, a solução deverá permitir configurar quais serviços o agente irá monitorar e em caso de parada do serviço o agente deverá reiniciar o mesmo;
- 2.18.1.69. A solução em nuvem deverá prover modulo de monitoramento de todas as soluções acima no mesmo painel de gerenciamento com objetivo de facilitar a operação;

- 2.18.1.70. O módulo de monitoramento deverá prover painel próprio na plataforma web com atualização em tempo real do alerta bem como prover app para ser instalado em dispositivos móveis da família android;
- 2.18.1.71. Deverá disponibilizar função modo tv para facilitar a análise das informações;
- 2.18.1.72. Deverá permitir configurar frequência de envio de alertas, com no mínimo configuração de 5, 25 ou 50 minutos entre a repetição do alerta.
- 2.18.1.73. O monitoramento de endpoint e servidores, a solução deverá prover ao menos os seguintes monitores: cpu, memória e disco;
- 2.18.1.74. Se o serviço de proteção está ativo, em caso de desativar o serviço de proteção em tempo real ou serviço de proteção de navegação, para esse item deverá ser enviado um relatório informando os equipamentos com proteção desativadas ou inexistentes;
- 2.18.1.75. Alerta configurável pelo administrador entre uma range de valores para emissão de alertas entre crítico, atenção ou informativo de no mínimo cpu, memória e carga média;
- 2.18.1.76. Permitir monitorar as interfaces de rede;
- 2.18.1.77. A solução deverá permitir o monitoramento dos serviços do sistema operacional.
- 2.18.1.78. Permitir emitir alertas de uptime de um determinado website através da configuração da url, assim como certificado ssl, lista negra;

2.19. MONITOR

- 2.19.1. Deverá ser fornecido 01 (um) monitor, com as características mínimas:
 - a. O monitor deve possuir tamanho de tela de no mínimo 21.5 polegadas;
 - b. Deverá ser do tipo LED, no formato Widescreen;
 - c. Deverá possuir proporção de 16:9;
 - d. Deverá possuir ângulo de visão de no mínimo 178° horizontal e vertical;
 - e. Deve possuir brilho de no mínimo 250 cd/m²;
 - f. A taxa de contraste real mínima de 1000:1;
 - g. O tempo de resposta não deve ultrapassar 8ms;
 - h. Deve suportar resolução nativa mínima de 1920x1080 pixels a 60 Hz;
 - i. Deve possuir pelo menos 1 (uma) conexão digital, DisplayPort ou HDMI;
 - j. Deve ser fornecido junto com o monitor, na mesma caixa e pelo fabricante do monitor, 1 (um) cabo DisplayPort ou HDMI para interligar o monitor ao microcomputador ofertado;
 - k. Deve possuir uma entrada analógica VGA;
 - l. Deve possuir fonte de alimentação interna com tensão de entrada bivolt automática;
 - m. Deve possuir base com ajustes mínimos, de: inclinação, altura e rotação pivot (retrato/paisagem).

2.20. COMPATIBILIDADES E CERTIFICAÇÕES:

- 2.20.1. Com EPEAT em qualquer categoria, comprovada através de atestado e certidões que comprovem que o monitor ofertado é aderente ao padrão de eficiência energética EPEAT, emitido por instituo credenciado junto ao INMETRO. Será admitida como comprovação também, a indicação que o monitor consta em listagem e em status de “active” no site EPEAT através do link: <http://www.epeat.net>;
- 2.20.2. Certificação ENERGY STAR, comprovando que o monitor ofertado atinge as exigências para o melhor aproveitamento de uso de energia elétrica. Essa característica deverá ser comprovada pela listagem do monitor no site <http://www.energystar.gov>. Serão aceitas as certificações emitidas pelo INMETRO, em conformidade com as Portarias nº 170/2012 e 304/2023;
- 2.20.3. O monitor ofertado deverá possuir certificação que sua fabricação está livre de 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).

3. LOTE ÚNICO – ITEM 02 - MICROCOMPUTADOR TIPO II

ESPECIFICAÇÕES MÍNIMAS:

3.1. PROCESSADOR:

- 3.1.1. O modelo do processador ofertado deve ser de uma geração recente fornecido pelo fabricante, não sendo aceito modelos de processadores com o ano de lançamento inferior a julho de 2024 e ainda deve atender aos seguintes requisitos de desempenho e funcionalidade:
 - a. Mínimo de 04 (quatro) núcleos de desempenho e 8 (oito) threads de processamento;
 - b. Atender a um índice mínimo de 14.980 (quatorze mil novecentos e oitenta) pontos de desempenho, conforme a base de dados Passmark CPU Mark. Este requisito deve ser comprovado por meio de um anexo extraído do site http://www.cpubenchmark.net/cpu_list.php, datado a partir da publicação inicial deste edital.
 - c. Deve ser compatível no mínimo com memória do tipo DDR5 ou superior;
 - d. Projetado e fabricado visando uma eficiência energética superior, utilizando uma litografia máxima de 14nm para uma dissipação de calor mais eficaz.

3.2. MEMÓRIA RAM (RANDOM ACCESS MEMORY)

- 3.2.1. Deve possuir no mínimo 16 GB de memória em um único módulo;

- 3.2.2. Deve ser de no mínimo padrão DDR5 com frequência de 4800 MT/s;
- 3.2.3. Deve ser compatível com a tecnologia Dual-Channel.

3.3. PLACA MÃE

- 3.3.1. Deve ser do mesmo fabricante do microcomputador ou projetada especificamente para o modelo de microcomputador ofertado, não sendo aceitas placas de livre comercialização no mercado;
- 3.3.2. Deve possuir chip de segurança TPM (Trusted Platform Module), versão 2.0, podendo ser discreto ou soldado à placa principal;
- 3.3.3. Deve suportar boot por pendrive ou disco conectado a uma porta USB;
- 3.3.4. Deve possuir suporte a expansão de memória RAM para no mínimo 32 GB;
- 3.3.5. Deve suportar a tecnologia Dual-Channel;
- 3.3.6. Deve possuir 1 slots de memória RAM livres ao final da configuração;
- 3.3.7. Deverá suportar a controladora de disco padrão SATA III (6.0 Gb/s);
- 3.3.8. Possuir 2 (dois) slots M.2 para SSD e 1 (um) para interface de rede wireless;
- 3.3.9. Deve suportar o padrão S.M.A.R.T.

3.4. BIOS

- 3.4.1. Deve ser desenvolvida pelo mesmo fabricante do microcomputador, armazenada em Flash ROM com direitos de copyright, e estar em conformidade com a especificação UEFI 2.7 (<http://www.uefi.org/specifications>) ou versão superior. Além disso, deve ser capturável por aplicativos do tipo UCM (User Centric Management);
- 3.4.2. Para comprovação técnica que o BIOS atende e está em conformidade com as especificações exigidas na UEFI versão 2.7, ou superior, poderá ser comprovado através consulta ao site oficial: <http://www.uefi.org/members>, onde o fabricante do microcomputador ofertado deverá constar em qualquer categoria”;
- 3.4.3. Deverá possuir capacidade de habilitar/desabilitar as interfaces USB;
- 3.4.4. Deverá suportar senhas, configuráveis através do BIOS, do tipo:
 - d. Power-On: senha para inicialização do microcomputador;
 - e. Setup: senha para acesso e alterações de configurações;
 - f. Hard Disk: senha para inicialização e acesso ao disco de armazenamento.
- 3.4.5. Possuir solução de diagnóstico capaz de ser executado (inicializado) a partir da UEFI (Unified Extensible Firmware Interface) ou do firmware do microcomputador através do acionamento de tecla função (F1...F12). O software de diagnóstico deverá ser capaz de fazer a verificação individual e ao mesmo tempo de todos os componentes: processador, memória, unidade de armazenamento e placa mãe.

3.5. CHIPSET

- 3.5.1. Deverá ser do mesmo fabricante do processador ofertado, para melhor compatibilidade.

3.6. SLOTS E INTERFACES

- 3.6.1. Possuir, no mínimo, 05 (cinco) portas USB, sendo:
- a. Pelo menos 02 (duas) portas USB 3.2, no padrão USB-A na parte frontal;
 - b. Pelo menos 01 (uma) porta USB 3.2, no padrão USB-C na parte frontal;
 - c. Pelo menos 02 (duas) portas USB 2.0 ou superior, no padrão USB-A na parte traseira.
- 3.6.2. O microcomputador deve possuir as seguintes saídas de vídeo:
- a. No mínimo, 01 (uma) saída digital no padrão HDMI;
 - b. No mínimo, 01 (uma) saída digital no padrão DisplayPort.
- 3.6.3. Todas as interfaces citadas devem ser integradas ao microcomputador ofertado. Não será aceito o uso de adaptadores para atingir a quantidade de portas solicitadas.

3.7. CONTROLADORA DE DISCO RÍGIDO E ÓPTICO

- 3.7.1. Deverá possuir controladora de unidade de disco integrada a placa mãe, compatível com o padrão Serial ATA 6.0Gb/s ou superior.

3.8. ARMAZENAMENTO

- 3.8.1. Entregue com (01) uma unidade de armazenamento em estado sólido (SSD) interna, com:
- a. Capacidade mínima de 512GB;
 - b. Padrão de conexão M.2 Card;
 - c. Padrão de barramento PCIe NVMe;
 - d. Suporte a tecnologia S.M.A.R.T., para verificação de integridade na unidade de armazenamento

3.9. VÍDEO

- 3.9.1. Interface com controladora de vídeo integrada com resolução mínima de 1920×1080 a 60Hz com alocação dinâmica de memória de vídeo;
- 3.9.2. Deverá suportar até 3 telas independentes no modo estendido ou espelhado;
- 3.9.3. Deverá possuir compatibilidade com a tecnologia DirectX 12.

3.10. ÁUDIO

- 3.10.1. Controladora de áudio integrada com suporte à tecnologia de Alta Definição;
- 3.10.2. Com conectores Line Out, Mic frontais integrado ao microcomputador ofertado, sendo aceito combo jack;

- 3.10.3. Deverá possuir no mínimo 01 (um) alto falante interno com potência mínima de 1 (um) Watt.

3.11. INTERFACES DE REDE

- 3.11.1. Interface de rede integrada padrão Gigabit Ethernet (IEEE 802.3) com:
- a. Taxa de transmissão 10/100/1000 Mbps;
 - b. Deverá possuir compatibilidade com as tecnologias WoL (Wake on Lan);
 - c. Conector RJ-45 fêmea integrado à placa mãe.
- 3.11.2. Interface de rede Wireless (sem fio) padrão IEEE 802.11ax com a configuração:
- a. Suporte as especificações IEEE 802.11 abgn;
 - b. Suporte à tecnologia Dual Band de 2.4GHz e 5GHz;
 - c. Suporte a transferência de dados mínima de 2.4 Gbps;
 - d. Suporte as autenticações WPA, WPA2 e 802.1X;
 - e. MU-MIMO 2x2;
- 3.11.3. Deve ser homologada e fornecida pelo mesmo fabricante do modelo de microcomputador ofertado.
- 3.11.4. Devendo possuir certificação Wifi-Alliance e homologado junto a entidade reguladora ANATEL, devendo estar vigente e serem apresentados junto a proposta.
- 3.11.5. O fabricante do microcomputador ofertado deve possuir a interface de rede homologada, a qual pode ser integrada à placa mãe ou conectada por meio de um slot padrão M.2 na placa mãe. Não serão aceitos adaptadores para atingir a quantidade de interfaces solicitadas, tampouco adaptadores externos via porta USB.

3.12. TECLADO

- 3.12.1. Teclado alfanumérico, ABNT II com 107 teclas;
- 3.12.2. Possuir bloco numérico separado das demais teclas;
- 3.12.3. Apresentar relevo nas teclas "F" e "J" do teclado alfanumérico e na tecla "5" do bloco numérico;
- 3.12.4. Possuir leds com indicação de "Numlock" e "CapsLock", e base com regulagem de inclinação;
- 3.12.5. Possuir identificação das teclas com serigrafia a quente, ou equivalente, resistente ao apagamento por uso prolongado, bem como ser resistente ao derramamento de líquidos;
- 3.12.6. Conector tipo USB, com conector compatível com o microcomputador ofertado, sem utilização de adaptador.

3.13. MOUSE

- 3.13.1. Mouse tipo óptico;

- 3.13.2. Resolução mínima de 1000 dpi;
- 3.13.3. Possuir 02 (dois) botões para seleção “click” e 01 (um) botão de rolagem “scroll”;
- 3.13.4. Possuir processo de construção para utilização ambidestra;
- 3.13.5. Conector tipo USB, com conector compatível com o microcomputador ofertado, sem utilização de adaptador.

3.14. GABINETE E FONTE DE ALIMENTAÇÃO

- 3.14.1. O gabinete deverá ser do tipo Small Form Factor (Compacto) com volume máximo de 9.500 cm³, e com índice de eficiência comprovado através de apresentação de documento emitido pelo IT ECO Declarations, ou equivalente, que conste compatibilidade do microcomputador ofertado com a ISO 9296, ou equivalente emitido pelo INMETRO;
- 3.14.2. O gabinete deverá possuir botão liga/desliga, luzes de indicação de atividade da unidade de disco rígido e de status ligado (power-on);
- 3.14.3. Possuir fonte de alimentação para corrente alternada com tensões de entrada de 100 a 240 VAC [±10%], 50-60Hz com ajuste automático, com potência mínima de 65 W e máxima de 360W e fator de eficiência igual ou superior a 85%; e ainda:
- 3.14.4. O modelo de fonte de alimentação ofertado deverá possuir certificação 80PLUS Bronze, comprovado através de consulta ou certificado emitido pelo site <https://www.plugloadsolutions.com/80PlusPowerSupplies.aspx>.
- 3.14.5. Possuir baixo nível de ruído conforme NBR 10.152, ISO 9296 e ISO 7779, ou equivalentes.

3.15. SISTEMA OPERACIONAL

- 3.15.1. O microcomputador deverá vir com o Microsoft Windows 11 Professional pré-instalado, em sua versão 64 bits, e em Português do Brasil;
- 3.15.2. O licenciamento do sistema operacional deverá ser fornecido pelo fabricante do microcomputador ofertado, em regime OEM, onde, por questões de segurança a chave de ativação deverá ser embarcada no próprio BIOS do microcomputador, o qual deverá ser consultada no processo ativação desta licença.

3.16. COMPATIBILIDADE

- 3.16.1. Compatibilidade com EPEAT em qualquer comprovada através de atestado e certidões que comprovem que o microcomputador ofertado é aderente ao padrão de eficiência energética EPEAT, emitido por instituo credenciado junto ao INMETRO. Será admitida como comprovação também, a indicação que o microcomputador conste em listagem e em status de "active" no site EPEAT através do link: <http://www.epeat.net>;

- 3.16.2. Apresentar certificação ou documento para o modelo de microcomputador ofertado que comprove compatibilidade com a norma IEC 60950, ou equivalente emitida pelo INMETRO;
- 3.16.3. O modelo de microcomputador ofertado deverá possuir certificação que sua fabricação está livre de 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), podendo ser comprovados através de relatório de conformidade ambiental por certificado EPEAT RoHS Criteria (<http://www.epeat.net/>);
- 3.16.4. O modelo de microcomputador ofertado deverá constar no Microsoft Windows HCL. A comprovação da compatibilidade será efetuada através de apresentação do documento Hardware Compatibility Test Report emitido especificamente para a versão do sistema operacional que o acompanha;
- 3.16.5. O fabricante do microcomputador ofertado deverá obrigatoriamente constar na lista de produtos habilitados para o padrão DMI 2.0, ou superior, como Board ou Leadership o que será conferido por meio de acesso ao site da DMTF (Distributed Management Task Force), no endereço: <http://www.dmtf.org>;
- 3.16.6. O modelo de microcomputador ofertado deve possuir certificação TCO Certified ou certificações similares nacionais, como o Rótulo Ecológico da ABNT, para garantir conformidade com os padrões de sustentabilidade e responsabilidade corporativa;
- 3.16.7. O fabricante do microcomputador ofertado deve possuir sistema de gestão ambiental com base na norma ISO 14001, devidamente comprovado através do respectivo certificado.

3.17. DIVERSOS

- 3.17.1. Todos os equipamentos (microcomputador e acessórios) a serem entregues deverão ser idênticos, conforme informados na Proposta Comercial. Caso o componente não mais se encontra disponível no mercado, admitem-se substitutos com qualidade e características idênticas ou superiores, mediante declaração técnica do fornecedor;
- 3.17.2. Componentes como teclado, mouse e demais acessórios devem ser do mesmo fabricante do microcomputador ou fabricados em regime de OEM com certificado ou declaração para os mesmos.

3.18. SISTEMA DE GERENCIAMENTO E SEGURANÇA

- 3.18.1. O microcomputador deverá possuir solução ou software do próprio fabricante que permita monitorar o sistema, realizar diagnósticos, emitir alertas e ajudar

a reparar erros do sistema, ajudando assim a manter a saúde e segurança do sistema;

- 3.18.1.1. A solução deverá funcionar tanto de forma integrada, quanto de forma isolada (“stand-alone”);
- 3.18.1.2. Todos os componentes necessários à implementação desta solução corporativa deverão pertencer à mesma família de solução corporativa, denominado neste certame como segurança de dispositivos (integrar uma única solução corporativa);
- 3.18.1.3. Todos os componentes tratados nesta descrição, deverão funcionar de forma integrada na solução. Não será aceito soluções diferentes com gestão separada;
- 3.18.1.4. A solução deverá permitir que haja troca de informações entre painel de gerenciamento e seus clientes. As informações de que trata o presente item são aqueles relevantes para a realização das ações de segurança e proteção de computadores ligados em rede, assim como monitoramento e controle.
- 3.18.1.5. A troca de informações de que trata o tópico anterior deverá permitir o recolhimento de informações sobre o estado de funcionamento da solução nas diferentes estações. As seguintes informações deverão ser contempladas, no mínimo: versão do sistema operacional, nome do host, versão do antimalware, status e informações cpu, memória, disco;
- 3.18.1.6. O acesso para ferramenta de configuração do gerenciamento em nuvem (plataforma) deverá ser com acesso seguro via https, com possibilidade de uso de duplo fator de autenticação.
- 3.18.1.7. Ter possibilidade de através de uma senha administrativa, desabilitar algumas funções do sistema de proteção local de estação ou servidor da família Windows;
- 3.18.1.8. A solução deverá permitir trabalhar obrigatoriamente na língua portuguesa do brasil e inglês;
- 3.18.1.9. A plataforma de gerenciamento em nuvem permitirá efetuar configurações e criação de políticas por grupos ou territórios em uma hierarquia do tipo árvore, selecionando qual grupo de dispositivos pertencente à que território aquela política se aplica.
- 3.18.1.10. A plataforma de gerenciamento em nuvem permitirá gerência granular de políticas, por nível hierárquico, permitindo usuário configurar políticas seguindo uma ordem de hierarquia determinada por grupos ou conjunto de computadores, sendo possível permitir a configuração de políticas como dominantes, ou seja, que não podem ser reescritas por políticas em nível hierárquico mais baixo;
- 3.18.1.11. A ferramenta deverá prover gerência de acesso para usuários de administração com vários níveis de permissão configuráveis pelo administrador principal.

- 3.18.1.12. Com relação ao sistema específico da família Microsoft Windows, o sistema deverá no mínimo ter as seguintes funcionalidades:
- 3.18.1.13. Suportar todas as funcionalidades nos sistemas Windows 10 e 11 e Windows server 2016/2019/2022
- 3.18.1.14. Verificar todos os tipos de códigos maliciosos contra os quais oferece proteção e realizar as tarefas de proteção de computadores ligados em rede em tempo real;
- 3.18.1.15. Permitir definir regras de funcionamento dos bloqueios comportamentais do antivírus, com no mínimo configuração do tipo de alerta, se o usuário será notificado para tomar uma ação, se o usuário será notificado e a ação será automática ou função silêncio onde a ação é tomada e o usuário não é notificado;
- 3.18.1.16. Permitir visualizar tempo de uso de cada aplicação e software filtrado pelo nome do usuário;
- 3.18.1.17. O console de gerenciamento web deverá prover na tela principal um dashboard com no mínimo informações sobre o percentual de máquina com número de antivírus/antimalware instalado e ameaças neutralizadas;
- 3.18.1.18. A solução deverá prover dashboard detalhado do gerenciamento do antimalware, do monitoramento e do inventário da rede com no mínimo as seguintes informações: estatísticas sobre ameaças identificadas, ameaças em quarentena, estatística de aplicação de licenças, informações quanto aos dispositivos ligados, desligados, informações sobre monitoramento de servidores, informações de monitoramento de banco de dados sqlserver, mysql, postgresql, oracle, monitoramento do serviço do Microsoft active directory e dns, informações quanto aos sistema operacionais instalados, versão do sistema operacional, informações quanto ao número de máquinas com licença ativa do Windows bem como licenças não validas, vencidas ou sem licença além de resumo dos 10 maiores fornecedores de software;
- 3.18.1.19. Ter painel de visualização que permita verificar através de cores e com informações básicas quais dispositivos estão com problemas, quais estão com alertas e quais estão com execução sem nenhum problema, identificando os que são ou não servidores;
- 3.18.1.20. A solução deverá prover relatórios referente as informações extraídas dos dispositivos, no mínimo deverá conter relatórios de inventário de software e hardware, relatório contendo equipamento e licença do Windows e seu status, informações da existência de algum software virtualizado instalado em algum dispositivo, relatório licença do antimalware e suas aplicações, relatório de infecções equipamento infectados, nome da infecção e nível de risco da mesma.

- 3.18.1.21. A solução deverá trazer informações sobre sistemas operacionais descontinuados, informando qual o sistema operacional bem como o equipamento que apresenta a condição;
- 3.18.1.22. Fornecer proteção, no mínimo, contra os seguintes tipos de códigos maliciosos: vírus de computador (em todas as suas variações), bombas lógicas, vermes ("worms"), cavalos de tróia ("trojan"), códigos espiões ("spyware", "keylogger", "screenlogger", etc), códigos de apoio à invasão e escalada de privilégio ("rootkit", "backdoor", etc), código e conteúdo indesejado ("dialer", "adware", "joke", etc);
- 3.18.1.23. Deverá ter a possibilidade de rastreamento manual nas estações de trabalho (programada ou não) de dispositivos móveis de armazenamento (ou não) e mídias removíveis ou quaisquer outros que permitam a transferência de arquivos para a estação de trabalho;
- 3.18.1.24. Deverá negar acesso ao arquivo infectado antes que o mesmo seja carregado em memória, aberto e/ou executado. Após negar o acesso ao arquivo infectado o antimalware deverá limpar o arquivo, e/ou apagar o arquivo infectado e enviar o arquivo infectado para uma área de segurança (quarentena);
- 3.18.1.25. Permitir detecção de ameaças em arquivos compactados nos principais algoritmos ("zip", "rar", "7zip")
- 3.18.1.26. A proteção de tempo real deverá trabalhar também com listas brancas (whitelist) permitindo adicionar um arquivo em específico ou um diretório, permitindo assim todos os arquivos de serem executados e recursivamente.
- 3.18.1.27. Permitir a execução de escaneamentos nos servidores e nas estações de trabalho (programada ou não).
- 3.18.1.28. Possuir camada de proteção contra acesso a sites fraudulentos e perigosos;
- 3.18.1.29. Possuir camada de proteção de arquivos contra sequestro de informações;
- 3.18.1.30. Possuir camada de proteção comportamental contra programas e/ou comportamentos suspeitos;
- 3.18.1.31. Ter módulo de histórico com uma lista de ações executadas pelo sistema antivírus/antimalware;
- 3.18.1.32. Permitir gerar "kit de emergência" que permitirá usuário dar boot na máquina e efetuar limpeza manual;
- 3.18.1.33. Possuir módulo de bloqueio por meio de comportamento dos processos, sistemas e programas;
- 3.18.1.34. A solução deverá proteger os arquivos através de análise comportamental, ou seja, proteger arquivos mesmo que a solução não disponha de assinatura para esse artefato, permitindo também a inclusão de arquivos na lista branca ou negra para análise comportamental de arquivos,

inclusão de um arquivo somente para monitoramento bem como definir um arquivo ou aplicação que deverá ser bloqueada, permitindo configurar se tal ação será ou não notificada ao usuário, sendo que essa notificação ao usuário deverá ser em português do brasil.

- 3.18.1.35. Além dos componentes responsáveis pelo combate a códigos maliciosos, possuir também componente responsável por implementar uma camada de proteção para acesso a internet que impeça abertura de sites com risco de acesso a conteúdos maliciosos;
- 3.18.1.36. Permitir a inclusão de arquivos na lista branca ou negra para com base em assinaturas, inclusão de um arquivo somente para monitoramento bem como definir um arquivo ou aplicação que deverá ser bloqueada, permitindo configurar se tal ação será ou não notificada ao usuário, sendo que essa notificação ao usuário deverá ser em português do brasil, para esse item deverá permitir ativação ou não de proteção quanto pup do acrônico em inglês possible unintended programs, ou seja, programas possivelmente indesejados como exemplos adwares e spywares;
- 3.18.1.37. A solução deverá prover proteção quanto a navegação, para essa função a solução deverá funcionar sem a necessidade de instalação de outro agente ou plugins nos navegadores;
- 3.18.1.38. Para a proteção de navegação a solução deverá permitir no mínimo proteção quanto sites maliciosos com base própria, sites com conteúdo indesejados (pup - possible unintended programs), bem como permitir a inclusão manual pelo administrador de sites na lista branca bem como na lista negra;
- 3.18.1.39. A solução deverá permitir agendamento de scan no dispositivo, podendo criar mais do que umas regras de agendamento separado entre rápido e completo, determinando dia e horário assim como a frequência;
- 3.18.1.40. A solução deverá permitir executar comandos e scripts remotos na estação, deverá permitir no mínimo acionar desinstalação de um software instalado, desinstalar ou instalar o antimalware, reiniciar dispositivo, desligar dispositivo, bloquear o dispositivo com possibilidade de desbloqueio através de uma senha específica.
- 3.18.1.41. Trazer a localização georreferenciada do dispositivo de maneira automática ou permitir configurar de maneira manual a latitude e longitude para localização do dispositivo;
- 3.18.1.42. Permitir acessar remotamente o equipamento direto do painel cloud, a solução permitirá o acesso através de solicitação ou diretamente sem solicitação de autorização;
- 3.18.1.43. Permitir configuração de tipos de alertas, para monitoramento dos dispositivos tais como: percentuais de cpu, memória e disco e tais informação

deverão estar disponíveis em um painel ou dashboard específico para monitoramento;

- 3.18.1.44. O sistema deverá trazer no mínimo as seguintes informações de cada dispositivo: status do dispositivo, data em que os dados foram coletados, o número da licença do sistema operacional Windows bem como o status da licença daquele dispositivo, nome do host, versão do antivírus/antimalware, versão do sistema operacional, usuário logado no dispositivo, tempo de atividade, consumo e total de cpu, consumo e total de memória ram, consumo e total de memória swap, consumo e volume total de disco, interfaces de rede, serviços que estão em execução, serviços que estão parados, processos que estão mais consumindo cpu, processos que estão mais consumindo memória, informações de hardware, tais como: drivers de impressora, cd-rom, dispositivos gerais, ide, usb, som, vídeo, adaptador de rede, processador, bios, memória, placa de som, disco, memória, informações dos softwares instalados, tais como: fabricantes, software e versão;
- 3.18.1.45. O sistema deverá permitir monitoramento por meio de protocolo snmp de qualquer dispositivo conectado na rede, através da definição de qual dispositivo será o coletor dos dados e o mesmo centralizar as informações mostrando na plataforma
- 3.18.1.46. A plataforma deverá permitir ligar os dispositivos através do recurso wake-on-lan, caso o dispositivo possua este recurso e esteja ativada na bios;
- 3.18.1.47. O sistema deverá ter funcionalidade de proteção contra gravação de tela e printscreen através da inserção automática de marcas d'água ao realizar capturas de tela ou gravações de vídeo;
- 3.18.1.48. O sistema deverá ter recurso de visualização de documentos, através do endpoint, alertando o usuário caso tenha um documento obrigatório a ser visualizado, permitindo o mesmo registrar a visualização através de um token recebido por e-mail;
- 3.18.1.49. O sistema deverá ter bloqueio da função que permite o dispositivo se torne um ponto de hotspot (ponto específico em uma área física onde é possível acessar a internet, geralmente por meio de uma rede sem fio (wifi)), mantendo assim sua rede protegida evitando potenciais ameaças, garantindo um ambiente seguro e confiável.
- 3.18.1.50. O sistema deverá permitir o controle e gestão de patches do sistema operacional e outros produtos Microsoft gerenciáveis pelo Windows update;
- 3.18.1.51. O sistema deverá permitir configurar alertas através de configuração de identificação de um padrão de log no dispositivo, que pode ser configurado direto no painel em nuvem.
- 3.18.1.52. O sistema permitirá definir quais dispositivos serão centralizados de atualizações na rede. A partir do momento que for definido, os demais dispositivos da mesma rede, se atualização direto no centralizador;

- 3.18.1.53. O sistema permitirá efetuar agendamentos com objetivo de descoberta de novos dispositivos na rede. O agendamento poderá ser feito por dispositivo localizado em uma sub-rede e deverá mostrar a listagem de todos dispositivos que possuam ip na mesma;
- 3.18.1.54. O sistema terá um módulo de prevenção contra vazamento de dados (dlp – data loss prevention), que permitirá identificar através de scan se o dispositivo scaneado possui algum dado previamente cadastrado como alvo da prevenção através de expressão regular, permitindo que o sistema possa cadastrar novas informações usando a mesma sintaxe.
- 3.18.1.55. No caso de smartphones android, o sistema deverá prover as funcionalidades de:
- 3.18.1.56. Gerenciar os aplicativos que poderão ou não serem executados no dispositivo
- 3.18.1.57. Permitir bloqueio de determinados aplicativos por horário
- 3.18.1.58. Restringir seu funcionamento pela velocidade em km por hora, a fim de garantir segurança durante o uso e veículos
- 3.18.1.59. Configuração remota de redes wifi
- 3.18.1.60. Disponibilizar informações sobre monitoramento de memória, bateria, temperatura, localização
- 3.18.1.61. Disponibilizar informações sobre o dispositivo como sistema operacional, modelo dos dispositivos, versões, contas cadastradas e em uso, operadora, redes conectadas
- 3.18.1.62. No caso de dispositivo com sistema operacional Linux, o sistema deverá prover as funcionalidades de:
- 3.18.1.63. A solução deverá prover agente para monitoramento dos sistemas operacionais Linux prevendo ao menos o funcionamento nas versões centos 7 e 7, debian 8, 9 e 10, ubuntu 14, 16 e 18;
- 3.18.1.64. A solução deverá prover monitoramento dos agentes em Linux prevendo ao menos:
- 3.18.1.65. Ativar ou desativar recebimento de alerta dos dispositivos;
- 3.18.1.66. Verificar todos os tipos de códigos maliciosos contra os quais oferece proteção;
- 3.18.1.67. Permitir configuração de tipos de alertas, para monitoramento dos dispositivos tais como: percentuais de cpu, memória e disco e tais informações deverão estar disponíveis em um painel ou dashboard específico para monitoramento;
- 3.18.1.68. Trazer as seguintes informações de cada dispositivo: status do dispositivo, data em que os dados foram coletados, nome do host, versão do sistema operacional, usuário logado no dispositivo, consumo e total de cpu, consumo e total de memória ram, consumo e total de memória swap, consumo e volume total de disco e suas partições, interfaces de rede, serviços que estão

em execução, serviços que estão parados, processos que estão mais consumindo cpu, processos que estão mais consumindo memória, histórico de comandos executados, localização do dispositivo em mapa georreferenciado, a solução deverá permitir configurar quais serviços o agente irá monitorar e em caso de parada do serviço o agente deverá reiniciar o mesmo;

- 3.18.1.69. A solução em nuvem deverá prover modulo de monitoramento de todas as soluções acima no mesmo painel de gerenciamento com objetivo de facilitar a operação;
- 3.18.1.70. O módulo de monitoramento deverá prover painel próprio na plataforma web com atualização em tempo real do alerta bem como prover app para ser instalado em dispositivos móveis da família android;
- 3.18.1.71. Deverá disponibilizar função modo tv para facilitar a análise das informações;
- 3.18.1.72. Deverá permitir configurar frequência de envio de alertas, com no mínimo configuração de 5, 25 ou 50 minutos entre a repetição do alerta.
- 3.18.1.73. O monitoramento de endpoint e servidores, a solução deverá prover ao menos os seguintes monitores: cpu, memória e disco;
- 3.18.1.74. Se o serviço de proteção está ativo, em caso de desativar o serviço de proteção em tempo real ou serviço de proteção de navegação, para esse item deverá ser enviado um relatório informando os equipamentos com proteção desativadas ou inexistentes;
- 3.18.1.75. Alerta configurável pelo administrador entre uma range de valores para emissão de alertas entre crítico, atenção ou informativo de no mínimo cpu, memória e carga média;
- 3.18.1.76. Permitir monitorar as interfaces de rede;
- 3.18.1.77. A solução deverá permitir o monitoramento dos serviços do sistema operacional.
- 3.18.1.78. Permitir emitir alertas de uptime de um determinado website através da configuração da url, assim como certificado ssl, lista negra;

3.19. MONITOR

- 3.19.1. Deverá ser fornecido 01 (um) monitor, com as características mínimas:
 - a. O monitor deve possuir tamanho de tela de no mínimo 21.5 polegadas;
 - b. Deverá ser do tipo LED, no formato Widescreen;
 - c. Deverá possuir proporção de 16:9;
 - d. Deverá possuir ângulo de visão de no mínimo 178° horizontal e vertical;
 - e. Deve possuir brilho de no mínimo 250 cd/m²;
 - f. A taxa de contraste real mínima de 1000:1;
 - g. O tempo de resposta não deve ultrapassar 8ms;
 - h. Deve suportar resolução nativa mínima de 1920x1080 pixels a 60 Hz;
 - i. Deve possuir pelo menos 1 (uma) conexão digital, DisplayPort ou HDMI;

- j. Deve ser fornecido junto com o monitor, na mesma caixa e pelo fabricante do monitor, 1 (um) cabo DisplayPort ou HDMI para interligar o monitor ao microcomputador ofertado;
- k. Deve possuir uma entrada analógica VGA;
- l. Deve possuir fonte de alimentação interna com tensão de entrada bivolt automática;
- m. Deve possuir base com ajustes mínimos, de: inclinação, altura e rotação pivot (retrato/paisagem);
- n. O monitor deverá possuir suporte VESA compatível com o padrão de fixação oferecido pelo gabinete conforme especificado no item 3.14.2 deste termo de referência.

3.20. COMPATIBILIDADES E CERTIFICAÇÕES:

- 3.20.1. Com EPEAT em qualquer categoria, comprovada através de atestado e certidões que comprovem que o monitor ofertado é aderente ao padrão de eficiência energética EPEAT, emitido por instituo credenciado junto ao INMETRO. Será admitida como comprovação também, a indicação que o monitor consta em listagem e em status de “active” no site EPEAT através do link: <http://www.epeat.net>;
- 3.20.2. Certificação ENERGY STAR, comprovando que o monitor ofertado atinge as exigências para o melhor aproveitamento de uso de energia elétrica. Essa característica deverá ser comprovada pela listagem do monitor no site <http://www.energystar.gov>. Serão aceitas as certificações emitidas pelo INMETRO, em conformidade com as Portarias nº 170/2012 e 304/2023;
- 3.20.3. O monitor ofertado deverá possuir certificação que sua fabricação está livre de 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. LOTE 01 - ITEM 03 - NOTEBOOK

ESPECIFICAÇÕES MÍNIMAS:

4.1. PROCESSADOR

- 4.1.1. O modelo do processador ofertado deve ser de uma geração recente fornecido pelo fabricante, não sendo aceito modelos de processadores com o ano de lançamento inferior a julho de 2023 e ainda deve atender aos seguintes requisitos de desempenho e funcionalidade:
- 4.1.2. Possuir mínimo de 6 (seis) núcleos de performance e mínimo de 12 (doze) threads de processamento;

- 4.1.3. O modelo de processador oferecido deve ser capaz de suportar um conjunto de instruções de 64 bits. Além disso, ele deve ser fabricado especificamente para ser utilizado em notebooks ou dispositivos portáteis, incorporando tecnologias que visem otimização e eficiência energética.
- 4.1.4. Atingir índice de, no mínimo, 16.000 (Dezesseis mil) pontos para o desempenho, tendo como referência a base de dados Passmark CPU Mark, deverá ser anexo a esta especificação extraído do site http://www.cpubenchmark.net/cpu_list.php a partir da data da primeira publicação deste edital;
- 4.1.5. Deve ser compatível no mínimo com memória do tipo DDR5 ou superior;
- 4.1.6. Fabricado especificamente para equipamento portátil, não sendo aceito processadores para desktops.

4.2. MEMÓRIA RAM (RANDOM ACCESS MEMORY)

- 4.2.1. Deve possuir no mínimo 16 GB de memória em um único módulo;
- 4.2.2. Deve ser de no mínimo padrão DDR5 com frequência de 4800 MT/s ou superior;
- 4.2.3. Deve ser compatível com a tecnologia Dual-Channel.

4.3. PLACA MÃE:

- 4.3.1. Ser do mesmo fabricante do notebook ou projetada especificamente para o modelo de notebook ofertado, não sendo aceitas placas de livre comercialização no mercado;
- 4.3.2. A placa mãe deve possuir número de série registrado em sua BIOS, possibilitando, ainda, sua leitura de forma remota por meio de comandos DMI ou SMBIOS;
- 4.3.3. Deve possuir chip de segurança TPM (Trusted Platform Module), versão 2.0, podendo ser discreto ou soldado à placa principal;
- 4.3.4. Deve possuir suporte a expansão de memória RAM para no mínimo 64 GB;
- 4.3.5. Deve suportar a tecnologia Dual-Channel;
- 4.3.6. O chipset deverá ser do mesmo fabricante do processador ofertado, garantido total compatibilidade e funcionamento entre esses componentes.

4.4. BIOS:

- 4.4.1. Desenvolvida pelo mesmo fabricante do notebook em "Flash ROM" ou com direito de Copyright, em conformidade com a especificação "UEFI 2.7" (<http://www.uefi.org/specifications>), ou superior, e capturáveis por aplicações do tipo "UCM" (User Centric Management);
- 4.4.2. Para comprovação técnica que o BIOS atende e está em conformidade com as especificações exigidas na "UEFI" versão 2.7, ou superior, poderá ser

- comprovado através consulta ao site oficial: <http://www.uefi.org/members>, onde o fabricante do notebook ofertado deverá constar em qualquer categoria;
- 4.4.3. Possuir solução de diagnóstico capaz de ser executado (inicializado) a partir da UEFI (Unified Extensible Firmware Interface) ou do firmware do notebook através do acionamento de tecla função (F1...F12). O software de diagnóstico deverá ser capaz de fazer a verificação individual e ao mesmo tempo de todos os componentes: processador, memória, unidade de armazenamento e placa mãe;
- 4.4.4. As atualizações do BIOS deverão ser disponibilizadas no próprio site oficial do fabricante do notebook ofertado, com acesso livre (não restrito por usuário/senha);
- 4.4.5. Deverá suportar senhas, configuráveis através do BIOS, do tipo:
- a. "Power-On": senha para inicialização do notebook;
 - b. "Setup": senha para acesso e alterações de configurações;
 - c. "Hard Disk": senha para inicialização e acesso ao disco de armazenamento.
- 4.4.6. A BIOS deve ser capaz de armazenar o número de série do equipamento além de disponibilizar campo editável que permita inserir identificação customizada podendo ser consultada por software de gerenciamento, como o número de patrimônio, por exemplo;
- 4.4.7. BIOS com recursos de controle de permissão através de senhas, uma para inicializar o computador e outra para acesso e alterações das configurações do programa "setup" da BIOS;
- 4.4.8. Deve possuir solução integrada a BIOS UEFI para diagnóstico do hardware além de identificar falhas de pelo menos os seguintes itens: processador, memória, unidades de armazenamento, interface gráfica e slots PCIe;
- 4.4.9. A ferramenta deve possuir interface gráfica, sendo possível executar o diagnóstico de cada item individualmente, ou teste completo dos componentes em único comando (caso necessário detectar falhas em mais de um item);
- 4.4.10. Os códigos de erro gerados pelas falhas encontradas devem ser suficientes para indicar os problemas do equipamento na abertura do chamado técnico em garantia junto ao fabricante. Não serão aceitos softwares externos para esta aplicação;
- 4.4.11. Deve permitir atualização da BIOS em ambiente Windows x64;
- 4.4.12. As atualizações da BIOS deverão ser disponibilizadas no site do fabricante do equipamento;
- 4.4.13. BIOS desenvolvida pelo mesmo fabricante do equipamento ou via Copyright. O fabricante do computador deverá possuir livre direito de edição sobre a BIOS, garantindo assim adaptabilidade do conjunto adquirido;

4.5.INTERFACES:

- 4.5.1. Deve possuir, no mínimo, 02 (duas) portas USB 3.2 ou superior, no padrão USB-A, sendo que pelo menos 01 (uma) das interfaces deve incluir a tecnologia "On Charging Port";
- 4.5.2. Possuir, no mínimo, 01 (uma) porta USB 3.2 ou superior, no padrão USB-C, com suporte a dados, vídeo e entrega de energia, podendo ser utilizada no carregamento do equipamento;
- 4.5.3. Possuir 01 (uma) saída digital de vídeo padrão "HDMI";
- 4.5.4. Possuir 01 (uma) saída de áudio para fone de ouvido (P2 - 3.5 mm) do tipo combinada;
- 4.5.5. Possuir 01 (uma) interface para leitura biométrica digital, sendo aceito o leitor integrado ao botão liga/desliga;
- 4.5.6. Todas as interfaces citadas devem ser integradas ao notebook ofertado. Não será aceito o uso de adaptadores para atingir a quantidade de portas solicitadas.

4.6.CÂMERA:

- 4.6.1. Deve possuir 01 (uma) câmera integrada ao monitor, com resolução mínima de "720p", e ainda, com microfones integrados ao notebook para a realização de videoconferências;
- 4.6.2. Deverá ter proteção mecânica integrada que permita ao usuário tapar a lente da câmera, evitando invasão de sua privacidade em casos de ataques Hacker com captura da câmera, não sendo aceito acessório acoplado a tela ou carcaça do notebook, devendo fazer parte do projeto do chassi do equipamento ofertado.

4.7.ARMazenamento:

- 4.7.1. Deve ser entregue com (01) uma unidade de armazenamento em estado sólido (SSD) interna, com:
 - a. Capacidade mínima de 512 GB;
 - b. Padrão de conexão M.2 Card;
 - c. Padrão de barramento PCIe NVMe 3.0 ou superior.
 - d. Suporte a tecnologia S.M.A.R.T., para verificação de integridade na unidade de armazenamento.

4.8.INTERFACE DE REDE (ETHERNET):

- 4.8.1. A interface de rede Ethernet deve ser integrada à placa mãe do notebook ou disponibilizada por meio de um adaptador Ethernet conectado em porta USB-C (Tipo-C), e ainda deve:
- 4.8.2. Suportar os protocolos IEEE 802.3ab ou IEEE 802.3;
- 4.8.3. Aceitar taxa de transmissão de 1000 Mbps (1 Gbps);

- 4.8.4. Para a interface via adaptador, o mesmo deve ser compatível com a porta USB-C (Tipo-C) ou superior do notebook;
- 4.8.5. O conector RJ45 no adaptador deve incluir LEDs para indicar o status de atividade e de link da conexão.

4.9. INTERFACE REDE SEM FIO (WIRELESS):

- 4.9.1. A interface de rede sem fio deve ser integrada ou slotada em padrão M.2 Card;
- 4.9.2. Não será aceito o uso de adaptadores externos;
- 4.9.3. Deve seguir o padrão 802.11ax (Wi-Fi 6);
- 4.9.4. Deve oferecer suporte às especificações "IEEE 802.11 abgn/ax";
- 4.9.5. Suporte à tecnologia "Dual Band" operando nas frequências de 2.4GHz e 5GHz;
- 4.9.6. Capacidade de transferência de dados mínima de 1,2 Gbps;
- 4.9.7. Suporte às autenticações "WPA", "WPA2" e "802.1X";
- 4.9.8. Suporte à tecnologia "MU-MIMO 2x2" para melhorar a eficiência da rede em ambientes com múltiplos dispositivos.
- 4.9.9. Deve possuir Bluetooth, sendo no mínimo versão 5.0.
- 4.9.10. Devendo possuir certificação Wifi-Alliance e homologado junto a entidade reguladora ANATEL, devendo estar vigente e serem apresentados junto a proposta.

4.10. TELA:

- 4.10.1. Deverá possuir tela LCD ou LED com tamanho mínimo de 14" (quatorze) polegadas e máximo de 15,6" (quinze vírgula seis) polegadas e tecnologia IPS;
- 4.10.2. Deve suportar resolução mínima de "1920x1080" (mil novecentos e vinte por mil e oitenta) "pixels" a "60 Hz";
- 4.10.3. Deve possuir tecnologia "Anti-Glare" não sendo aceito película;
- 4.10.4. Deve possuir contraste mínimo de "400:1" e brilho mínimo de "300nits".

4.11. CONTROLADOR GRÁFICO INTEGRADO:

- 4.11.1. Interface com controladora de vídeo integrada ao processador com resolução mínima de 1920x1080 a 30Hz com capacidade de alocação dinâmica de memória de vídeo;
- 4.11.2. A controladora de vídeo deve suportar, nativamente, a utilização de, pelo menos 03 (três) telas simultaneamente em modo "estendido" ou "clone".

4.12. ÁUDIO:

- 4.12.1. Controladora de áudio integrada com suporte à tecnologia de "Alta Definição";
- 4.12.2. Possuir 02 (dois) autofalantes estéreos integrados, com potência mínima de "1,5 Watt" cada.

4.13. TECLADO E MOUSE:

- 4.13.1. O teclado no padrão mínimo de "six-row" (seis linhas), obrigatoriamente atendendo a norma ABNT2, com teclas e botões adicionais e configuráveis/específicos; Função Mute, Aumentar ou Diminuir Volume, por botões específicos ou combinação de tecla de funções do tipo "Fn + Key";
- 4.13.2. O notebook deverá possuir "Touch-Pad" com tecnologia "Multi-Touch" integrado ao gabinete;
- 4.13.3. O "Touch-Pad" deve permitir a função "Scroll" (função barra de rolagem) e possuir 02 (dois) botões para seleção (click);
- 4.13.4. Apresentar relevo nas teclas "F" e "J";
- 4.13.5. Possuir identificação das teclas com serigrafia a quente, ou equivalente, resistente ao apagamento por uso prolongado.

4.14. BATERIA E FONTE DE ALIMENTAÇÃO:

- 4.14.1. Deve possuir bateria de "Lítio Íon" ou "Polímero de Lítio" com capacidade mínima de "42 Wh" (quarenta e duas watts hora);
- 4.14.2. Deve possuir fonte de alimentação automática "110/220 V" (cento e dez e duzentos e vinte volts) 65W podendo usar o conector "USB Type-C" sem uso de adaptadores;
- 4.14.3. A tensão de saída da fonte deve ser compatível com a tensão de entrada suportada pelo modelo de notebook ofertado e compatível com "Fast changing technology";
- 4.14.4. A bateria deve suportar "Fast changing technology";
- 4.14.5. O adaptador de energia deve vir acompanhado de cabo de alimentação com comprimento mínimo de 1,5 (um vírgula cinco) metros e tomada no padrão "NBR 14136".

4.15. GERENCIAMENTO E SEGURANÇA:

- 4.15.1. O gabinete do modelo de notebook ofertado deverá possuir um local para fixação de trava do tipo "Security Lock" ou "Kesington Lock", será aceito ainda nas suas versões nano;
- 4.15.2. O modelo do notebook ofertado deverá possuir solução ou software do próprio fabricante que permita monitorar o sistema, realizar diagnósticos, emitir alertas, efetuar verificação e instalação das últimas atualizações do hardware do dispositivo, ajudando assim a manter a saúde e segurança do sistema.
 - 4.15.2.1. A solução deverá funcionar tanto de forma integrada, quanto de forma isolada ("stand-alone");
 - 4.15.2.2. Todos os componentes necessários à implementação desta solução corporativa deverão pertencer à mesma família de solução corporativa,

denominado neste certame como segurança de dispositivos (integrar uma única solução corporativa);

- 4.15.2.3. Todos os componentes tratados nesta descrição, deverão funcionar de forma integrada na solução. Não será aceito soluções diferentes com gestão separada;
- 4.15.2.4. A solução deverá permitir que haja troca de informações entre painel de gerenciamento e seus clientes. As informações de que trata o presente item são aqueles relevantes para a realização das ações de segurança e proteção de computadores ligados em rede, assim como monitoramento e controle.
- 4.15.2.5. A troca de informações de que trata o tópico anterior deverá permitir o recolhimento de informações sobre o estado de funcionamento da solução nas diferentes estações. As seguintes informações deverão ser contempladas, no mínimo: versão do sistema operacional, nome do host, versão do antimalware, status e informações cpu, memória, disco;
- 4.15.2.6. O acesso para ferramenta de configuração do gerenciamento em nuvem (plataforma) deverá ser com acesso seguro via https, com possibilidade de uso de duplo fator de autenticação.
- 4.15.2.7. Ter possibilidade de através de uma senha administrativa, desabilitar algumas funções do sistema de proteção local de estação ou servidor da família Windows;
- 4.15.2.8. A solução deverá permitir trabalhar obrigatoriamente na língua portuguesa do brasil e inglês;
- 4.15.2.9. A plataforma de gerenciamento em nuvem permitirá efetuar configurações e criação de políticas por grupos ou territórios em uma hierarquia do tipo árvore, selecionando qual grupo de dispositivos pertencente à que território aquela política se aplica.
- 4.15.2.10. A plataforma de gerenciamento em nuvem permitirá gerência granular de políticas, por nível hierárquico, permitindo usuário configurar políticas seguindo uma ordem de hierarquia determinada por grupos ou conjunto de computadores, sendo possível permitir a configuração de políticas como dominantes, ou seja, que não podem ser reescritas por políticas em nível hierárquico mais baixo;
- 4.15.2.11. A ferramenta deverá prover gerência de acesso para usuários de administração com vários níveis de permissão configuráveis pelo administrador principal.
- 4.15.2.12. Com relação ao sistema específico da família Microsoft Windows, o sistema deverá no mínimo ter as seguintes funcionalidades:
- 4.15.2.13. Suportar todas as funcionalidades nos sistemas Windows 10 e 11 e Windows server 2016/2019/2022

- 4.15.2.14. Verificar todos os tipos de códigos maliciosos contra os quais oferece proteção e realizar as tarefas de proteção de computadores ligados em rede em tempo real;
- 4.15.2.15. Permitir definir regras de funcionamento dos bloqueios comportamentais do antivírus, com no mínimo configuração do tipo de alerta, se o usuário será notificado para tomar uma ação, se o usuário será notificado e a ação será automática ou função silêncio onde a ação é tomada e o usuário não é notificado;
- 4.15.2.16. Permitir visualizar tempo de uso de cada aplicação e software filtrado pelo nome do usuário;
- 4.15.2.17. O console de gerenciamento web deverá prover na tela principal um dashboard com no mínimo informações sobre o percentual de máquina com número de antivírus/antimalware instalado e ameaças neutralizadas;
- 4.15.2.18. A solução deverá prover dashboard detalhado do gerenciamento do antimalware, do monitoramento e do inventário da rede com no mínimo as seguintes informações: estatísticas sobre ameaças identificadas, ameaças em quarentena, estatística de aplicação de licenças, informações quanto aos dispositivos ligados, desligados, informações sobre monitoramento de servidores, informações de monitoramento de banco de dados sqlserver, mysql, postgresql, oracle, monitoramento do serviço do Microsoft active directory e dns, informações quanto aos sistemas operacionais instalados, versão do sistema operacional, informações quanto ao número de máquinas com licença ativa do Windows bem como licenças não válidas, vencidas ou sem licença além de resumo dos 10 maiores fornecedores de software;
- 4.15.2.19. Ter painel de visualização que permita verificar através de cores e com informações básicas quais dispositivos estão com problemas, quais estão com alertas e quais estão com execução sem nenhum problema, identificando os que são ou não servidores;
- 4.15.2.20. A solução deverá prover relatórios referente as informações extraídas dos dispositivos, no mínimo deverá conter relatórios de inventário de software e hardware, relatório contendo equipamento e licença do Windows e seu status, informações da existência de algum software virtualizado instalado em algum dispositivo, relatório licença do antimalware e suas aplicações, relatório de infecções equipamento infectados, nome da infecção e nível de risco da mesma.
- 4.15.2.21. A solução deverá trazer informações sobre sistemas operacionais descontinuados, informando qual o sistema operacional bem como o equipamento que apresenta a condição;
- 4.15.2.22. Fornecer proteção, no mínimo, contra os seguintes tipos de códigos maliciosos: vírus de computador (em todas as suas variações), bombas lógicas, vermes ("worms"), cavalos de tróia ("trojan"), códigos espiões ("spyware",

- “keylogger”, “screenlogger”, etc), códigos de apoio à invasão e escalada de privilégio (“rootkit”, “backdoor”, etc), código e conteúdo indesejado (“dialer”, “adware”, “joke”, etc);
- 4.15.2.23. Deverá ter a possibilidade de rastreamento manual nas estações de trabalho (programada ou não) de dispositivos móveis de armazenamento (ou não) e mídias removíveis ou quaisquer outros que permitam a transferência de arquivos para a estação de trabalho;
- 4.15.2.24. Deverá negar acesso ao arquivo infectado antes que o mesmo seja carregado em memória, aberto e/ou executado. Após negar o acesso ao arquivo infectado o antimalware deverá limpar o arquivo, e/ou apagar o arquivo infectado e enviar o arquivo infectado para uma área de segurança (quarentena);
- 4.15.2.25. Permitir detecção de ameaças em arquivos compactados nos principais algoritmos (“zip”, “rar”, “7zip”)
- 4.15.2.26. A proteção de tempo real deverá trabalhar também com listas brancas (whitelist) permitindo adicionar um arquivo em específico ou um diretório, permitindo assim todos os arquivos de serem executados e recursivamente.
- 4.15.2.27. Permitir a execução de escaneamentos nos servidores e nas estações de trabalho (programada ou não).
- 4.15.2.28. Possuir camada de proteção contra acesso a sites fraudulentos e perigosos;
- 4.15.2.29. Possuir camada de proteção de arquivos contra sequestro de informações;
- 4.15.2.30. Possuir camada de proteção comportamental contra programas e/ou comportamentos suspeitos;
- 4.15.2.31. Ter módulo de histórico com uma lista de ações executadas pelo sistema antivírus/antimalware;
- 4.15.2.32. Permitir gerar “kit de emergência” que permitirá usuário dar boot na máquina e efetuar limpeza manual;
- 4.15.2.33. Possuir módulo de bloqueio por meio de comportamento dos processos, sistemas e programas;
- 4.15.2.34. A solução deverá proteger os arquivos através de análise comportamental, ou seja, proteger arquivos mesmo que a solução não disponha de assinatura para esse artefato, permitindo também a inclusão de arquivos na lista branca ou negra para análise comportamental de arquivos, inclusão de um arquivo somente para monitoramento bem como definir um arquivo ou aplicação que deverá ser bloqueada, permitindo configurar se tal ação será ou não notificada ao usuário, sendo que essa notificação ao usuário deverá ser em português do Brasil.
- 4.15.2.35. Além dos componentes responsáveis pelo combate a códigos maliciosos, possuir também componente responsável por implementar uma

camada de proteção para acesso a internet que impeça abertura de sites com risco de acesso a conteúdos maliciosos;

- 4.15.2.36. Permitir a inclusão de arquivos na lista branca ou negra para com base em assinaturas, inclusão de um arquivo somente para monitoramento bem como definir um arquivo ou aplicação que deverá ser bloqueada, permitindo configurar se tal ação será ou não notificada ao usuário, sendo que essa notificação ao usuário deverá ser em português do Brasil, para esse item deverá permitir ativação ou não de proteção quanto pup do acronico em inglês possible unintended programs, ou seja, programas possivelmente indesejados como exemplos adwares e spywares;
- 4.15.2.37. A solução deverá prover proteção quanto a navegação, para essa função a solução deverá funcionar sem a necessidade de instalação de outro agente ou plugins nos navegadores;
- 4.15.2.38. Para a proteção de navegação a solução deverá permitir no mínimo proteção quanto sites maliciosos com base própria, sites com conteúdo indesejados (pup - possible unintended programs), bem como permitir a inclusão manual pelo administrador de sites na lista branca bem como na lista negra;
- 4.15.2.39. A solução deverá permitir agendamento de scan no dispositivo, podendo criar mais do que umas regras de agendamento separado entre rápido e completo, determinando dia e horário assim como a frequência;
- 4.15.2.40. A solução deverá permitir executar comandos e scripts remotos na estação, deverá permitir no mínimo acionar desinstalação de um software instalado, desinstalar ou instalar o antimalware, reiniciar dispositivo, desligar dispositivo, bloquear o dispositivo com possibilidade de desbloqueio através de uma senha específica.
- 4.15.2.41. Trazer a localização georreferenciada do dispositivo de maneira automática ou permitir configurar de maneira manual a latitude e longitude para localização do dispositivo;
- 4.15.2.42. Permitir acessar remotamente o equipamento direto do painel cloud, a solução permitirá o acesso através de solicitação ou diretamente sem solicitação de autorização;
- 4.15.2.43. Permitir configuração de tipos de alertas, para monitoramento dos dispositivos tais como: percentuais de CPU, memória e disco e tais informações deverão estar disponíveis em um painel ou dashboard específico para monitoramento;
- 4.15.2.44. O sistema deverá trazer no mínimo as seguintes informações de cada dispositivo: status do dispositivo, data em que os dados foram coletados, o número da licença do sistema operacional Windows bem como o status da licença daquele dispositivo, nome do host, versão do antivírus/antimalware, versão do sistema operacional, usuário logado no dispositivo, tempo de

atividade, consumo e total de cpu, consumo e total de memória ram, consumo e total de memória swap, consumo e volume total de disco, interfaces de rede, serviços que estão em execução, serviços que estão parados, processos que estão mais consumindo cpu, processos que estão mais consumindo memória, informações de hardware, tais como: drivers de impressora, cd-rom, dispositivos gerais, ide, usb, som, vídeo, adaptador de rede, processador, bios, memória, placa de som, disco, memória, informações dos softwares instalados, tais como: fabricantes, software e versão;

- 4.15.2.45. O sistema deverá permitir monitoramento por meio de protocolo snmp de qualquer dispositivo conectado na rede, através da definição de qual dispositivo será o coletor dos dados e o mesmo centralizar as informações mostrando na plataforma
- 4.15.2.46. A plataforma deverá permitir ligar os dispositivos através do recurso wake-on-lan, caso o dispositivo possua este recurso e esteja ativada na bios;
- 4.15.2.47. O sistema deverá ter funcionalidade de proteção contra gravação de tela e printscreen através da inserção automática de marcas d'água ao realizar capturas de tela ou gravações de vídeo;
- 4.15.2.48. O sistema deverá ter recurso de visualização de documentos, através do endpoint, alertando o usuário caso tenha um documento obrigatório a ser visualizado, permitindo o mesmo registrar a visualização através de um token recebido por e-mail;
- 4.15.2.49. O sistema deverá ter bloqueio da função que permite o dispositivo se torne um ponto de hotspot (ponto específico em uma área física onde é possível acessar a internet, geralmente por meio de uma rede sem fio (wifi)), mantendo assim sua rede protegida evitando potenciais ameaças, garantindo um ambiente seguro e confiável.
- 4.15.2.50. O sistema deverá permitir o controle e gestão de patches do sistema operacional e outros produtos Microsoft gerenciáveis pelo Windows update;
- 4.15.2.51. O sistema deverá permitir configurar alertas através de configuração de identificação de um padrão de log no dispositivo, que pode ser configurado direto no painel em nuvem.
- 4.15.2.52. O sistema permitirá definir quais dispositivos serão centralizados de atualizações na rede. A partir do momento que for definido, os demais dispositivos da mesma rede, se atualização direto no centralizador;
- 4.15.2.53. O sistema permitirá efetuar agendamentos com objetivo de descoberta de novos dispositivos na rede. O agendamento poderá ser feito por dispositivo localizado em uma sub-rede e deverá mostrar a listagem de todos dispositivos que possuam ip na mesma;
- 4.15.2.54. O sistema terá um módulo de prevenção contra vazamento de dados (dlp – data loss prevention), que permitirá identificar através de scan se o dispositivo scaneado possui algum dado previamente cadastrado como alvo da

prevenção através de expressão regular, permitindo que o sistema possa cadastrar novas informações usando a mesma sintaxe.

- 4.15.2.55. No caso de smartphones android, o sistema deverá prover as funcionalidades de:
- 4.15.2.56. Gerenciar os aplicativos que poderão ou não serem executados no dispositivo
- 4.15.2.57. Permitir bloqueio de determinados aplicativos por horário
- 4.15.2.58. Restringir seu funcionamento pela velocidade em km por hora, a fim de garantir segurança durante o uso e veículos
- 4.15.2.59. Configuração remota de redes wifi
- 4.15.2.60. Disponibilizar informações sobre monitoramento de memória, bateria, temperatura, localização
- 4.15.2.61. Disponibilizar informações sobre o dispositivo como sistema operacional, modelo dos dispositivos, versões, contas cadastradas e em uso, operadora, redes conectadas
- 4.15.2.62. No caso de dispositivo com sistema operacional Linux, o sistema deverá prover as funcionalidades de:
- 4.15.2.63. A solução deverá prover agente para monitoramento dos sistemas operacionais Linux prevendo ao menos o funcionamento nas versões centos 7 e 7, debian 8, 9 e 10, ubuntu 14, 16 e 18;
- 4.15.2.64. A solução deverá prover monitoramento dos agentes em Linux prevendo ao menos:
- 4.15.2.65. Ativar ou desativar recebimento de alerta dos dispositivos;
- 4.15.2.66. Verificar todos os tipos de códigos maliciosos contra os quais oferece proteção;
- 4.15.2.67. Permitir configuração de tipos de alertas, para monitoramento dos dispositivos tais como: percentuais de cpu, memória e disco e tais informações deverão estar disponíveis em um painel ou dashboard específico para monitoramento;
- 4.15.2.68. Trazer as seguintes informações de cada dispositivo: status do dispositivo, data em que os dados foram coletados, nome do host, versão do sistema operacional, usuário logado no dispositivo, consumo e total de cpu, consumo e total de memória ram, consumo e total de memória swap, consumo e volume total de disco e suas partições, interfaces de rede, serviços que estão em execução, serviços que estão parados, processos que estão mais consumindo cpu, processos que estão mais consumindo memória, histórico de comandos executados, localização do dispositivo em mapa georreferenciado, a solução deverá permitir configurar quais serviços o agente irá monitorar e em caso de parada do serviço o agente deverá reiniciar o mesmo;

- 4.15.2.69. A solução em nuvem deverá prover modulo de monitoramento de todas as soluções acima no mesmo painel de gerenciamento com objetivo de facilitar a operação;
- 4.15.2.70. O módulo de monitoramento deverá prover painel próprio na plataforma web com atualização em tempo real do alerta bem como prover app para ser instalado em dispositivos móveis da família android;
- 4.15.2.71. Deverá disponibilizar função modo tv para facilitar a análise das informações;
- 4.15.2.72. Deverá permitir configurar frequência de envio de alertas, com no mínimo configuração de 5, 25 ou 50 minutos entre a repetição do alerta.
- 4.15.2.73. O monitoramento de endpoint e servidores, a solução deverá prover ao menos os seguintes monitores: cpu, memória e disco;
- 4.15.2.74. Se o serviço de proteção está ativo, em caso de desativar o serviço de proteção em tempo real ou serviço de proteção de navegação, para esse item deverá ser enviado um relatório informando os equipamentos com proteção desativadas ou inexistentes;
- 4.15.2.75. Alerta configurável pelo administrador entre uma range de valores para emissão de alertas entre crítico, atenção ou informativo de no mínimo cpu, memória e carga média;
- 4.15.2.76. Permitir monitorar as interfaces de rede;
- 4.15.2.77. A solução deverá permitir o monitoramento dos serviços do sistema operacional.
- 4.15.2.78. Permitir emitir alertas de uptime de um determinado website através da configuração da url, assim como certificado ssl, lista negra;

4.16. SISTEMA OPERACIONAL:

- 4.16.1. O notebook deverá vir com o Microsoft Windows 11 Professional, em sua versão 64 bits, e em Português do Brasil;
- 4.16.2. O licenciamento do sistema operacional deverá ser fornecido pelo fabricante do notebook ofertado, em regime OEM, onde, por questões de segurança a chave de ativação deverá ser embarcada no próprio BIOS do notebook, o qual deverá ser consultada no processo ativação desta licença;
- 4.16.3. O fabricante deve disponibilizar download gratuito de todos os drivers de dispositivos do equipamento ofertado, na versão mais atual para download.

4.17. CERTIFICAÇÕES:

- 4.17.1. Compatibilidade com EPEAT em qualquer comprovada através de atestado e certidões que comprovem que o notebook ofertado é aderente ao padrão de eficiência energética EPEAT “Nacional ou Internacional”, emitido por instituo credenciado junto ao INMETRO. Será admitida como comprovação também,

- a indicação que o notebook conste em listagem e em status de "active" no site EPEAT através do link: <http://www.epeat.net>;
- 4.17.2. Deverá ser apresentada certificação ou documento que comprove compatibilidade do modelo de notebook ofertado com a norma "IEC 60950" ou equivalente emitida pelo "INMETRO";
- 4.17.3. O modelo de notebook ofertado deverá possuir certificação que sua fabricação está livre de 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), podendo ser comprovados através de relatório de conformidade ambiental por certificado "EPEAT RoHS Criteria" (<http://www.epeat.net/>);
- 4.17.4. O modelo de notebook ofertado deverá constar no "Microsoft Windows HCL". A comprovação da compatibilidade será efetuada através de apresentação do documento "Hardware Compatibility Test Report" emitido especificamente para a versão do sistema operacional que o acompanha;
- 4.17.5. O fabricante do notebook ofertado deverá obrigatoriamente constar na lista de produtos habilitados para o padrão "DMI 2.0", ou superior, como "Board" ou "Leadership", o que será conferido por meio de acesso ao site da "DMTF - Distributed Management Task Force", no endereço: <http://www.dmtf.org>;
- 4.17.6. O fabricante do notebook ofertado deve possuir sistema de gestão ambiental com base na norma "ISO 14001", devidamente comprovado através do respectivo certificado;
- 4.17.7. O notebook ofertado deverá ter laudo de teste para impactos, umidade, vibração, poeira e alta temperatura emitido pelo fabricante do produto ou equivalente INMETRO;
- 4.17.8. O equipamento deve pertencer à linha corporativa do fabricante, não sendo aceitos dispositivos destinados ao uso doméstico, e ainda deve ser novo, de primeiro uso e em linha de fabricação recente.

4.18. ESPECIFICAÇÕES FÍSICAS:

- 4.18.1. Deve possuir peso máximo de até "1,50 Kg" (um quilo vírgula quinhentas gramas) incluindo a bateria;
- 4.18.2. O gabinete do notebook deverá ser composto por alumínio ou titânio ou magnésio ou carbono, ou PC/ABS ou superior sendo aceito quaisquer destes combinados entre si ou todo de um só tipo dos citados, em cor sóbria de uso corporativo, isto é, sem efeitos de transparência e cores além dos tons tradicionais de preto, grafite ou prata;
- 4.18.3. Todos os notebooks a serem entregues deverão ser idênticos, ou seja, todos os componentes externos e internos de mesmo modelo e marca, conforme informado na Proposta Comercial. Caso o componente não mais se encontre

disponível no mercado, admitem-se substitutos com qualidade e características idênticas ou superiores, mediante declaração técnica.

4.19. MALETA OU MOCHILA PARA TRANSPORTE

- 4.19.1. Deverá ser fornecida 01 (uma) Mochila ou Maleta para o transporte do notebook com segurança;
- 4.19.2. Deverá ser da mesma marca do fabricante do notebook ofertado.

5. LOTE 01 – ITEM 04 - WORKSTATION

ESPECIFICAÇÕES MÍNIMAS:

5.1. PROCESSADOR:

- 5.1.1. O modelo do processador ofertado deve ser de uma geração recente fornecido pelo fabricante, não sendo aceito modelos de processadores com o ano de lançamento inferior a julho de 2024 e ainda deve atender aos seguintes requisitos de desempenho e funcionalidade:
 - a. Mínimo de 16 (dezesesseis) núcleos e 24 (vinte e quatro) threads de processamento;
 - b. Atender a um índice mínimo de 55.000 (cinquenta e cinco mil) pontos de desempenho, conforme a base de dados Passmark CPU Mark. Este requisito deve ser comprovado por meio de um anexo extraído do site http://www.cpubenchmark.net/cpu_list.php, datado a partir da publicação inicial deste edital.
 - c. Deve ser compatível com memória DDR5 com taxa de transferência mínima de 4400MT/s;
 - d. Permitir acesso e gerenciamento remoto via hardware, através de conexão TCP/IP, à interface gráfica do equipamento (tela) com acesso e controle do teclado, independente do estado, tipo e versão do sistema operacional instalado, permitindo ainda, ligar e desligar o mesmo remotamente, assim como, o acesso e controle remoto da BIOS e as visualização das telas de POST;
 - e. Projetado e fabricado, visando melhor eficiência energética, com litografia máxima 14nm, para melhor dissipação de calor.

5.2. MEMÓRIA RAM (RANDOM ACCESS MEMORY)

- 5.2.1. Deve possuir no mínimo 64 GB de memória;
- 5.2.2. Deve ser de no mínimo padrão DDR5 com frequência de 4800 MT/s ou superior;
- 5.2.3. Deve ser compatível com a tecnologia Dual-Channel;
- 5.2.4. Deverá ser do tipo ECC (Error-Correcting Code).

5.3. PLACA MÃE

- 5.3.1. Ser do mesmo fabricante do microcomputador ou projetada especificamente para o modelo de microcomputador ofertado, não sendo aceitas placas de livre comercialização no mercado;
- 5.3.2. Chip de segurança TPM (Trusted Platform Module), versão 2.0, podendo ser discreto ou soldado à placa principal;
- 5.3.3. Suportar boot por pendrive ou disco conectado a uma porta USB;
- 5.3.4. Deve possuir suporte a expansão de memória mínima para 128GB (128 gigabytes);
- 5.3.5. Deve suportar e estar configurada com a tecnologia Dual-Channel;
- 5.3.6. Deve possuir 2 (dois) Slots de memória livres ao final da configuração;
- 5.3.7. Deve suportar a controladora de disco padrão SATA III (6.0 Gb/s);
- 5.3.8. Deve suportar ao padrão S.M.A.R.T.

5.4. BIOS

- 5.4.1. Desenvolvida pelo mesmo fabricante do workstation em Flash ROM ou com direito de Copyright, em conformidade com a especificação UEFI 2.7 (<http://www.uefi.org/specifications>), ou superior, e capturáveis por aplicações do tipo UCM (User Centric Management);
- 5.4.2. Para comprovação técnica que o BIOS atende e está em conformidade com as especificações exigidas na UEFI versão 2.7, ou superior, poderá ser comprovado através consulta ao site oficial: <http://www.uefi.org/members>, onde o fabricante do equipamento ofertado deverá constar nas categorias "PROMOTER" ou "CONTRIBUTOR";
- 5.4.3. Deverá possuir capacidade de habilitar/desabilitar as interfaces USB;
- 5.4.4. Deverá suportar senhas, configuráveis através do BIOS, do tipo:
 - a. Power-On: senha para inicialização do workstation;
 - b. Setup: senha para acesso e alterações de configurações;
 - c. Hard Disk: senha para inicialização e acesso ao disco de armazenamento.
- 5.4.5. Possuir solução de diagnóstico capaz de ser executado (inicializado) a partir da UEFI (Unified Extensible Firmware Interface) ou do firmware do workstation através do acionamento de tecla função (F1...F12). O software de diagnóstico deverá ser capaz de fazer a verificação individual e ao mesmo tempo de todos os componentes: processador, memória, unidade de armazenamento e placa mãe.

5.5. CHIPSET

- 5.5.1. Deverá ser do mesmo fabricante do processador ofertado, para melhor compatibilidade.

5.6. SLOTS E INTERFACES

- 5.6.1. O workstation ofertado deve possuir 02 (dois) slot PCI Express livre ao final da configuração solicitada, sendo PCIe 3.0 ou superior;
- 5.6.2. Possuir, no mínimo, 08 (oito) portas USB 3.2 Gen 1 ou superior, sendo:
 - a. Pelo menos 02 (duas) portas USB 3.2, no padrão USB-A na parte frontal do gabinete;
 - b. Pelo menos 04 (quatro) portas USB 3.2, no padrão USB-A na parte frontal do gabinete;
 - c. Pelo menos 01 (uma) porta USB 3.2, no padrão USB-C na parte frontal do gabinete;
- 5.6.3. Possuir as seguintes saídas de vídeo:
 - a. No mínimo, 01 (uma) saída digital no padrão HDMI;
 - b. No mínimo, 02 (duas) saídas digitais no padrão DisplayPort.
- 5.6.4. Possuir slot PCIe 3.0 ou superior, desde que seja compatível com a placa de vídeo solicitada item 5.7;
- 5.6.5. Todas as interfaces citadas devem ser integradas ao workstation ofertado. Não será aceito o uso de adaptadores para atingir a quantidade de portas solicitadas.

5.7. PLACA GRÁFICA

- 5.7.1. Deve possuir interface com controladora de vídeo dedicada com resolução mínima de "5.120x2.880" pixels 60Hz com no mínimo 12 GB de memória de vídeo dedicadas do tipo GDDR6 e ainda;
- 5.7.2. Trabalhar com no mínimo 128 bits de interface de memória;
- 5.7.3. Possuir velocidade de largura de banda da memória mínima de 160GB/s, com 890 CUDA cores;
- 5.7.4. A interface de vídeo off-board deverá constar da lista de "Graphics Hardware Certified" para utilização do software para ilustração geométrica AutoCAD 2022, disponível através de consulta, pelo link: <http://usa.autodesk.com/adsk/servlet/syscert?siteID=123112&id=18844534>.
- 5.7.5. Possuir no mínimo 4 (quatro) interfaces DisplayPort ou Mini DisplayPort;
- 5.7.6. Deverá possuir compatibilidade com a tecnologia Shader Model 5.17, Vulkan 1.2, DirectX 12 e OpenGL 4.68;
- 5.7.7. Deverá possuir certificado ISV, e ainda ter disponível via site do próprio fabricante;
- 5.7.8. Capacidade de alcançar até 2,5 TFLOPs de desempenho.
- 5.7.9. Devem ser fornecidos junto ao equipamento dois (2) adaptadores de DisplayPort para HDMI ou dois (2) adaptadores de Mini DisplayPort para HDMI. OBS: Serão aceito adaptadores de livre circulação no mercado, desde que atendam aos padrões exigidos, garantam a plena funcionalidade da solução e estejam incluídos na garantia da Workstation.

5.8. ÁUDIO

- 5.8.1. Controladora de áudio integrada com suporte à tecnologia de Alta Definição;
- 5.8.2. Com conectores Line Out, Mic frontais integrado ao workstation ofertado;

5.9. INTERFACES DE REDE

- 5.9.1. Interface de rede integrada padrão Gigabit Ethernet (IEEE 802.3) com:
- 5.9.2. Taxa de transmissão 10/100/1000 Mbps;
- 5.9.3. Deverá possuir compatibilidade com a tecnologia WoL (Wake on Lan);
- 5.9.4. Conector RJ-45 fêmea integrado à placa mãe.
- 5.9.5. Interface de rede Wireless (sem fio) padrão IEEE 802.11ax com a configuração:
- 5.9.6. Suporte as especificações IEEE 802.11 abgn;
- 5.9.7. Suporte à tecnologia Dual Band de 2.4GHz e 5GHz;
- 5.9.8. Suporte a transferência de dados mínima de 2.4 Gbps;
- 5.9.9. Suporte as autenticações WPA, WPA2 e 802.1X;
- 5.9.10. MU-MIMO 2x2;
- 5.9.11. Deve ser homologada e fornecida pelo mesmo fabricante do modelo de microcomputador ofertado.
- 5.9.12. Todas as interfaces citadas devem ser integradas ao workstation ofertado, ou slotadas em padrão M2. Card, não aceito uso de adaptadores para atingir a quantidade de interfaces solicitadas.

5.10. CONTROLADORA DE DISCO RÍGIDO E ÓPTICO

- 5.10.1. Deverá possuir 01 (uma) controladora de unidade de disco integrada a placa mãe, com no mínimo 03 (três) canais Serial ATA 6.0Gb/s;

5.11. ARMAZENAMENTO

- 5.11.1. Entregue com (01) uma unidade de armazenamento em estado sólido (SSD) interna, com:
- 5.11.2. Capacidade mínima de 1 TB;
- 5.11.3. Padrão de conexão M.2 Card;
- 5.11.4. Padrão de barramento PCIe NVMe;
- 5.11.5. Tecnologia S.M.A.R.T., para detecção de pré-falhas do disco rígido.
- 5.11.6. Possuir (01) uma unidade de disco rígido de no mínimo 2TB, com:
- 5.11.7. Padrão Serial ATA 6.0Gb/s;
- 5.11.8. Velocidade de Rotação de 7.200 rpm;
- 5.11.9. Cache de no mínimo 16 MB;
- 5.11.10. Tecnologia S.M.A.R.T., para detecção de pré-falhas do disco rígido.
- 5.11.11.

5.12. TECLADO

- 5.12.1. Teclado alfanumérico, ABNT II com 107 teclas;
- 5.12.2. Possuir bloco numérico separado das demais teclas;
- 5.12.3. Apresentar relevo nas teclas "F" e "J" do teclado alfanumérico e na tecla "5" do bloco numérico;
- 5.12.4. Possuir leds com indicação de "Numlock" e "CapsLock", e base com regulagem de inclinação;
- 5.12.5. Possuir identificação das teclas com serigrafia a quente, ou equivalente, resistente ao apagamento por uso prolongado, bem como ser resistente ao derramamento de líquidos;
- 5.12.6. Conector tipo USB, com conector compatível com o microcomputador ofertado, sem utilização de adaptador.

5.13. MOUSE

- 5.13.1. Mouse tipo óptico;
- 5.13.2. Resolução mínima de 1000 dpi;
- 5.13.3. Possuir 02 (dois) botões para seleção "click" e 01 (um) botão de rolagem "scroll";
- 5.13.4. Possuir processo de construção para utilização ambidestra;
- 5.13.5. Conector tipo USB, com conector compatível com o microcomputador ofertado, sem utilização de adaptador.

5.14. GABINETE E FONTE DE ALIMENTAÇÃO

- 5.14.1. O gabinete deverá ser do tipo Tower Form Factor (Torre) com volume mínimo de 20.000 cm³ e máximo de 27.639 cm³, e com índice de eficiência comprovado através de apresentação de documento emitidos pelo IT ECO Declarations, ou equivalente, que conste compatibilidade do workstation ofertado com a ISO 9296, ou equivalente emitido pelo INMETRO;
- 5.14.2. O gabinete deverá possuir botão liga/desliga, luzes de indicação de atividade da unidade de disco rígido e de status ligado (power-on);
- 5.14.3. O gabinete deve permitir a abertura e troca dos componentes do workstation (placas de expansão, pentes de memória, disco rígido e M.2) sem necessidade de ferramentas (Tool Less), será aceito o uso de parafusos recartilhado para a abertura da tampa do gabinete;
- 5.14.4. Possuir fonte de alimentação para corrente alternada com tensões de entrada de 100 a 240 VAC [+/-10%], 50-60Hz com ajuste automático, com potência mínima de 500w e máxima de 900W e fator de eficiência igual ou superior a 92%; e ainda:
- 5.14.5. O modelo de fonte de alimentação ofertado deverá possuir certificação mínima 80PLUS Platinum, comprovado através de consulta ou certificado

emitido pelo site
<https://www.plugloadsolutions.com/80PlusPowerSupplies.aspx>.

5.14.6. Possuir sensor de intrusão;

5.14.7. Possuir baixo nível de ruído conforme NBR 10.152, ISO 9296 e ISO 7779, ou equivalentes.

5.15. SISTEMA OPERACIONAL

5.15.1. O microcomputador deverá vir com o Microsoft Windows 11 Professional pré-instalado sua versão 64 bits, e em Português do Brasil;

5.15.2. O licenciamento do sistema operacional deverá ser fornecido pelo fabricante do workstation ofertado, em regime OEM, onde, por questões de segurança a chave de ativação deverá ser embarcada no próprio BIOS do workstation, o qual deverá ser consultada no processo ativação desta licença.

5.16. COMPATIBILIDADE

5.16.1. Compatibilidade com EPEAT em qualquer categoria, comprovada através de atestado e certidões que comprovem que o workstation ofertado é aderente ao padrão de eficiência energética EPEAT, emitido por instituo credenciado junto ao INMETRO. Será admitida como comprovação também, a indicação que o workstation conste em listagem e em status de "active" no site EPEAT através do link: <http://www.epeat.net>;

5.16.2. Apresentar certificação ou documento para o modelo de workstation ofertado que comprove compatibilidade com a norma IEC 60950, ou equivalente emitida pelo INMETRO;

5.16.3. O modelo de workstation ofertado deverá possuir certificação que sua fabricação está livre de 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), podendo ser comprovados através de relatório de conformidade ambiental por certificado EPEAT RoHS Criteria (<http://www.epeat.net/>);

5.16.4. O modelo de workstation ofertado deverá constar no Microsoft Windows HCL. A comprovação da compatibilidade será efetuada através de apresentação do documento Hardware Compatibility Test Report emitido especificamente para a versão do sistema operacional que o acompanha;

5.16.5. O fabricante do workstation ofertado deverá obrigatoriamente constar na lista de produtos habilitados para o padrão DMI 2.0, ou superior, como Board ou Leadership o que será conferido por meio de acesso ao site da DMTF (Distributed Management Task Force), no endereço: <http://www.dmtf.org>;

- 5.16.6. O fabricante do workstation ofertado deve possuir sistema de gestão ambiental com base na norma ISO 14001, devidamente comprovado através do respectivo certificado.

5.17. DIVERSOS

- 5.17.1. Todos os equipamentos (workstation e acessórios) a serem entregues deverão ser idênticos, ou seja, todos os componentes externos e internos de mesmos modelos e marca conforme informados na Proposta Comercial. Caso o componente não mais se encontra disponível no mercado, admitem-se substitutos com qualidade e características idênticas ou superiores, mediante declaração técnica;
- 5.17.2. Componentes como teclado e mouse devem ser do mesmo fabricante do workstation ou fabricados em regime de OEM com certificado ou declaração para os mesmos.

5.18. SISTEMA DE GERENCIAMENTO E SEGURANÇA

- 5.18.1. O workstation deverá possuir solução ou software do próprio fabricante que permita monitorar o sistema, realizar diagnósticos, emitir alertas e ajudar a reparar erros do sistema, ajudando assim a manter a saúde e segurança do sistema;
- 5.18.1.1. A solução deverá funcionar tanto de forma integrada, quanto de forma isolada ("stand-alone");
- 5.18.1.2. Todos os componentes necessários à implementação desta solução corporativa deverão pertencer à mesma família de solução corporativa, denominado neste certame como segurança de dispositivos (integrar uma única solução corporativa);
- 5.18.1.3. Todos os componentes tratados nesta descrição, deverão funcionar de forma integrada na solução. Não será aceito soluções diferentes com gestão separada;
- 5.18.1.4. A solução deverá permitir que haja troca de informações entre painel de gerenciamento e seus clientes. As informações de que trata o presente item são aqueles relevantes para a realização das ações de segurança e proteção de computadores ligados em rede, assim como monitoramento e controle.
- 5.18.1.5. A troca de informações de que trata o tópico anterior deverá permitir o recolhimento de informações sobre o estado de funcionamento da solução nas diferentes estações. As seguintes informações deverão ser contempladas, no mínimo: versão do sistema operacional, nome do host, versão do antimalware, status e informações cpu, memória, disco;
- 5.18.1.6. O acesso para ferramenta de configuração do gerenciamento em nuvem (plataforma) deverá ser com acesso seguro via https, com possibilidade de uso de duplo fator de autenticação.

- 5.18.1.7. Ter possibilidade de através de uma senha administrativa, desabilitar algumas funções do sistema de proteção local de estação ou servidor da família Windows;
- 5.18.1.8. A solução deverá permitir trabalhar obrigatoriamente na língua portuguesa do brasil e inglês;
- 5.18.1.9. A plataforma de gerenciamento em nuvem permitirá efetuar configurações e criação de políticas por grupos ou territórios em uma hierarquia do tipo árvore, selecionando qual grupo de dispositivos pertencente à que território aquela política se aplica.
- 5.18.1.10. A plataforma de gerenciamento em nuvem permitirá gerência granular de políticas, por nível hierárquico, permitindo usuário configurar políticas seguindo uma ordem de hierarquia determinada por grupos ou conjunto de computadores, sendo possível permitir a configuração de políticas como dominantes, ou seja, que não podem ser reescritas por políticas em nível hierárquico mais baixo;
- 5.18.1.11. A ferramenta deverá prover gerência de acesso para usuários de administração com vários níveis de permissão configuráveis pelo administrador principal.
- 5.18.1.12. Com relação ao sistema específico da família Microsoft Windows, o sistema deverá no mínimo ter as seguintes funcionalidades:
- 5.18.1.13. Suportar todas as funcionalidades nos sistemas Windows 10 e 11 e Windows server 2016/2019/2022
- 5.18.1.14. Verificar todos os tipos de códigos maliciosos contra os quais oferece proteção e realizar as tarefas de proteção de computadores ligados em rede em tempo real;
- 5.18.1.15. Permitir definir regras de funcionamento dos bloqueios comportamentais do antivírus, com no mínimo configuração do tipo de alerta, se o usuário será notificado para tomar uma ação, se o usuário será notificado e a ação será automática ou função silêncio onde a ação é tomada e o usuário não é notificado;
- 5.18.1.16. Permitir visualizar tempo de uso de cada aplicação e software filtrado pelo nome do usuário;
- 5.18.1.17. O console de gerenciamento web deverá prover na tela principal um dashboard com no mínimo informações sobre o percentual de máquina com número de antivírus/antimalware instalado e ameaças neutralizadas;
- 5.18.1.18. A solução deverá prover dashboard detalhado do gerenciamento do antimalware, do monitoramento e do inventário da rede com no mínimo as seguintes informações: estatísticas sobre ameaças identificadas, ameaças em quarentena, estatística de aplicação de licenças, informações quanto aos dispositivos ligados, desligados, informações sobre monitoramento de servidores, informações de monitoramento de banco de dados sqlserver,

- mysql, postgresql, oracle, monitoramento do serviço do Microsoft active directory e dns, informações quanto aos sistemas operacionais instalados, versão do sistema operacional, informações quanto ao número de máquinas com licença ativa do Windows bem como licenças não válidas, vencidas ou sem licença além de resumo dos 10 maiores fornecedores de software;
- 5.18.1.19. Ter painel de visualização que permita verificar através de cores e com informações básicas quais dispositivos estão com problemas, quais estão com alertas e quais estão com execução sem nenhum problema, identificando os que são ou não servidores;
- 5.18.1.20. A solução deverá fornecer relatórios referente às informações extraídas dos dispositivos, no mínimo deverá conter relatórios de inventário de software e hardware, relatório contendo equipamento e licença do Windows e seu status, informações da existência de algum software virtualizado instalado em algum dispositivo, relatório licença do antimalware e suas aplicações, relatório de infecções equipamento infectados, nome da infecção e nível de risco da mesma.
- 5.18.1.21. A solução deverá trazer informações sobre sistemas operacionais descontinuados, informando qual o sistema operacional bem como o equipamento que apresenta a condição;
- 5.18.1.22. Fornecer proteção, no mínimo, contra os seguintes tipos de códigos maliciosos: vírus de computador (em todas as suas variações), bombas lógicas, vermes ("worms"), cavalos de tróia ("trojan"), códigos espiões ("spyware", "keylogger", "screenlogger", etc), códigos de apoio à invasão e escalada de privilégio ("rootkit", "backdoor", etc), código e conteúdo indesejado ("dialer", "adware", "joke", etc);
- 5.18.1.23. Deverá ter a possibilidade de rastreamento manual nas estações de trabalho (programada ou não) de dispositivos móveis de armazenamento (ou não) e mídias removíveis ou quaisquer outros que permitam a transferência de arquivos para a estação de trabalho;
- 5.18.1.24. Deverá negar acesso ao arquivo infectado antes que o mesmo seja carregado em memória, aberto e/ou executado. Após negar o acesso ao arquivo infectado o antimalware deverá limpar o arquivo, e/ou apagar o arquivo infectado e enviar o arquivo infectado para uma área de segurança (quarentena);
- 5.18.1.25. Permitir detecção de ameaças em arquivos compactados nos principais algoritmos ("zip", "rar", "7zip")
- 5.18.1.26. A proteção de tempo real deverá trabalhar também com listas brancas (whitelist) permitindo adicionar um arquivo em específico ou um diretório, permitindo assim todos os arquivos de serem executados e recursivamente.
- 5.18.1.27. Permitir a execução de escaneamentos nos servidores e nas estações de trabalho (programada ou não).

- 5.18.1.28. Possuir camada de proteção contra acesso a sites fraudulentos e perigosos;
- 5.18.1.29. Possuir camada de proteção de arquivos contra sequestro de informações;
- 5.18.1.30. Possuir camada de proteção comportamental contra programas e/ou comportamentos suspeitos;
- 5.18.1.31. Ter módulo de histórico com uma lista de ações executadas pelo sistema antivírus/antimalware;
- 5.18.1.32. Permitir gerar “kit de emergência” que permitirá usuário dar boot na máquina e efetuar limpeza manual;
- 5.18.1.33. Possuir módulo de bloqueio por meio de comportamento dos processos, sistemas e programas;
- 5.18.1.34. A solução deverá proteger os arquivos através de análise comportamental, ou seja, proteger arquivos mesmo que a solução não disponha de assinatura para esse artefato, permitindo também a inclusão de arquivos na lista branca ou negra para análise comportamental de arquivos, inclusão de um arquivo somente para monitoramento bem como definir um arquivo ou aplicação que deverá ser bloqueada, permitindo configurar se tal ação será ou não notificada ao usuário, sendo que essa notificação ao usuário deverá ser em português do Brasil.
- 5.18.1.35. Além dos componentes responsáveis pelo combate a códigos maliciosos, possuir também componente responsável por implementar uma camada de proteção para acesso a internet que impeça abertura de sites com risco de acesso a conteúdos maliciosos;
- 5.18.1.36. Permitir a inclusão de arquivos na lista branca ou negra para com base em assinaturas, inclusão de um arquivo somente para monitoramento bem como definir um arquivo ou aplicação que deverá ser bloqueada, permitindo configurar se tal ação será ou não notificada ao usuário, sendo que essa notificação ao usuário deverá ser em português do Brasil, para esse item deverá permitir ativação ou não de proteção quanto pup do acrônimo em inglês possible unintended programs, ou seja, programas possivelmente indesejados como exemplos adwares e spywares;
- 5.18.1.37. A solução deverá prover proteção quanto a navegação, para essa função a solução deverá funcionar sem a necessidade de instalação de outro agente ou plugins nos navegadores;
- 5.18.1.38. Para a proteção de navegação a solução deverá permitir no mínimo proteção quanto sites maliciosos com base própria, sites com conteúdo indesejados (pup - possible unintended programs), bem como permitir a inclusão manual pelo administrador de sites na lista branca bem como na lista negra;

- 5.18.1.39. A solução deverá permitir agendamento de scan no dispositivo, podendo criar mais do que umas regras de agendamento separado entre rápido e completo, determinando dia e horário assim como a frequência;
- 5.18.1.40. A solução deverá permitir executar comandos e scripts remotos na estação, deverá permitir no mínimo acionar desinstalação de um software instalado, desinstalar ou instalar o antimalware, reiniciar dispositivo, desligar dispositivo, bloquear o dispositivo com possibilidade de desbloqueio através de uma senha específica.
- 5.18.1.41. Trazer a localização georreferenciada do dispositivo de maneira automática ou permitir configurar de maneira manual a latitude e longitude para localização do dispositivo;
- 5.18.1.42. Permitir acessar remotamente o equipamento direto do painel cloud, a solução permitirá o acesso através de solicitação ou diretamente sem solicitação de autorização;
- 5.18.1.43. Permitir configuração de tipos de alertas, para monitoramento dos dispositivos tais como: percentuais de cpu, memória e disco e tais informação deverão estar disponíveis em um painel ou dashboard específico para monitoramento;
- 5.18.1.44. O sistema deverá trazer no mínimo as seguintes informações de cada dispositivo: status do dispositivo, data em que os dados foram coletados, o número da licença do sistema operacional Windows bem como o status da licença daquele dispositivo, nome do host, versão do antivírus/antimalware, versão do sistema operacional, usuário logado no dispositivo, tempo de atividade, consumo e total de cpu, consumo e total de memória ram, consumo e total de memória swap, consumo e volume total de disco, interfaces de rede, serviços que estão em execução, serviços que estão parados, processos que estão mais consumindo cpu, processos que estão mais consumindo memória, informações de hardware, tais como: drivers de impressora, cd-rom, dispositivos gerais, ide, usb, som, vídeo, adaptador de rede, processador, bios, memória, placa de som, disco, memória, informações dos softwares instalados, tais como: fabricantes, software e versão;
- 5.18.1.45. O sistema deverá permitir monitoramento por meio de protocolo snmp de qualquer dispositivo conectado na rede, através da definição de qual dispositivo será o coletor dos dados e o mesmo centralizar as informações mostrando na plataforma
- 5.18.1.46. A plataforma deverá permitir ligar os dispositivos através do recurso wake-on-lan, caso o dispositivo possua este recurso e esteja ativada na bios;
- 5.18.1.47. O sistema deverá ter funcionalidade de proteção contra gravação de tela e printscreen através da inserção automática de marcas d'água ao realizar capturas de tela ou gravações de vídeo;

- 5.18.1.48. O sistema deverá ter recurso de visualização de documentos, através do endpoint, alertando o usuário caso tenha um documento obrigatório a ser visualizado, permitindo o mesmo registrar a visualização através de um token recebido por e-mail;
- 5.18.1.49. O sistema deverá ter bloqueio da função que permite o dispositivo se torne um ponto de hotspot (ponto específico em uma área física onde é possível acessar a internet, geralmente por meio de uma rede sem fio (wifi)), mantendo assim sua rede protegida evitando potenciais ameaças, garantindo um ambiente seguro e confiável.
- 5.18.1.50. O sistema deverá permitir o controle e gestão de patches do sistema operacional e outros produtos Microsoft gerenciáveis pelo Windows update;
- 5.18.1.51. O sistema deverá permitir configurar alertas através de configuração de identificação de um padrão de log no dispositivo, que pode ser configurado direto no painel em nuvem.
- 5.18.1.52. O sistema permitirá definir quais dispositivos serão centralizados de atualizações na rede. A partir do momento que for definido, os demais dispositivos da mesma rede, se atualização direto no centralizador;
- 5.18.1.53. O sistema permitirá efetuar agendamentos com objetivo de descoberta de novos dispositivos na rede. O agendamento poderá ser feito por dispositivo localizado em uma sub-rede e deverá mostrar a listagem de todos dispositivos que possuam ip na mesma;
- 5.18.1.54. O sistema terá um módulo de prevenção contra vazamento de dados (dlp – data loss prevention), que permitirá identificar através de scan se o dispositivo scaneado possui algum dado previamente cadastrado como alvo da prevenção através de expressão regular, permitindo que o sistema possa cadastrar novas informações usando a mesma sintaxe.
- 5.18.1.55. No caso de smartphones android, o sistema deverá prover as funcionalidades de:
- 5.18.1.56. Gerenciar os aplicativos que poderão ou não serem executados no dispositivo
- 5.18.1.57. Permitir bloqueio de determinados aplicativos por horário
- 5.18.1.58. Restringir seu funcionamento pela velocidade em km por hora, a fim de garantir segurança durante o uso e veículos
- 5.18.1.59. Configuração remota de redes wifi
- 5.18.1.60. Disponibilizar informações sobre monitoramento de memória, bateria, temperatura, localização
- 5.18.1.61. Disponibilizar informações sobre o dispositivo como sistema operacional, modelo dos dispositivos, versões, contas cadastradas e em uso, operadora, redes conectadas
- 5.18.1.62. No caso de dispositivo com sistema operacional Linux, o sistema deverá prover as funcionalidades de:

- 5.18.1.63. A solução deverá prover agente para monitoramento dos sistemas operacionais Linux prevendo ao menos o funcionamento nas versões centos 7 e 7, debian 8, 9 e 10, ubuntu 14, 16 e 18;
- 5.18.1.64. A solução deverá prover monitoramento dos agentes em Linux prevendo ao menos:
- 5.18.1.65. Ativar ou desativar recebimento de alerta dos dispositivos;
- 5.18.1.66. Verificar todos os tipos de códigos maliciosos contra os quais oferece proteção;
- 5.18.1.67. Permitir configuração de tipos de alertas, para monitoramento dos dispositivos tais como: percentuais de cpu, memória e disco e tais informações deverão estar disponíveis em um painel ou dashboard específico para monitoramento;
- 5.18.1.68. Trazer as seguintes informações de cada dispositivo: status do dispositivo, data em que os dados foram coletados, nome do host, versão do sistema operacional, usuário logado no dispositivo, consumo e total de cpu, consumo e total de memória ram, consumo e total de memória swap, consumo e volume total de disco e suas partições, interfaces de rede, serviços que estão em execução, serviços que estão parados, processos que estão mais consumindo cpu, processos que estão mais consumindo memória, histórico de comandos executados, localização do dispositivo em mapa georreferenciado, a solução deverá permitir configurar quais serviços o agente irá monitorar e em caso de parada do serviço o agente deverá reiniciar o mesmo;
- 5.18.1.69. A solução em nuvem deverá prover modulo de monitoramento de todas as soluções acima no mesmo painel de gerenciamento com objetivo de facilitar a operação;
- 5.18.1.70. O módulo de monitoramento deverá prover painel próprio na plataforma web com atualização em tempo real do alerta bem como prover app para ser instalado em dispositivos móveis da família android;
- 5.18.1.71. Deverá disponibilizar função modo tv para facilitar a análise das informações;
- 5.18.1.72. Deverá permitir configurar frequência de envio de alertas, com no mínimo configuração de 5, 25 ou 50 minutos entre a repetição do alerta.
- 5.18.1.73. O monitoramento de endpoint e servidores, a solução deverá prover ao menos os seguintes monitores: cpu, memória e disco;
- 5.18.1.74. Se o serviço de proteção está ativo, em caso de desativar o serviço de proteção em tempo real ou serviço de proteção de navegação, para esse item deverá ser enviado um relatório informando os equipamentos com proteção desativadas ou inexistentes;
- 5.18.1.75. Alerta configurável pelo administrador entre uma range de valores para emissão de alertas entre crítico, atenção ou informativo de no mínimo cpu, memória e carga média;

- 5.18.1.76. Permitir monitorar as interfaces de rede;
- 5.18.1.77. A solução deverá permitir o monitoramento dos serviços do sistema operacional.
- 5.18.1.78. Permitir emitir alertas de uptime de um determinado website através da configuração da url, assim como certificado ssl, lista negra.

5.19. MONITOR

- 5.19.1. Deverá ser fornecido 01 (um) monitor, com as características mínimas:
 - a. O monitor deve possuir tamanho de tela de no mínimo 27 polegadas;
 - b. Deverá ser do tipo LED ou equivalente, no formato Widescreen;
 - c. Deverá possuir proporção de 16:9;
 - d. Deverá possuir ângulo de visão de no mínimo 178° horizontal e vertical;
 - e. Deve possuir brilho de no mínimo 250 cd/m²;
 - f. A taxa de contraste real mínima de 1.000:1;
 - g. O tempo de resposta não deve ultrapassar 6ms;
 - h. Deve suportar resolução nativa mínima de 1920x1080 pixels a 60 Hz;
 - i. Deve possuir tecnologia IPS (In-Plane-Switching);
 - j. Deve possuir pelo menos 1 (uma) conexão digital, DisplayPort ou HDMI;
 - k. Deve ser fornecido junto com o monitor, na mesma caixa e pelo fabricante do monitor, 1 (um) cabo DisplayPort ou HDMI para interligar o monitor ao workstation ofertado;
 - l. Deve possuir uma entrada analógica VGA;
 - m. Deve possuir fonte de alimentação interna com tensão de entrada bivolt automática;
 - n. Deve possuir base com ajustes mínimos, de: inclinação, altura e rotação pivot (retrato/paisagem);

5.20. COMPATIBILIDADES E CERTIFICAÇÕES:

- a. Compatibilidade com EPEAT na categoria Gold, comprovada através de atestado e certidões que comprovem que o monitor ofertado é aderente ao padrão de eficiência energética EPEAT, emitido por instituo credenciado junto ao INMETRO. Será admitida como comprovação também, a indicação que o monitor consta em listagem e em status de "active" no site EPEAT através do link: <http://www.epeat.net>;
- b. Certificação ENERGY STAR, comprovando que o monitor ofertado atinge as exigências para o melhor aproveitamento de uso de energia elétrica. Essa característica deverá ser comprovada pela listagem do monitor no site <http://www.energystar.gov>. Serão aceitas as certificações emitidas pelo INMETRO, em conformidade com as Portarias nº 170/2012 e 304/2023;
- c. O monitor ofertado deverá possuir certificação que sua fabricação está livre de 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).

5.21. CONDIÇÕES GERAIS:

- a. O monitor ofertado deverá possuir cor predominante: Preto, ou cinza ou Prata;
- b. Deverá ser fornecido 01 (um) cabo de alimentação com comprimento mínimo de 1.8 metros, no padrão NBR 14.136;
- c. Deverá ser fornecido cabos compatíveis com as entradas de vídeos entre o conjunto (monitor e CPU);
- d. O monitor e acessórios devem ser do mesmo fabricante dos desktops e workstations. O monitor deve ser produzido em regime de ODM (Original Design Manufacturer), ou seja, ainda que fabricado por um terceiro, tem design próprio do fabricante do desktop, com nr. de série padronizado segundo sistema de garantia do fabricante do pc; apresenta design exclusivo no mesmo padrão de acabamento do pc. Não serão aceitos monitores de livre comercialização no mercado nem aqueles fornecidos em regime de OEM (que possuem apenas a logomarca do fabricante do workstation, porém se trata do mesmo modelo fornecido sob outras marcas).

5.22. NOBREAK

Os *microcomputadores do Tipo I, Tipo II e o Workstation* (detalhados nos itens 2, 3 e 5 deste Anexo I) devem vir acompanhados do equipamento NOBREAK (UPS), observando as especificações técnicas descritas abaixo:

5.23.ESPECIFICAÇÃO TÉCNICA – NOBREAK

O equipamento deverá atender aos seguintes requisitos mínimos:

- Potência nominal mínima de 600 VA;
- Tensão de entrada compatível com a rede elétrica local (bivolt automático ou conforme padrão adotado pela Administração);
- Tensão de saída de 115V ou bivolt, compatível com os equipamentos a serem protegidos;
- Frequência de operação de 60 Hz;
- Autonomia mínima de 25 (vinte e cinco) minutos, considerando carga típica, devendo ser comprovada por meio de catálogo técnico, manual do fabricante ou declaração oficial do fabricante;
- Tecnologia de estabilização e filtragem de linha integrada;

- Proteção contra:
- Sobrecarga;
- Curto-circuito;
- Subtensão e sobretensão;
- Possuir, no mínimo, 4 (quatro) tomadas de saída padrão brasileiro (NBR 14136);
- Tempo de recarga da bateria conforme especificação do fabricante;
- Bateria interna selada, livre de manutenção ou com manutenção simplificada;
- Indicação visual ou sonora de funcionamento (LEDs e/ou alarmes);
- Possuir chave liga/desliga e proteção contra descarga total da bateria;
- Garantia mínima de 12 (doze) meses.

5.24.EXIGÊNCIAS COMPLEMENTARES

- O equipamento deverá ser novo, sem uso, original de fábrica;
- Deverá acompanhar todos os acessórios necessários ao pleno funcionamento;
- O fornecedor deverá apresentar documentação técnica oficial do fabricante que comprove o atendimento às especificações exigidas, especialmente quanto à autonomia;
- O produto deverá estar em conformidade com as normas brasileiras aplicáveis, especialmente certificação do INMETRO, quando aplicável.

6. LOTE ÚNICO – ITEM 05 - MONITOR 21,5”

6.1. DEVERÁ SER FORNECIDO 01 (UM) MONITOR, COM AS CARACTERÍSTICAS MÍNIMAS:

- 6.1.1. O monitor deve possuir tamanho de tela de no mínimo 21.5 polegadas;
- 6.1.2. Deverá ser do tipo LED, no formato Widescreen;
- 6.1.3. Deverá possuir proporção de 16:9;
- 6.1.4. Deverá possuir ângulo de visão de no mínimo 178° horizontal e vertical;
- 6.1.5. Deve possuir brilho de no mínimo 250 cd/m²;
- 6.1.6. A taxa de contraste real mínima de 1.000:1;
- 6.1.7. O tempo de resposta não deve ultrapassar 8ms;
- 6.1.8. Deve suportar resolução nativa mínima de 1920x1080 pixels a 60 Hz;
- 6.1.9. Deve possuir pelo menos 1 (uma) conexão digital, DisplayPort ou HDMI;
- 6.1.10. Deve ser fornecido junto com o monitor, na mesma caixa e pelo fabricante do monitor, 1 (um) cabo DisplayPort ou HDMI;
- 6.1.11. Deve possuir uma entrada analógica VGA;

- 6.1.12. Deve possuir fonte de alimentação interna com tensão de entrada bivolt automática;
- 6.1.13. Deve possuir base com ajustes mínimos, de: inclinação, altura e rotação pivot (retrato/paisagem);

6.2. COMPATIBILIDADES E CERTIFICAÇÕES:

- 6.2.1. Compatibilidade com EPEAT em qualquer categoria, comprovada através de atestado e certidões que comprovem que o monitor ofertado é aderente ao padrão de eficiência energética EPEAT, emitido por instituo credenciado junto ao INMETRO. Será admitida como comprovação também, a indicação que o monitor consta em listagem e em status de "active" no site EPEAT através do link: <http://www.epeat.net>;
- 6.2.2. Certificação ENERGY STAR, comprovando que o monitor ofertado atinge as exigências para o melhor aproveitamento de uso de energia elétrica. Essa característica deverá ser comprovada pela listagem do monitor no site <http://www.energystar.gov>. Serão aceitas as certificações emitidas pelo INMETRO, em conformidade com as Portarias nº 170/2012 e 304/2023;
- 6.2.3. O monitor ofertado deverá possuir certificação que sua fabricação está livre de 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).

6.3. CONDIÇÕES GERAIS:

- 6.3.1. O monitor ofertado deverá possuir cor predominante: Preto, ou Cinza ou Prata;
- 6.3.2. Deverá ser fornecido 01 (um) cabo de alimentação com comprimento mínimo de 1.8 metros, no padrão NBR 14.136;
- 6.3.3. O monitor e acessórios devem ser do mesmo fabricante dos microcomputadores. O monitor deve ser produzido em regime de ODM (Original Design Manufacturer), ou seja, ainda que fabricado por um terceiro, tem design próprio do fabricante do desktop e workstation, com nr. de série padronizado segundo sistema de garantia do fabricante do pc; apresenta design exclusivo no mesmo padrão de acabamento do desktop e workstation. Não serão aceitos monitores de livre comercialização no mercado nem aqueles fornecidos em regime de OEM (que possuem apenas a logomarca do fabricante do pc, porém se trata do mesmo modelo fornecido sob outras marcas). Esta exigência se baseia na necessidade de padronização e garantia uniforme do fabricante ao conjunto do desktop e monitor adquiridos, bem como da perfeita compatibilidade entre os acessórios para afiação do pc e a base do monitor, sem prejudicar ajustes ergonômicos do monitor nem a conexão de todos os cabos em ambos, pc e monitor.

7. LOTE ÚNICO – ITEM 06 - MONITOR 23,8"

7.1. DEVERÁ SER FORNECIDO 01 (UM) MONITOR, COM AS CARACTERÍSTICAS MÍNIMAS:

- 7.1.1. O monitor deve possuir tamanho de tela de no mínimo 23.8 polegadas;
- 7.1.2. Deverá ser do tipo LED ou equivalente, no formato Widescreen;
- 7.1.3. Deverá possuir proporção de 16:9;
- 7.1.4. Deverá possuir ângulo de visão de no mínimo 178° horizontal e vertical;
- 7.1.5. Deve possuir brilho de no mínimo 250 cd/m²;
- 7.1.6. A taxa de contraste real mínima de 1.000:1;
- 7.1.7. O tempo de resposta não deve ultrapassar 8ms;
- 7.1.8. Deve suportar resolução nativa mínima de 1920x1080 pixels a 60 Hz;
- 7.1.9. Deve possuir tecnologia IPS (In-Plane-Switching);
- 7.1.10. Deve possuir pelo menos 1 (uma) conexão digital, DisplayPort ou HDMI;
- 7.1.11. Deve ser fornecido junto com o monitor, na mesma caixa e pelo fabricante do monitor, 1 (um) cabo DisplayPort ou HDMI;
- 7.1.12. Deve possuir uma entrada analógica VGA;
- 7.1.13. Deve possuir fonte de alimentação interna com tensão de entrada bivolt automática;
- 7.1.14. Deve possuir base com ajustes mínimos, de: inclinação, altura e rotação pivot (retrato/paisagem);

7.2. COMPATIBILIDADES E CERTIFICAÇÕES:

- 7.2.1. Compatibilidade com EPEAT na categoria Gold, comprovada através de atestado e certidões que comprovem que o monitor ofertado é aderente ao padrão de eficiência energética EPEAT, emitido por instituo credenciado junto ao INMETRO. Será admitida como comprovação também, a indicação que o monitor consta em listagem e em status de "active" no site EPEAT através do link: <http://www.epeat.net>;
- 7.2.2. Certificação ENERGY STAR, comprovando que o monitor ofertado atinge as exigências para o melhor aproveitamento de uso de energia elétrica. Essa característica deverá ser comprovada pela listagem do monitor no site <http://www.energystar.gov>. Serão aceitas as certificações emitidas pelo INMETRO, em conformidade com as Portarias nº 170/2012 e 304/2023;
- 7.2.3. O monitor ofertado deverá possuir certificação que sua fabricação está livre de 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).

7.3. CONDIÇÕES GERAIS:

- 7.3.1. O monitor ofertado deverá possuir cor predominante: Preto, ou cinza ou Prata;
- 7.3.2. Deverá ser fornecido 01 (um) cabo de alimentação com comprimento mínimo de 1.8 metros, no padrão NBR 14.136;

- 7.3.3. O monitor e acessórios devem ser do mesmo fabricante dos desktops e workstations. O monitor deve ser produzido em regime de ODM (Original Design Manufacturer), ou seja, ainda que fabricado por um terceiro, tem design próprio do fabricante do desktop, com nr. de série padronizado segundo sistema de garantia do fabricante do pc; apresenta design exclusivo no mesmo padrão de acabamento do pc. Não serão aceitos monitores de livre comercialização no mercado nem aqueles fornecidos em regime de OEM (que possuem apenas a logomarca do fabricante do workstation, porém se trata do mesmo modelo fornecido sob outras marcas).

8. LOTE ÚNICO – ITEM 07 – TABLET

8.1. DEVERÁ SER FORNECIDO DISPOSITIVO TABLET, COM AS CARACTERÍSTICAS MÍNIMAS:

- 8.1.1. Processador octa-core de clock de 2,0 ghz octa-core, capaz de executar arquivos de áudio e vídeo,
- 8.1.2. As funções de decodificação de áudio e vídeo devem ser aceleradas por hardware, possuir decodificação por hardware para pelo menos os seguintes formatos: h263, h264 e mpeg4;
- 8.1.3. Memória capacidade mínima de 3gb (três gigabyte);
- 8.1.4. Tela: colorida e construída com tecnologia lcd ou oled, com retro iluminação
- 8.1.5. Tamanho mínimo de 10 (dez) polegadas
- 8.1.6. Resolução mínima fhd (1920x1080);
- 8.1.7. Armazenamento: interno do tipo flash/emmc, mais específica e maior qualidade,
- 8.1.8. Capacidade de 128 gb de armazenamento interno,
- 8.1.9. Possuir slot para cartão de memória padrão micro sd para expansão do armazenamento interno
- 8.1.10. Compatível com cartões de até 1tb;
- 8.1.11. Conectividade:
- 8.1.12. Wi-fi padrão ieee 802.11 b/g/n/ac, integrado (interno) ao equipamento,
- 8.1.13. Modem interno com suporte a redes 4g (no mínimo dual-band 2100mhz e 850mhz) habilitado para funcionamento nas frequências do sistema brasileiro de comunicação móvel, desbloqueado para todas as operadoras,
- 8.1.14. Bluetooth versão 5.0 ou superior, integrado (interno) ao equipamento,
- 8.1.15. Sistema de gps integrado (interno) com antena interna;
- 8.1.16. Sistema de áudio
- 8.1.17. Interfaces: microfone e alto-falante integrados ao gabinete,
- 8.1.18. Saída para fone de ouvidos para conector padrão p2 de 3,5 mm e com 03 (três) pontos de contato (terra, áudio direito e esquerdo),
- 8.1.19. Câmera frontal e traseira:
- 8.1.20. Integrada ao equipamento,
- 8.1.21. Câmera traseira com resolução mínima de 08 mp (oito megapixels),

- 8.1.22. Ajuste de foco automático e zoom digital,
- 8.1.23. Câmera frontal com resolução mínima 05 mp (cinco megapixels),
- 8.1.24. Ambas as câmeras devem permitir filmar e tirar fotos;
- 8.1.25. Bateria:
 - 8.1.25.1. Interna e recarregável
 - 8.1.25.2. Lítio-ion ou polímero de lítio,
 - 8.1.25.3. Capacidade mínima da bateria: 7000 ma/h,
 - 8.1.25.4. Permitir que o tablet seja utilizado enquanto a bateria estiver carregando,
 - 8.1.25.5. Possuir pelo menos os seguintes mecanismos de segurança: circuito para interromper a conexão da bateria em casos de sobrecorrente e sobrecarga, com carregador conectado à energia;
- 8.1.26. Gabinete:
 - 8.1.26.1. O gabinete não poderá apresentar saliências, pontas ou estruturas externas perfurantes ou cortantes,
 - 8.1.26.2. Deve possuir teclas para controle de volume do som,
- 8.1.27. Peso máximo com bateria de 500g;
- 8.1.28. Funcionalidades:
 - 8.1.28.1. Possuir acelerômetro,
 - 8.1.28.2. Funcionar como “usb mass storage”,
 - 8.1.28.3. Sensor de luz ambiente com capacidade para ajuste automático do brilho da tela,
 - 8.1.28.4. Permitir a mudança da orientação da tela e o bloqueio da posição,
 - 8.1.28.5. Recursos de vídeo: gravação com resolução de pelo menos 640 x 480 fhd, formatos mínimos de reprodução: h.263, h.264 e mpeg-4;
- 8.1.29. Sistema operacional:
 - 8.1.29.1. Sistema operacional android 12 português ou versão superior em português,
 - 8.1.29.2. Suporte a configuração de proxy para rede wifi (este suporte deve ser integrado à aplicação de configuração de rede sem fio e sem a necessidade de aplicativos ou softwares extras),
- 8.1.30. Aplicações:
 - 8.1.30.1. Agenda, calendário, relógio com horário mundial, alarme, calculadora, cronômetro,
 - 8.1.30.2. Devendo permitir reinstalação do sistema operacional através de partição de recovery, sendo ela acionada através de boot por meio de teclas próprias do teclado, validando a chave de licenciamento do equipamento de forma automática.
- 8.1.31. Solução de Gerenciamento e segurança
 - 8.1.31.1. Acompanhar solução de monitoramento, gerenciamento e antivírus, conforme as especificação técnica abaixo:
 - 8.1.31.2. O fabricante do produto deverá ser uma empresa atuante na área de segurança da informação a fim de garantir eficácia das soluções de proteção, e possuir modelo de boas práticas baseado em padrões de mercado.

- 8.1.31.3. A solução deverá possuir em um único painel em nuvem que agregue em grande parte o gerenciamento e monitoramento das soluções listadas. As funções de gerenciamento e monitoramento que deverão ter no painel em nuvem estão listadas neste documento.
- 8.1.31.4. A solução entregue por um único fornecedor precisará deter a capacidade de fazer ajustes/correções, mesmo que no código fonte do sistema em nuvem, caso necessário.
- 8.1.31.5. A proponente deverá garantir que ao longo do presente contrato, nenhum produto, software, estejam em uma versão considerada não oficial, não comercializada, “end-of-life, end-of-sale ou end-of-support”. Ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte e vida. Devendo estar em linha de produção do fabricante, sempre em sua versão mais atualizada (seja software e sistema, caso o fabricante lance uma nova versão etc.) A proponente deverá garantir que estão cobertos por garantia ao longo do contrato pela proponente.
- 8.1.31.6. Todas as funcionalidades descritas, deverão ser comprovadas por meio de documento oficial do fabricante, a fim de garantir que as funcionalidades de grande importância para proteção estejam contempladas.
- 8.1.31.7. Apresentar carta emitida pelo próprio fabricante, dirigida ao contratante, referenciando ao edital em epígrafe, informando que a proponente é revenda autorizada a comercializar seus produtos e serviços, e o fabricante confirma que atende a todos os itens listados no referente edital.
- 8.1.31.8. Será feita a verificação da compatibilidade dos recursos e das capacidades, facilidades operacionais informadas na proposta para cada item ofertado com base nas informações dos catálogos, folhetos, manuais técnicos e semelhantes produzidos pelo fabricante. Documentos estes que deverão ser anexados a proposta comercial, referenciar o endereço web para consultas e diligências de todo material apresentado. Salienta-se que não serão aceitos materiais produzidos pela proponente a não ser que ela seja fabricante.
- 8.1.31.9. Apresentar no mínimo 1 técnico certificado em todas as soluções ofertadas. Este deverá ser comprovado através de documento emitido pelo fabricante da solução ou empresa devidamente autorizada para emissão de certificados, no caso de a certificação não ser realizada pelo fabricante da solução, deverá apresentar comprovação que a empresa fornecedora da certificação é devidamente credenciada para emitir tal documentação.
- 8.1.31.10. Apresentar no mínimo 1 técnico certificado com cursos voltados para segurança da informação, oferecidos por empresas cujo foco seja segurança da informação.
- 8.1.31.11. Apresentar no mínimo 1 técnico que possua atestado de capacidade técnica que já tenha executado projetos nas soluções mencionadas
- 8.1.31.12. Na proposta. O atestado deverá ser assinado pela empresa contratante ou pelo fabricante da solução.
- 8.1.31.13. A proponente deverá disponibilizar serviços de treinamento especializado em segurança da informação oficiais do fabricante da solução,

com certificado do fabricante, de forma a atender aos seguintes requisitos: carga horária mínima de 40 horas, até 20 participantes na turma.

- 8.1.31.14. Item – serviço de controle e segurança de dispositivos
- 8.1.31.15. A solução deverá funcionar tanto de forma integrada, quanto de forma isolada (“stand-alone”);
- 8.1.31.16. Todos os componentes necessários à implementação desta solução corporativa deverão pertencer à mesma família de solução corporativa, denominado neste certame como segurança de dispositivos (integrar uma única solução corporativa);
- 8.1.31.17. Todos os componentes tratados nesta descrição, deverão funcionar de forma integrada na solução. Não será aceito soluções diferentes com gestão separada;
- 8.1.31.18. A solução deverá permitir que haja troca de informações entre painel de gerenciamento e seus clientes. As informações de que trata o presente item são aqueles relevantes para a realização das ações de segurança e proteção de computadores ligados em rede, assim como monitoramento e controle.
- 8.1.31.19. A troca de informações de que trata o tópico anterior deverá permitir o recolhimento de informações sobre o estado de funcionamento da solução nas diferentes estações. As seguintes informações deverão ser contempladas, no mínimo: versão do sistema operacional, nome do host, versão do antimalware, status e informações cpu, memória, disco;
- 8.1.31.20. O acesso para ferramenta de configuração do gerenciamento em nuvem (plataforma) deverá ser com acesso seguro via https, com possibilidade de uso de duplo fator de autenticação.
- 8.1.31.21. Ter possibilidade de através de uma senha administrativa, desabilitar algumas funções do sistema de proteção local de estação ou servidor da família Windows;
- 8.1.31.22. A solução deverá permitir trabalhar obrigatoriamente na língua portuguesa do brasil e inglês;
- 8.1.31.23. A plataforma de gerenciamento em nuvem permitirá efetuar configurações e criação de políticas por grupos ou territórios em uma hierarquia do tipo árvore, selecionando qual grupo de dispositivos pertencente à que território aquela política se aplica.
- 8.1.31.24. A plataforma de gerenciamento em nuvem permitirá gerência granular de políticas, por nível hierárquico, permitindo usuário configurar políticas seguindo uma ordem de hierarquia determinada por grupos ou conjunto de computadores, sendo possível permitir a configuração de políticas como dominantes, ou seja, que não podem ser reescritas por políticas em nível hierárquico mais baixo;
- 8.1.31.25. A ferramenta deverá prover gerência de acesso para usuários de administração com vários níveis de permissão configuráveis pelo administrador principal.
- 8.1.31.26. Com relação ao sistema específico da família Microsoft Windows, o sistema deverá no mínimo ter as seguintes funcionalidades:

- 8.1.31.27. Suportar todas as funcionalidades nos sistemas Windows 10 e 11 e Windows server 2016/2019/2022
- 8.1.31.28. Verificar todos os tipos de códigos maliciosos contra os quais oferece proteção e realizar as tarefas de proteção de computadores ligados em rede em tempo real;
- 8.1.31.29. Permitir definir regras de funcionamento dos bloqueios comportamentais do antivírus, com no mínimo configuração do tipo de alerta, se o usuário será notificado para tomar uma ação, se o usuário será notificado e a ação será automática ou função silêncio onde a ação é tomada e o usuário não é notificado;
- 8.1.31.30. Permitir visualizar tempo de uso de cada aplicação e software filtrado pelo nome do usuário;
- 8.1.31.31. O console de gerenciamento web deverá prover na tela principal um dashboard com no mínimo informações sobre o percentual de máquina com número de antivírus/antimalware instalado e ameaças neutralizadas;
- 8.1.31.32. A solução deverá prover dashboard detalhado do gerenciamento do antimalware, do monitoramento e do inventário da rede com no mínimo as seguintes informações: estatísticas sobre ameaças identificadas, ameaças em quarentena, estatística de aplicação de licenças, informações quanto aos dispositivos ligados, desligados, informações sobre monitoramento de servidores, informações de monitoramento de banco de dados sqlserver, mysql, postgresql, oracle, monitoramento do serviço do Microsoft active directory e dns, informações quanto aos sistemas operacionais instalados, versão do sistema operacional, informações quanto ao número de máquinas com licença ativa do Windows bem como licenças não válidas, vencidas ou sem licença além de resumo dos 10 maiores fornecedores de software;
- 8.1.31.33. Ter painel de visualização que permita verificar através de cores e com informações básicas quais dispositivos estão com problemas, quais estão com alertas e quais estão com execução sem nenhum problema, identificando os que são ou não servidores;
- 8.1.31.34. A solução deverá prover relatórios referente às informações extraídas dos dispositivos, no mínimo deverá conter relatórios de inventário de software e hardware, relatório contendo equipamento e licença do Windows e seu status, informações da existência de algum software virtualizado instalado em algum dispositivo, relatório licença do antimalware e suas aplicações, relatório de infecções equipamento infectados, nome da infecção e nível de risco da mesma.
- 8.1.31.35. A solução deverá trazer informações sobre sistemas operacionais descontinuados, informando qual o sistema operacional bem como o equipamento que apresenta a condição;
- 8.1.31.36. Fornecer proteção, no mínimo, contra os seguintes tipos de códigos maliciosos: vírus de computador (em todas as suas variações), bombas lógicas, vermes ("worms"), cavalos de tróia ("trojan"), códigos espiões ("spyware", "keylogger", "screenlogger", etc), códigos de apoio à invasão e escalada de

- privilégio (“rootkit”, “backdoor”, etc), código e conteúdo indesejado (“dialer”, “adware”, “joke”, etc);
- 8.1.31.37. Deverá ter a possibilidade de rastreamento manual nas estações de trabalho (programada ou não) de dispositivos móveis de armazenamento (ou não) e mídias removíveis ou quaisquer outros que permitam a transferência de arquivos para a estação de trabalho;
- 8.1.31.38. Deverá negar acesso ao arquivo infectado antes que o mesmo seja carregado em memória, aberto e/ou executado. Após negar o acesso ao arquivo infectado o antimalware deverá limpar o arquivo, e/ou apagar o arquivo infectado e enviar o arquivo infectado para uma área de segurança (quarentena);
- 8.1.31.39. Permitir detecção de ameaças em arquivos compactados nos principais algoritmos (“zip”, “rar”, “7zip”)
- 8.1.31.40. A proteção de tempo real deverá trabalhar também com listas brancas (whitelist) permitindo adicionar um arquivo em específico ou um diretório, permitindo assim todos os arquivos de serem executados e recursivamente.
- 8.1.31.41. Permitir a execução de escaneamentos nos servidores e nas estações de trabalho (programada ou não).
- 8.1.31.42. Possuir camada de proteção contra acesso a sites fraudulentos e perigosos;
- 8.1.31.43. Possuir camada de proteção de arquivos contra sequestro de informações;
- 8.1.31.44. Possuir camada de proteção comportamental contra programas e/ou comportamentos suspeitos;
- 8.1.31.45. Ter módulo de histórico com uma lista de ações executadas pelo sistema antivírus/antimalware;
- 8.1.31.46. Permitir gerar “kit de emergência” que permitirá usuário dar boot na máquina e efetuar limpeza manual;
- 8.1.31.47. Possuir módulo de bloqueio por meio de comportamento dos processos, sistemas e programas;
- 8.1.31.48. A solução deverá proteger os arquivos através de análise comportamental, ou seja, proteger arquivos mesmo que a solução não disponha de assinatura para esse artefato, permitindo também a inclusão de arquivos na lista branca ou negra para análise comportamental de arquivos, inclusão de um arquivo somente para monitoramento bem como definir um arquivo ou aplicação que deverá ser bloqueada, permitindo configurar se tal ação será ou não notificada ao usuário, sendo que essa notificação ao usuário deverá ser em português do Brasil.
- 8.1.31.49. Além dos componentes responsáveis pelo combate a códigos maliciosos, possuir também componente responsável por implementar uma camada de proteção para acesso a internet que impeça abertura de sites com risco de acesso a conteúdos maliciosos;
- 8.1.31.50. Permitir a inclusão de arquivos na lista branca ou negra para com base em assinaturas, inclusão de um arquivo somente para monitoramento bem

como definir um arquivo ou aplicação que deverá ser bloqueada, permitindo configurar se tal ação será ou não notificada ao usuário, sendo que essa notificação ao usuário deverá ser em português do Brasil, para esse item deverá permitir ativação ou não de proteção quanto pup do acronico em inglês possible unintended programs, ou seja, programas possivelmente indesejados como exemplos adwares e spywares;

- 8.1.31.51. A solução deverá prover proteção quanto a navegação, para essa função a solução deverá funcionar sem a necessidade de instalação de outro agente ou plugins nos navegadores;
- 8.1.31.52. Para a proteção de navegação a solução deverá permitir no mínimo proteção quanto sites maliciosos com base própria, sites com conteúdo indesejados (pup - possible unintended programs), bem como permitir a inclusão manual pelo administrador de sites na lista branca bem como na lista negra;
- 8.1.31.53. A solução deverá permitir agendamento de scan no dispositivo, podendo criar mais do que umas regras de agendamento separado entre rápido e completo, determinando dia e horário assim como a frequência;
- 8.1.31.54. A solução deverá permitir executar comandos e scripts remotos na estação, deverá permitir no mínimo acionar desinstalação de um software instalado, desinstalar ou instalar o antimalware, reiniciar dispositivo, desligar dispositivo, bloquear o dispositivo com possibilidade de desbloqueio através de uma senha específica.
- 8.1.31.55. Trazer a localização georreferenciada do dispositivo de maneira automática ou permitir configurar de maneira manual a latitude e longitude para localização do dispositivo;
- 8.1.31.56. Permitir acessar remotamente o equipamento direto do painel cloud, a solução permitirá o acesso através de solicitação ou diretamente sem solicitação de autorização;
- 8.1.31.57. Permitir configuração de tipos de alertas, para monitoramento dos dispositivos tais como: percentuais de cpu, memória e disco e tais informações deverão estar disponíveis em um painel ou dashboard específico para monitoramento;
- 8.1.31.58. O sistema deverá trazer no mínimo as seguintes informações de cada dispositivo: status do dispositivo, data em que os dados foram coletados, o número da licença do sistema operacional Windows bem como o status da licença daquele dispositivo, nome do host, versão do antivírus/antimalware, versão do sistema operacional, usuário logado no dispositivo, tempo de atividade, consumo e total de cpu, consumo e total de memória ram, consumo e total de memória swap, consumo e volume total de disco, interfaces de rede, serviços que estão em execução, serviços que estão parados, processos que estão mais consumindo cpu, processos que estão mais consumindo memória, informações de hardware, tais como: drivers de impressora, cd-rom, dispositivos gerais, ide, usb, som, vídeo, adaptador de rede, processador, bios,

- memória, placa de som, disco, memória, informações dos softwares instalados, tais como: fabricantes, software e versão;
- 8.1.31.59. O sistema deverá permitir monitoramento por meio de protocolo snmp de qualquer dispositivo conectado na rede, através da definição de qual dispositivo será o coletor dos dados e o mesmo centralizar as informações mostrando na plataforma
- 8.1.31.60. A plataforma deverá permitir ligar os dispositivos através do recurso wake-on-lan, caso o dispositivo possua este recurso e esteja ativada na bios;
- 8.1.31.61. O sistema deverá ter funcionalidade de proteção contra gravação de tela e printscreen através da inserção automática de marcas d'água ao realizar capturas de tela ou gravações de vídeo;
- 8.1.31.62. O sistema deverá ter recurso de visualização de documentos, através do endpoint, alertando o usuário caso tenha um documento obrigatório a ser visualizado, permitindo o mesmo registrar a visualização através de um token recebido por e-mail;
- 8.1.31.63. O sistema deverá ter bloqueio da função que permite o dispositivo se torne um ponto de hotspot (ponto específico em uma área física onde é possível acessar a internet, geralmente por meio de uma rede sem fio (wifi)), mantendo assim sua rede protegida evitando potenciais ameaças, garantindo um ambiente seguro e confiável.
- 8.1.31.64. O sistema deverá permitir o controle e gestão de patches do sistema operacional e outros produtos Microsoft gerenciáveis pelo Windows update;
- 8.1.31.65. O sistema deverá permitir configurar alertas através de configuração de identificação de um padrão de log no dispositivo, que pode ser configurado direto no painel em nuvem.
- 8.1.31.66. O sistema permitirá definir quais dispositivos serão centralizados de atualizações na rede. A partir do momento que for definido, os demais dispositivos da mesma rede, se atualização direto no centralizador;
- 8.1.31.67. O sistema permitirá efetuar agendamentos com objetivo de descoberta de novos dispositivos na rede. O agendamento poderá ser feito por dispositivo localizado em uma sub-rede e deverá mostrar a listagem de todos dispositivos que possuam ip na mesma;
- 8.1.31.68. O sistema terá um módulo de prevenção contra vazamento de dados (dlp – data loss prevention), que permitirá identificar através de scan se o dispositivo scaneado possui algum dado previamente cadastrado como alvo da prevenção através de expressão regular, permitindo que o sistema possa cadastrar novas informações usando a mesma sintaxe.
- 8.1.31.69. No caso de smartphones android, o sistema deverá prover as funcionalidades de:
- 8.1.31.70. Gerenciar os aplicativos que poderão ou não serem executados no dispositivo
- 8.1.31.71. Permitir bloqueio de determinados aplicativos por horário
- 8.1.31.72. Restringir seu funcionamento pela velocidade em km por hora, a fim de garantir segurança durante o uso e veículos

- 8.1.31.73. Configuração remota de redes wifi
- 8.1.31.74. Disponibilizar informações sobre monitoramento de memória, bateria, temperatura, localização
- 8.1.31.75. Disponibilizar informações sobre o dispositivo como sistema operacional, modelo dos dispositivos, versões, contas cadastradas e em uso, operadora, redes conectadas
- 8.1.31.76. No caso de dispositivo com sistema operacional Linux, o sistema deverá prover as funcionalidades de:
- 8.1.31.77. A solução deverá prover agente para monitoramento dos sistemas operacionais Linux prevendo ao menos o funcionamento nas versões centos 7 e 7, debian 8, 9 e 10, ubuntu 14, 16 e 18;
- 8.1.31.78. A solução deverá prover monitoramento dos agentes em Linux prevendo ao menos:
- 8.1.31.79. Ativar ou desativar recebimento de alerta dos dispositivos;
- 8.1.31.80. Verificar todos os tipos de códigos maliciosos contra os quais oferece proteção;
- 8.1.31.81. Permitir configuração de tipos de alertas, para monitoramento dos dispositivos tais como: percentuais de cpu, memória e disco e tais informações deverão estar disponíveis em um painel ou dashboard específico para monitoramento;
- 8.1.31.82. Trazer as seguintes informações de cada dispositivo: status do dispositivo, data em que os dados foram coletados, nome do host, versão do sistema operacional, usuário logado no dispositivo, consumo e total de cpu, consumo e total de memória ram, consumo e total de memória swap, consumo e volume total de disco e suas partições, interfaces de rede, serviços que estão em execução, serviços que estão parados, processos que estão mais consumindo cpu, processos que estão mais consumindo memória, histórico de comandos executados, localização do dispositivo em mapa georreferenciado, a solução deverá permitir configurar quais serviços o agente irá monitorar e em caso de parada do serviço o agente deverá reiniciar o mesmo;
- 8.1.31.83. A solução em nuvem deverá prover modulo de monitoramento de todas as soluções acima no mesmo painel de gerenciamento com objetivo de facilitar a operação;
- 8.1.31.84. O módulo de monitoramento deverá prover painel próprio na plataforma web com atualização em tempo real do alerta bem como prover app para ser instalado em dispositivos móveis da família android;
- 8.1.31.85. Deverá disponibilizar função modo tv para facilitar a análise das informações;
- 8.1.31.86. Deverá permitir configurar frequência de envio de alertas, com no mínimo configuração de 5, 25 ou 50 minutos entre a repetição do alerta.
- 8.1.31.87. O monitoramento de endpoint e servidores, a solução deverá prover ao menos os seguintes monitores: cpu, memória e disco;
- 8.1.31.88. Se o serviço de proteção está ativo, em caso de desativar o serviço de proteção em tempo real ou serviço de proteção de navegação, para esse item

deverá ser enviado um relatório informando os equipamentos com proteção desativadas ou inexistentes;

- 8.1.31.89. Alerta configurável pelo administrador entre uma range de valores para emissão de alertas entre crítico, atenção ou informativo de no mínimo cpu, memória e carga média;
- 8.1.31.90. Permitir monitorar as interfaces de rede;
- 8.1.31.91. A solução deverá permitir o monitoramento dos serviços do sistema operacional.
- 8.1.31.92. Permitir emitir alertas de uptime de um determinado website através da configuração da url, assim como certificado ssl, lista negra
- 8.1.31.93. Documentação:
- 8.1.31.94. Objeto ofertado deverá ser discriminado para que suas características sejam conferidas com o catalogo a ser apresentado;
- 8.1.31.95. Deve possuir tecnologia de conectividade sem fio de rádio frequência de 2.4 GHz, sendo aceitos modelos que utilizem Bluetooth Low Energy;
- 8.1.31.96. Deve possuir design ergonômico, com apoio de pulso integrado;
- 8.1.31.97. Deve ser resistente a derramamentos de líquidos, possuindo recursos de drenagem ou resistência a respingos acidentais. O licitante deve fornecer documentação oficial do fabricante comprovando a resistência a derramamentos;
- 8.1.31.98. Deve possuir teclas duráveis, que mantenham a impressão dos caracteres intacta mesmo com uso prolongado. O licitante deve fornecer documentação oficial do fabricante comprovando a durabilidade das teclas;
- 8.1.31.99. Deve ser compatível com sistemas operacionais Windows 10 e superiores e macOS 10.14 e superiores;

8.2. CONDIÇÕES GERAIS

- 8.2.1. O receptor deve ser do tipo nano USB unificador para teclado e mouse, com alcance mínimo de 10 metros em espaço aberto.

8.3. GARANTIA:

- 8.3.1. Todos os conjuntos de teclados e mouse sem fio deveram possuir garantia mínima de 24 (vinte e quatro) meses pelo fabricante, com troca em caso defeito.

9. DA GARANTIA LOTE ÚNICO

- 9.1. Todos os equipamentos deverão possuir garantia mínima de 60 (sessenta) meses, exceto bateria, do item 3, que deve vir com 36 (trinta e seis) meses e tablete, do item 7, que deve vir com 12 (doze) meses pelo fabricante conforme sua política de garantia/serviços.

- 9.2. Todos os demais itens deverão ser do tipo “On-Site”, pelo fabricante, para reposição de peças, bateria, mão de obra e atendimento no local na modalidade 9x5, com o tempo máximo de solução dos equipamentos ofertados de até o Quinto Próximo Dia Útil (Fifth Next Business Day-NBD), a partir da abertura do chamado. Caso o fabricante não termine o reparo dos equipamentos ofertados no prazo estabelecido neste Termo de Referência, poderá ser acionada a empresa contratada, que deverá substituí-lo por outro, com características e capacidades iguais ou superior ao item substituído.
- 9.3. A garantia deve ser dada pelo fabricante, com atendimento por empresa pertencente à sua rede autorizada, devidamente capacitada para tal função, devendo ser comprovado via anexação de cópia do contrato ou documento equivalente que comprove a existência desse tipo de vínculo.
- 9.4. A empresa licitante deverá, ainda, apresentar em sua proposta comercial declaração própria e/ou emitida pelo fabricante do equipamento ofertado, onde conste:
 - a. Que a garantia do equipamento ofertado assim como o prazo de solução ou nível de serviço, de acordo com o ITEM, é igual a exigida neste Anexo deste Termo de Referência, devendo informar os “partnumbers” ou códigos de serviços contratados.
- 9.5. O fabricante do equipamento ofertado, de acordo com os ITENS, deve disponibilizar para realização do 1º atendimento (troubleshooting e abertura de chamado técnico) uma central telefônica “própria” para contato através de ligação gratuita para suporte e atendimento técnico (0800), além de Chat, E-mail, whatsapp e Formulário website, bem como possuir site na internet de acesso público, sem necessidade de autenticação, com a disponibilidade de drivers, firmwares e todas as atualizações existentes relativas ao equipamento ofertado e ainda disponibilizar relatórios mensais de chamados para análise do cumprimento dos níveis de SLA.

10. SERVIÇOS DE RETENÇÃO OU GUARDA DAS UNIDADES DE UNIDADES DE ARMAZENAMENTO DO LOTE ÚNICO:

- 10.1. Todos os equipamentos ofertados, em caso de necessidade, durante todo o período da garantia, de troca das unidades de armazenamento por falha, as unidades de armazenamento com problema deverão ficar em posse da CONTRATANTE, por medida de segurança e confidencialidade de informações, onde, as trocas das unidades de armazenamento com problema deverão ser realizadas nos locais onde os equipamentos ofertados encontram-se instalados, sendo vetado, em qualquer hipótese, o envio dos discos rígidos pelos correios ou por outros meios de entrega;

- 10.2. A empresa licitante deverá apresentar em sua proposta comercial declaração própria e/ou emitida pelo fabricante do equipamento ofertado, onde conste e:
- 10.3. Que esses serviços de retenção de unidades de armazenamentos ofertados são iguais os exigidos neste Anexo deste Termo de Referência.
- 10.4. A falta de qualquer documentação informadas e solicitadas acima, implicará na inabilitação e desclassificação da empresa licitante para participação do certame.

11. SERVIÇOS DE REPLICAÇÃO DE IMAGEM PARA O LOTE ÚNICO:

- 11.1. A empresa licitante contratada, deverá realizar os serviços de replicação de “Imagem Padrão” nos equipamentos adquiridos, nas condições mínimas:
 - a. O processo de criação da “Imagem Padrão” será responsabilidade da CONTRATANTE, na qual, de posse de 01 (um) equipamento entregue pela empresa licitante contratada, podendo ser utilizado o mesmo equipamento enviado para a etapa de Homologação, terá um prazo de até 10 (dez) dias úteis para elaboração dessa “Imagem Padrão”, onde está equipe da CONTRATANTE, será responsável pelo processo de instalar e parametrizar todos os softwares necessários para uso interno e corporativo dos funcionários e servidores da CONTRATANTE;
- 11.2. Posterior ao processo de criação da “Imagem Padrão” pela equipe designada pela CONTRATANTE, a empresa licitante vencedora, de posse desse equipamento com a imagem padrão (com todos os softwares devidamente instalados), será responsável por avaliar e validar essa imagem padrão entregue, para o seu processo de replicação nos equipamentos eventualmente adquiridos, devendo ainda a empresa licitante contratada:
 - a. Caso a sua equipe técnica, constate algum problema na validação da “Imagem Padrão” enviada, a mesma deverá reenviar imediatamente, além do equipamento utilizado no processo anterior, um profissional técnico devidamente capacitado, para auxílio a equipe técnica da CONTRATANTE para submeter um novo processo de elaboração da “Imagem Padrão”;
 - b. Deverá, ainda, além de realizar a guarda desta “Imagem Padrão” em seus servidores de rede, para a replicação nos equipamentos eventualmente adquiridos, deverá também disponibilizar em meio eletrônico, quando solicitado, para a equipe técnica designada CONTRATANTE, o acesso a esta “Imagem Padrão”.
 - c. A empresa licitante contratada deverá emitir uma declaração para comprovação da ciência desta exigência.

12. SERVIÇOS DE ASSET TAG PARA O LOTE ÚNICO:

12.1. A empresa licitante contratada, deverá realizar os serviços de “ASSET TAG” no BIOS dos equipamentos adquiridos, nas condições mínimas:

12.1.1. A empresa licitante contrata, através de sua equipe técnica devidamente capacitada, deverá inserir, através de procedimento “ASSET TAG”, diretamente no BIOS do equipamento adquirido, o “Número de Patrimônio”, limitado em até 15 (quinze) caracteres, os quais deverão ser definidos e informados pelo responsável designado pela Prefeitura Municipal de Vila Velha, e ainda:

- a. Este procedimento deverá ser realizado de modo, não registrar ou alterar qualquer informação de identificação junto ao fabricante do equipamento (número de série, ou id ou modelo).
- b. O “Número de Patrimônio” inserido no BIOS do equipamento, deverá suportar a leitura remota através de consulta SMBIOS;
- c. Os números de patrimônios que deverão ser registrados no BIOS (via procedimento ASSET TAG) dos equipamentos ofertados, serão definidos pelo responsável designado pela Prefeitura Municipal de Vila Velha, e fornecidos durante a Autorização de Fornecimento (AF), de acordo com os quantitativos de equipamentos solicitados;
- d. A empresa CONTRATADA deverá fornecer para o setor ou responsável designado pela CONTRATANTE, em meio digital, nos formatos .odf ou .xls, contendo as seguintes informações (vide “Tabela Exemplo”):
 - Número da “Autorização de Fornecimento (AF)”;
 - Número de série do equipamento;
 - Número de patrimônio do equipamento.

12.1.2. Além da tabela solicitada em meio digital, a empresa licitante contratada, deverá entregar os equipamentos ofertados, de acordo com o ITEM, com suas caixas devidamente identificadas, através de etiquetas em fonte “Arial” tamanho “22”, afixadas em local visível, essa identificação visa facilitar o processo aplicação de placas ou etiquetas de patrimônio da pela equipe de almoxarifado da CONTRATANTE, contendo e relacionando as informações:

- Número da “Autorização de Fornecimento (AF)”;
- Número de série do equipamento;
- Número de patrimônio do equipamento.

Tabela Exemplo

Autorização de Fornecimento 12345678910/2018

Número de Série	Número de Patrimônio
...	...
...	...
...	...

A empresa licitante contratada deverá emitir uma declaração para comprovação da ciência desta exigência.

13. OUTRAS SOLICITAÇÕES

- 13.1. Para fins de comprovação de atendimento das exigências apresentadas, deverá ser apresentado junto da proposta a comprovação de cumprimento de todas exigências solicitadas, podendo ser através de uma planilha, indicando a fonte/origem oficial de atendimento, com a indicação da pagina/link e/ou declaração remetida para este processo do (s) fabricante (s) das soluções/equipamentos ofertados atestando o atendimento de todas as exigências solicitadas.
- 13.2. Todas as especificações, comprovações, certificados e/ou declarações de atendimento as exigências deverão ser apresentadas junto a proposta que deverão ser enviadas/anexada ao portal eletrônico. Deverá ser apresentado na proposta de forma clara e detalhada a marca/modelo/part number de todos os equipamentos, acessórios e garantia, para que sejam aferidos junto ao fabricante o atendimento das exigências solicitadas.
- 13.3. Deverá ser comprovado que o fornecedor é revenda e/ou distribuidor do fabricante das soluções proposta, devendo apresentar comprovação vigente.



MANIFESTO DE ASSINATURAS

