CONSELHO FEDERAL DE MEDICINA

DESPACHO COINF Nº 58/2022

Brasília - DF, 8 de agosto de 2022.

De: Coordenação de Tecnologia da Informação – COINF

Para: Licitações – COLIC

Ref: PE 013/2022 - Verificação de Documentação

Em atendimento à solicitação da Comissão de Licitação, analisamos a documentação técnica para fornecimento do item 03: **Mini Desktop com 02 (dois) Monitores de 23.8'** apresentado pela empresa **Northware Comércio e Serviços Ltda.**

Considerando os documentos arrolados, para fins de verificação de qualificação, composto por proposta e modelo/especificações do objeto, conferiu-se os itens exigidos no Edital 013/2022, item **9. Detalhamento do Objeto: 9.3 –** item 03: **Mini Desktop com 02 (dois) Monitores de 23.8',** com as características do equipamento ofertado.

Nesse sentido, a Equipe de Planejamento da Contratação apresenta suas considerações acerca das configurações do equipamento apresentada pela empresa licitante para fornecimento do item 03, considerando a conferência das configurações, anexo I - Planilha de conferência.

Para subsidiar a avaliação técnica do fornecedor, foi solicitado comprovação de item de segurança, em diligência junto ao licitante, referente ao subitem 9.3.13, onde se pediu documento de demonstração ponto a ponto do cumprimento dos itens 9.3.19.1; 9.3.19.2; 9.3.19.3; 9.3.19.4; 9.3.19.5; 9.3.19.6; 9.3.19.7, anexo II.

Em análise, a equipe constatou que a documentação apresentada pela licitante para fornecer o objeto do item, **ATENDE** as especificações mínimas exigidas no Edital e em seus anexos.

Diante do exposto, a Equipe de Planejamento da Contratação concluiu que o equipamento ofertado pela empresa licitante possui a totalidade dos requisitos técnicos definidos no Edital. Sendo assim, a empresa **N**orthware Comércio e Serviços Ltda. **ESTÁ HABILITADA** para fornecer o objeto do item 03: **Mini Desktop com 02 (dois) Monitores de 23.8'**, com base nas especificações mínimas exigidas.

SMJ, este é o nosso entendimento,

Conselho Federal de Medicina
João V. O. Ferreira
Mat. 336
COINF - SEINF

João Victor de Oliveira Ferreira
Setor de Infraestrutura de TI

Conselho Federal de Medicina
Marcelo Sodré Silva
Mat. 209
COINF - SEINF

Marcelo Sodré Silva
Chefe do Setor de Infraestrutura de TI

Conselho Federal de Medicina
Gleidson Batista Porto
Coordenador de Informática

Gleidson Batista Porto
Coordenador de Informática

CFM | SGAS 915 Lote 72, Asa Sul | Fone: (61) 3445-5900
CEP: 70390-150 Brasília DF | http://www.portalmedico.org.br

Anexo I: Conferência das configurações do ITEM03 - Mini Desktop com 02 (dois) Monitores de 23.8

CFM CONSELHO FEDERAL DE MEDICINA	**Homologação de Equipamento**

9.3 Item 03 - Mini Desktop com 02 (dois) Monitores de 23.8'- Especificações técnicas mínimas.

9.3.1.1	O Equipamento testado deverá possuir todos os componentes e as mesmas características do equipamento ofertado no edital, sendo aceitos componentes e especificações superiores	Atende
9.3.1.2	Não serão admitidos configurações e ajustes que impliquem no funcionamento do equipamento fora as condições normais recomendadas pelo fabricante, ou dos componentes, tais como, alterações de frequência de clock (overclock), características de disco ou memória, e drivers não recomendados pelo fabricante do equipamento.	Atende
9.3.1.3	Os equipamentos devem ser novos, sem uso, e estarem em linha de produção na época da entrega.	Atende
9.3.1.4	Deverão ser entregues todos os cabos, drivers e manuais necessários à sua instalação bem como a de seus componentes.	Atende
9.3.2	**PLACA PRINCIPAL**	Atende
9.3.2.1	Possuir instruções que implementem extensões de virtualização de I/O	Atende
9.3.2.2	Suporte ao módulo de Plataforma Confiável (TPM), versão 2.0 ou superior. Serão aceitas as formas de implementação do TPM: discreta, integrada e de firmware.	Atende
9.3.2.3	Atualização da BIOS deverá ser por meio de interface gráfica, através de utilitário próprio do fabricante.	Atende
9.3.3	**BIOS**	Atende
9.3.3.1	Tipo Flash EPROM, atualizável por software com o padrão *plug-and-play,* sendo suportada a atualização remota da BIOS por meio de software de gerenciamento.	Atende
9.3.3.2	Desenvolvida pelo fabricante em conformidade com a especificação UEFI 2.1 (http://www.uefi.org). A compatibilidade com o padrão UEFI deve ser comprovada através do site http://www.uefi.org/members, na categoria Promoters.	Atende
9.3.3.3	Suportar Boot por dispositivos USB e por rede.	Atende
9.3.3.4	Permitir a inserção do número do patrimônio e acesso ao número de série do equipamento na própria BIOS.	Atende
9.3.3.5	BIOS deve estar em conformidade com a normativa NIST 800-147 ou ISO/IEC 19678, baseado nos padrões de mercado de maneira a usar métodos de	Atende

CFM | SGAS 915 Lote 72, Asa Sul | Fone: (61) 3445-5900
CEP: 70390-150 Brasília DF | http://www.portalmedico.org.br

	criptografia robusta para verificar a integridade da BIOS antes de passar o controle de execução a mesma.	
9.3.3.6	A BIOS e suas ferramentas deverão possuir interface acessível através de teclado e mouse.	Atende
9.3.3.7	A BIOS possui uma cópia de segurança armazenada localmente ou na nuvem, através da qual o equipamento é capaz de realizar a validação de integridade da BIOS do sistema, garantindo assim que aversão utilizada esteja integra, sem alteração geradas por códigos maliciosos.	Atende
9.3.3.8	A BIOS deve possuir no próprio hardware, cópia de segurança capaz de restaurar automaticamente, caso a BIOS seja corrompida ou ocorra falha durante sua atualização.	Atende
9.3.3.9	Deverá possuir recursos de controle de permissão através de senhas, uma para inicialização o computador e outra para acesso e alterações das configurações do BIOS;	Atende
9.3.3.10	Deverá permitir salvar as configurações em arquivo e carregá-las em outro equipamento do mesmo modelo facilitando a aplicação automatizada de configurações e políticas de segurança.	Atende
9.3.3.11	Deve suportar a atualização de **BIOS** através do Windows.	Atende
9.3.3.12	Deve ser do mesmo fabricante do equipamento ou customizado para seu uso exclusivo.	Atende
9.3.3.13	As atualizações, quando necessárias, devem ser disponibilizadas no site do fabricante.	Atende
9.3.3.14	Possuir suporte **ACPI** (Advanced Configuration and Power Interface).	Atende
9.3.3.15	Possuir suporte mínimo a **SMBIOS** (System Management **BIOS**) versão 3.1.	Atende
9.3.3.16	Deve ter a função de auto recuperação no caso de erro/corrompimento da BIOS no momento da atualização	Atende
9.3.4	**PROCESSADOR**	
9.3.4.1	01 (um) processador com arquitetura x86 de 32 bits com suporte a extensão 64 bits, no mínimo 08 núcleos físicos com no mínimo 16 threads, com tecnologia de fabricação de 14 nanômetros ou menor (AMD Ryzen 7 ou Intel Core I7 ou superiores.)	Atende
9.3.4.2	Deve possuir clock base mínimo de 2.0 GHz	Atende
9.3.4.3	O modelo do processador ofertado deverá ser explicitado na proposta de fornecimento. O processador deverá estar em linha de produção pelo fabricante, sendo aceitos apenas modelos de processador que esteja em sua última geração vigente de acordo com o fabricante. Não serão aceitos processadores descontinuados.	Atende
9.3.4.4	TDP (Thermal Design Power) Máxima.	Atende
9.3.4.5	Processador com performance, mínima, 13000 (treze mil) pontos, no Performance Test 10 da Passmark software; O desempenho será	Atende

CFM | CONSELHO FEDERAL DE MEDICINA
SGAS 915 Lote 72, Asa Sul | Fone: (61) 3445-5900
CEP: 70390-150 Brasília DF | http://www.portalmedico.org.br

	comprovado por intermédio de resultados BenchMark, disponível em: http://www.cpubenchmark.net/cpu_list.php, até a data de abertura do pregão.	
9.3.4.6	Fabricante especificamente para equipamento portátil não sendo aceito processadores para desktops.	Atende
9.3.5	**MEMÓRIA RAM**	
9.3.5.1	Memória SDRAM Tipo DDR4 frequência mínima de MHZ. DDR-2933	Atende
9.3.5.2	Deverá ter capacidade instalada de no mínimo 16 GB	Atende
9.3.6	**UNIDADE DE ARMAZENAMENTO**	
9.3.6.1	Unidade de armazenamento de estado sólido SSD (Solid State Drive) interna, com tecnologia MLC ou TLC.	Atende
9.3.6.2	Utilização de padrão NVMe com interface PCI express e taxa no mínimo 1.500 MB/s para leitura e 800 MB/s para escrita.	Atende
9.3.6.3	Capacidade nominal de armazenamento SSD - 512 GB	
9.3.7	**GABINETE**	
9.3.7.1	Design do tipo compacto (mini desktop), que possibilite o uso em posição vertical ou horizontal.	Atende
9.3.7.2	construção em metal ou alumínio, pintura em epóxi ou outro material superior, na cor preta.	Atende
9.3.7.3	O Chassi deve possuir área cubica de no máximo 1200 centímetros ou 1,2 Litros.	Atende
9.3.7.4	O equipamento deverá vir acompanhado de suporte para fixação do gabinete em mesa de forma horizontal.	Atende
9.3.7.5	O computador deve possuir botão liga/desliga e deve ser desligado por software mantendo pressionado o botão, qual deve possuir dispositivo de proteção para prevenir o desligamento acidental do computador.	Atende
9.3.7.6	Deverá vir acompanhado de todos os suportes e opcionais necessários para instalação do equipamento na parte traseira do monitor para integração do gabinete junto a base do Monitor, homologado pelo fabricante do desktop, totalmente compatível com o Monitor, de forma que o ajuste de altura não seja impedido.	Atende

CFM | SGAS 915 Lote 72, Asa Sul | Fone: (61) 3445-5900
CEP: 70390-150 Brasília DF | http://www.portalmedico.org.br

9.3.7.7	Peso máximo de 1,4 kg sendo aceito variação de 10%.	Atende
9.3.8	**ÁUDIO**	
9.3.8.1	Deve possuir alto-falante interno com potência mínima de 2 W, conectado à saída de som interna da placa mãe.	Atende
9.3.8.2	Quando da conexão de fone do ouvido no conector frontal, o alto-falante interno deve ser automaticamente desabilitado, evitando o indesejável efeito de som de duas fontes simultâneas e diferentes.	Atende
9.3.8.3	Este conjunto de som interno deve ser a principal fonte de som do equipamento, sendo possível a reprodução de áudio sem a conexão de nenhum dispositivo externo. Não serão aceitas quaisquer adaptações sobre o gabinete original para se atingir essa exigência.	Atende
9.3.8.4	Não será aceita solução USB para interfaces de áudio.	Atende
9.3.9	**CONEXÕES**	
9.3.9.1	Possuir 04 (quatro) portas USB, padrão 3.2 ou superior, sendo 1 (uma) frontal, no mínimo, permitindo-se a habilitação e a desabilitação de portas USB pela BIOS para definição da ordem de discos de inicialização (boot) do sistema operacional.	Atende
9.3.9.2	Possuir 02 (duas) saídas de vídeo padrão HDMI, e/ou Display Port.	Atende
9.3.9.3	Possuir 01 (uma) saída de áudio para fones de ouvido, sendo aceito solução do tipo "combo".	Atende
9.3.9.4	01 (uma) entrada de microfone, sendo aceito solução do tipo "combo".	Atende
9.3.10	**INTERFACES DE REDE**	
9.3.10.1	Controladora de rede de interface RJ-45 compatível com padrões Ethernet, Fast-Ethernet e Gigabit Ethernet (10/100/1000), *autosense, full-duplex e plug-and-play*, configurável totalmente por software.	Atende
9.3.10.2	Placa de rede sem fio.	Atende
9.3.10.3	Deve ser compatível com os padrões 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac e 802.11ax.	Atende
9.3.10.4	Possibilidade de encriptação WEP 64-bits e 128-bits, TKIP e AES-CCMP 128-bits.	Atende

CFM | SGAS 915 Lote 72, Asa Sul | Fone: (61) 3445-5900
CEP: 70390-150 Brasília DF | http://www.portalmedico.org.br

9.3.10.5	Permitir a habilitar ou desabilitar o sistema de radiocomunicação na BIOS do equipamento e por comandos DMI ou DASH, caso não sendo possível a desabilitação, permitir a desabilitação por envio de comando do sistema operacional.	Atende
9.3.10.6	A rede sem fio deverá estar integrada e embutida na unidade principal.	Atende
9.3.10.7	Não será aceita conexão da rede sem fio via USB ou qualquer outro dispositivo externo de forma que possa ser removido.	Atende
9.3.10.8	Deve ser capaz de operar em dual-band (2.4GHz e 5GHz) no padrão 802.11ac e 802.11ax.	Atende
9.3.10.9	Deve permitir transferência de dados a 270MB/s no padrão 802.11ac.	Atende
9.3.10.10	Deve possuir certificação da ANATEL.	Atende
9.3.10.11	Acompanha Bluetooth 5.0	Atende
9.3.10.12	Não será aceita solução USB para as interfaces de conectividade	Atende
9.3.11	**PLACA DE VÍDEO ON BOARD**	
9.3.11.1	Integrada ao processador, possuindo alocação dinâmica de memória, operando com suporte à resolução 1920x1080 pixels, deve permitir o uso de até 3 (três) monitores simultaneamente.	Atende
9.3.11.2	Deve possuir ao menos duas interfaces digitais.	Atende
9.3.12	**MONITOR 01**	
9.3.12.1	Fornecer 01 (Monitores LED de no mínimo 23,8 polegadas, *widescreen*.	Atende
9.3.12.2	Possui webcam com resolução mínima de 720p em HD, deverá possui microfone integrada, será aceita webcam externa com conexão USB.	Atende
9.3.12.3	Tempo de resposta de no mínimo 8 ms.	Atende
9.3.12.4	Resolução mínima de 1920 x 1080.	Atende
9.3.12.5	Possuir 01 (um) conector HDMI.	Atende
9.3.12.6	Possuir 01 (um) conector Display ou HDMI.	Atende
9.3.12.7	Deve possuir ao menos 02 (duas) portas USB 3.0 ou superior, sendo essas embutidas no chassi do monitor, não sendo aceitas adaptações ou HUBs	Atende
9.3.12.8	Número de cores mínimo de 16,7 milhões.	Atende
9.3.12.9	Frequência Horizontal de no mínimo 30 à 80 kHz.	Atende

CFM | SGAS 915 Lote 72, Asa Sul | Fone: (61) 3445-5900
CEP: 70390-150 Brasília DF | http://www.portalmedico.org.br

9.3.12.10	Frequência Vertical de no mínimo 50 à 60 Hz.	Atende
9.3.12.11	Ajustes de Imagem desejáveis: Contraste, Brilho, Posição (Vertical e Horizontal), Autoajuste, Reset (Geometria / Cor), Ajuste de imagem (fino e grosseiro), Nitidez, Temperatura de Cor, Controle de Cor, (RGB), Controle de Gama, Posição do Menu Digital, (Vertical e Horizontal), Tempo de Exibição do Menu Digital, Idioma, posição (H/V).	Atende
9.3.12.12	Economia de Energia: Compatível com Energy Star	Atende
9.3.12.13	Deve estar em conformidade com a normativa RoHS.	Atende
9.3.12.14	Deve possuir certificação INMETRO.	Atende
9.3.12.15	Deverá ser de do mesmo fabricante do microcomputador	Atende
9.3.12.16	Monitores que permite integração com o mini desktop, feito através de um encaixe/slot específico na parte traseira do monitor	Atende
9.3.12.17	Os monitores devem aceitar tensões de 110 e 220 Volts de forma automática.	Atende
9.3.12.18	O Monitor deverá permitir integração com o suporte para fixação de monitores definido no **item 9.3.14**.	Atende
9.3.13	**MONITOR 02**	Atende
9.3.13.1	Fornecer 01 (Monitores LED de no mínimo 23,8 polegadas, *widescreen*.	Atende
9.3.13.2	Tempo de resposta de no mínimo 8 ms.	Atende
9.3.13.3	Resolução mínima de 1920 x 1080.	Atende
9.3.13.4	Possuir 01 (um) conector HDMI.	Atende
9.3.13.5	Possuir 01 (um) conector Display ou VGA.	Atende
9.3.13.6	Deve possuir ao menos 02 (duas) portas USB 3.0 ou superior, sendo essas embutidas no chassi do monitor, não sendo aceitas adaptações ou HUBs	Atende
9.3.13.7	Número de cores mínimo de 16,7 milhões.	Atende
9.3.13.8	Frequência Horizontal de no mínimo 30 à 80 kHz.	Atende
9.3.13.9	Frequência Vertical de no mínimo 50 à 60 Hz.	Atende
9.3.13.10	Ajustes de Imagem desejáveis: Contraste, Brilho, Posição (Vertical e Horizontal), Autoajuste, Reset (Geometria / Cor), Ajuste de imagem (fino e grosseiro), Nitidez, Temperatura de Cor, Controle de Cor, (RGB), Controle de Gama, Posição do Menu Digital, (Vertical e Horizontal), Tempo de Exibição do Menu Digital, Idioma, posição (H/V).	Atende
9.3.13.11	Economia de Energia: Compatível com Energy Star	Atende
9.3.13.12	Deve estar em conformidade com a normativa RoHS.	Atende
9.3.13.13	Deve possuir certificação INMETRO.	Atende
9.3.13.14	Deverá ser de do mesmo fabricante do microcomputador	Atende
9.3.13.15	Monitores que permite integração com o mini desktop, feito através de um encaixe/slot específico na parte traseira do monitor	Atende

CFM | SGAS 915 Lote 72, Asa Sul | Fone: (61) 3445-5900
CEP: 70390-150 Brasília DF | http://www.portalmedico.org.br

9.3.13.16	Os monitores devem aceitar tensões de 110 e 220 Volts de forma automática.	Atende
9.3.12.17	O Monitor deverá permitir integração com o suporte para fixação de monitores definido no **item 9.3.14**.	Atende
9.3.14	**Suporte Articulado para Fixação dos Monitores**	Atende
9.3.14.1	Deverá possuir apenas uma base	Atende
9.3.14.2	Deverá suportar 02 (dois) monitores de até 26"	Atende
9.3.14.3	Deverá permitir rotação de até 360º	Atende
9.3.14.4	Deverá permitir ajuste de altura, giro e inclinação.	Atende
9.3.14.5	Deverá ser fornecido todos os parafusos, buchas, cabos e demais acessórios e materiais necessários à instalação dos monitores no suporte.	Atende
9.3.15	**APONTADOR (MOUSE)**	Atende
9.3.15.1	Mouse óptico com 03 (três) botões (incluindo *scroll* de rolagem), com formato ergonômico e conformação ambidestra.	Atende
9.3.15.2	Tecnologia LED, Laser ou Glass laser (glaser).	Atende
9.3.15.3	Resolução mínima de 800 dp.	Atende
9.3.15.4	Interface USB.	Atende
9.3.16	**TECLADO**	Atende
9.3.16.1	Padrão brasileiro (ABNT-2), com fio, na cor preta, possuindo bloco de teclas numéricas à direita do bloco de letras, com a marca do mesmo fabricante do conjunto do equipamento proposto.	Atende
9.3.16.2	Possuir leitor de Smart Card embutido no teclado.	Atende
9.3.17	**CERTIFICADO E COMPATIBILIDADE**	Atende
9.3.17.1	Deverá vir acompanhando a proposta, cópia do atestado de conformidade, para o equipamento, emitido por um órgão credenciado INMETRO ou Documento Internacional similar, comprovando que o equipamento está em conformidade com as normas IEC60950 ou IEC62368 (Safety of Information Technology Equipament Includins Eletrical Business Equipament).	Atende
9.3.17.2	Deverá possuir atestado de conformidade EPEAT em qualquer nível; ou alternativamente à comprovação de conformidade com certificado EPEAT, apresentação da certificação ISO 14001.	Atende
9.3.17.3	Demonstrar (mediante apresentação de catálogos, especificações, manuais, etc) que os equipamentos fornecidos, periféricos, acessórios e componentes da Instalação não contém substâncias perigosas como mercúrio (Hg), Chumbo (Pb), cromo hexavalente (Cr(VI)), cádmio (Cd), bifenilpolibromados (PBBs) éteres difenilpolibromados (PBDEs) em concentração acima da recomendada pela diretiva da Comunidade Econômica Europeia Restriction of Certain Hazardous Substances Ro HS (IN nº 1/2010 - Secretaria de Logística e Tecnologia da Informação (SLTI)do Mistério do Planejamento, Orçamento e Gestão).	Atende
9.3.17.4	O equipamento ofertado deverá constar no Microsoft Windows Catálog. A comprovação da compatibilidade será efetuada pela apresentação do	Atende

CFM | SGAS 915 Lote 72, Asa Sul | Fone: (61) 3445-5900
CEP: 70390-150 Brasília DF | http://www.portalmedico.org.br

	documento Harware Compatibility Test Report e consulta ao site Microsoft emitido especificamente para o modelo ofertado.	
9.3.18	**SISTEMA OPERACIONAL**	Atende
9.3.18.1	Sistema Operacional Windows 10 Professional Edition 64 bits em caráter perpétuo com todos recursos, para garantir atualizações de segurança gratuitas durante todo o prazo de garantia estabelecida pelo fabricante do equipamento.	Atende
9.3.18.2	O Sistema operacional Windows 10 Professional, 64 bits, em Português, deverá vir com a licença de uso habilitada no BIOS para ativação automática.	Atende
9.3.18.3	Deverá fornecer mídias externa (Pen Drive ou DVDs) contendo os drivers e o sistema operacional ou a imagem do disco rígido com o sistema operacional e drivers já instalados ou fornecer software que oferece tal funcionalidade.	Atende
9.3.18.4	O sistema operacional deverá ser fornecido no idioma Português **BR instalado e em pleno funcionamento,** acompanhado de mídias de instalação e recuperação do sistema e de todos os seus drivers, além da documentação técnica em português necessárias à instalação e operação.	Atende
9.3.19	**SEGURANÇA**	Atende
9.3.19.1	Possuir suíte de segurança com gerenciamento centralizado, acessada através de um Browser compatível com HTML5, que permite aplicar políticas de segurança (criptografia e proteção contra ameaças) para dispositivos de armazenamento internos (HDD/SSD e cartões SD) e também dispositivos externos (Pendrives e HDDs). O software deverá permitir definição de políticas via grupos de equipamentos e também de forma individual, por usuário. A suíte de segurança disponibiliza ainda sistema de proteção contra vírus com análise em tempo real e análise de ataques em tempo de boot. A proteção deverá englobar proteção tanto contra vírus/trojans já identificados (com vacina conhecida) quanto ameaças ainda não mapeadas (sem vacinas conhecidas também por proteção de dia zero), assim contemplando uma solução de proteção avançada de softwares maliciosos. Suporte para antivírus de 60 meses e suporte para criptografia para 36 meses.	Atende
9.3.19.2	Deverão ser fornecidos licenças de uso para Sistema de Gestão de Ativos. Tal ferramenta deverá contemplar minimamente as seguintes características.	Atende
9.3.19.3	Dever possuir serviços de bloqueio e Wipe remoto.	Atende
9.3.19.4	Possuir gerenciamento de inventário de Hardware e Software através de console em nuvem.	Atende
9.3.19.5	Possuir serviços de Geolocalização e permitir o perímetro de funcionamento.	Atende
9.3.19.6	Possuir Gerência de alterações em Hardware e Software;	Atende

CFM | SGAS 915 Lote 72, Asa Sul | Fone: (61) 3445-5900
CEP: 70390-150 Brasília DF | http://www.portalmedico.org.br

9.3.19.7	A solução deverá ser persistente e carregada no firmware do equipamento e funcionar independentemente do Sistema Operacional.	Atende
9.3.20	**SUITE DE ESCRITÓRIO**	Atende
9.3.20.1	Deverá fornecer licença Microsoft® Office Home and Business 2021 ou Professional 2021.	Atende
9.3.21	**FONTE DE ALIMENTAÇÃO**	Atende
9.3.21.1	Fonte de Alimentação: externa ao gabinete, com chaveamento automático (bivolt 110V e 220V).	Atende
9.3.22	**CABOS INCLUSOS POR EQUIPAMENTO**	Atende
9.3.22.1	01 (um) cabo de energia padrão NBR14136, em tamanho mínimo de 1,40m.	Atende
9.3.23	**GARANTIA**	Atende
9.3.23.1	O período de Garantia Técnica do mesmo fabricante do hardware, deve envolver o mínimo de 60 (sessenta) meses *on-site*. O período de garantia da bateria deve envolver o mínimo de 36 (trinta e seis) meses *on-site*.	Atende
9.3.23.2	A empresa FABRICANTE do equipamento devera prover assistência técnica em todo o território brasileiro e deverá dispor de um número telefônico (0800) para suporte técnico e abertura de chamados técnicos.	Atende
9.3.23.3	Possuir recurso disponibilizado via site do próprio FABRICANTE (Informar URL para comprovação) que faça a validação e verificação da garantia do equipamento através da inserção do seu número de série e modelo/número do equipamento.	Atende
9.3.23.4	Quando houver a inclusão de extensão de 1arantla, com prazos de garantia estendido ou modalidade de prestação dos serviços para atendimento *on-site* e/ou tempos de soluçã, o LICITANTE deverá apresentar declaração do fabricante Informando os respectivos códigos/partnumbers destes serviços.	Atende
9.3.23.5	Comprovação que, o(s) produto (s) pertence(m) à linha corporativa. Não serão aceitos equipamentos destinados ao uso da linha doméstica.	Atende
9.3.23.6	Deverá ser fornecido instalado ou disponibilizar na Internet software do próprio fabricante ou homologação para o mesmo que permita a verificação e instalação das últimas atualizações de todas as ferramentas e drivers disponíveis pelo fabricante do hardware.	Atende

CFM | SGAS 915 Lote 72, Asa Sul | Fone: (61) 3445-5900
CEP: 70390-150 Brasília DF | http://www.portalmedico.org.br

	Devendo ser capaz de monitorar o sistema, realizar diagnósticos remoto ou on-site, emitir alertas e ajudar a reparar erros do sistema, ajudando assim a manter a saúde e segurança do sistema.	

Conselho Federal de Medicina
João Pedro da Silva
Centro de Informática

João Pedro da Silva
Setor de Infraestrutura de TI

João V. O. Ferreira
Mat. 336
COINF - SEINF

João Victor de Oliveira Ferreira
Setor de Infraestrutura de TI

Conselho Federal de Medicina
Marcelo Sodré Silva
Mat. 209
COINF - SEINF

Marcelo Sodré Silva
Chefe do Setor de Infraestrutura de TI

SGAS 915 Lote 72, Asa Sul | Fone: (61) 3445-5900
CEP: 70390-150 Brasília DF | http://www.portalmedico.org.br

Anexo II: Resposta à Diligência

CFM | CONSELHO FEDERAL DE MEDICINA
SGAS 915 Lote 72, Asa Sul | Fone: (61) 3445-5900
CEP: 70390-150 Brasília DF | http://www.portalmedico.org.br

CFM Serviço de Email

Marcelo Sodré <marcelo@portalmedico.org.br>

Comprovação Segurança - CFM - Pregão nº 132022

5 de agosto de 2022 15:39

Frank <frank.jacome@northware.com.br>
Para: suporteti@portalmedido.org.br
Cc: Marcelo Sodré <marcelo@portalmedico.org.br>, Gleidson Porto <gleidson@portalmedico.org.br>

Prezados, boa tarde!

Segue a comprovação dos itens do edital - 9.1.21, 9.2.17 e 9.3.19 – SEGURANÇA.

Ponto a ponto dos itens e documentação em anexo.

1.1.6SEGURANÇA	Documento e pagina	
1.1.6.1Possuir suíte de segurança com gerenciamento centralizado, acessada através de um Browser compatível com HTML5, que permite aplicar políticas de segurança (criptografia e proteção contra ameaças) para dispositivos de armazenamento internos (HDD/SSD e cartões SD) e também dispositivos externos (Pendrives e HDDs). O software deverá permitir definição de políticas via grupos de equipamentos e também de forma individual, por usuário. A suíte de segurança disponibiliza ainda sistema de proteção contra vírus com análise em tempo real e análise de ataques em tempo de boot. A proteção deverá englobar proteção tanto contra vírus/trojans já identificados (com vacina conhecida) quanto ameaças ainda não mapeadas (sem vacinas conhecidas também por proteção de dia zero), assim contemplando uma solução de proteção avançada de softwares maliciosos. Suporte para antivírus de 60 meses e suporte para criptografia para 36 meses.	**Software - Trend Micro -APEX One.pdf**	**1 e 2**
1.1.6.2Deverão ser fornecidos licenças de uso para Sistema de Gestão de Ativos. Tal ferramenta deverá contemplar minimamente as seguintes características.	**Software - Absolute feature editions matrix.pdf**	**1**
1.1.6.3Dever possuir serviços de bloqueio e Wipe remoto.	**Software - Absolute feature editions matrix.pdf**	**1**
1.1.6.4Possuir gerenciamento de inventário de Hardware e Software através de console em nuvem.	**Software - Absolute feature editions matrix.pdf**	**1 e 2**
1.1.6.5Possuir serviços de Geolocalização e permitir o perímetro de funcionamento.	**Software - Absolute feature editions matrix.pdf**	**1**
1.1.6.6Possuir Gerência de alterações em Hardware e Software;	**Software - Absolute feature editions matrix.pdf**	**1**
1.1.6.7A solução deverá ser persistente e carregada no firmware do equipamento e funcionar independentemente do Sistema Operacional.	**Software - Absolute feature editions matrix.pdf**	**1**

Fico à disposição para eventuais esclarecimentos.

Atenciosamente,

NorthWare Tecnologia

Frank Jácome

Gerente de Contas

SCN, Quadra 1, Bloco F, Sala 502, Edifício América Office Tower,
CEP 70.711-905 — Brasília-DF - Telefone: 61 3202-9393 – **61. 98152 5600**

frank.jacome@northware.com.br — www.northware.com.br

2 anexos

- **Software - Absolute feature editions matrix.pdf** 201K
- **Software - Trend Micro -APEX One.pdf** 989K

TREND MICRO APEX ONE™

Endpoint security redefined

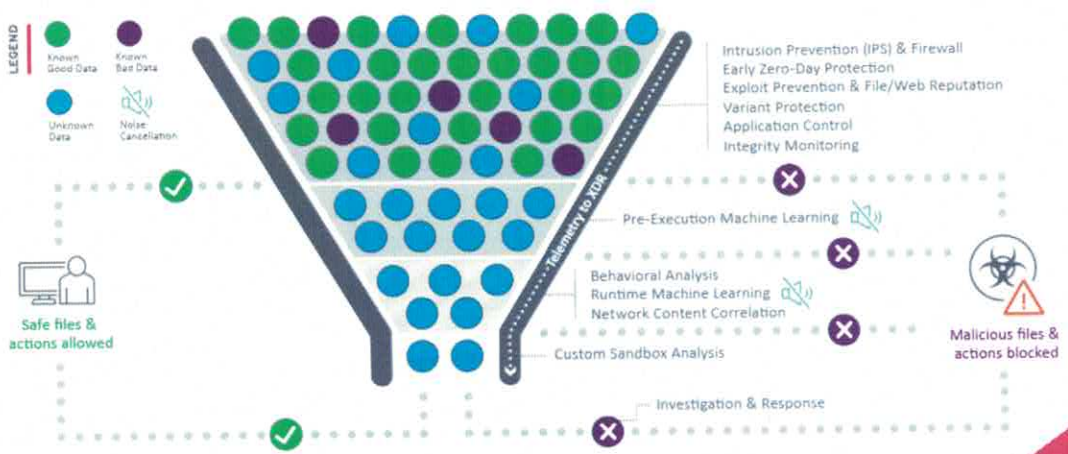
Eliminate security gaps across any user activity and endpoint with a blend of advanced threat protection techniques combined with detection and response, delivered through a single-agent portfolio.

- **Automated:** Stop attackers sooner with the most effective protection against zero-day threats: a blend of next-gen anti-malware techniques and the industry's most timely virtual patching.
- **Insightful:** Get exceptional visibility and control across your environment. Integrated extended detection and response (XDR) capabilities for cross-layer detection, investigation, and threat hunting.
- **Connected:** Quickly respond to attacks with real-time and local threat intelligence updates and a broad API set for integration with third-party security tools. Flexible deployment options fit perfectly with your environment.

YOU CAN HAVE IT ALL

- **Malware and ransomware protection:** Defends endpoints against malware, ransomware, malicious scripts, and more. Advanced protection capabilities adapt to protect against unknown and stealthy new threats.
- **Extensive detection and response capabilities in one console:** XDR goes beyond EDR with cross-layer detection and threat hunting and investigation across email, endpoints, servers, cloud workloads, and networks.
- **The industry's most timely virtual patching:** Vulnerability protection applies virtual patches for protection before a patch is available or deployable.
- **Ransomware rollback:** Detects ransomware with runtime machine learning and expert rules to block encryption processes in milliseconds. Rollback restores any files encrypted before the detection.
- **Connected threat defense:** Trend Micro Apex One integrates with other security products via our global cloud threat intelligence, delivering sandbox rapid response updates to endpoints.
- **Flexible deployment:** Trend Micro Apex One™ as a Service saves time, money, and is always up to date with the latest protection. On-premises and hybrid deployments are also fully supported.

PROTECTION AND EFFICIENCY: THE RIGHT TECHNIQUE AT THE RIGHT TIME



Protection Points

- Physical endpoints
- Microsoft® Windows® PCs and servers
- Mac computers
- Point of sale (POS) and ATM endpoints

Threat Detection Capabilities

- High-fidelity machine learning (pre-execution and runtime)
- Behavioral analysis (against scripts, injection, ransomware, memory, and browser attacks)
- In-memory analysis for identification of fileless malware
- Variant protection
- Census check
- Web reputation
- Exploit prevention (host firewall, exploit protection)
- Command and control (C&C) blocking
- Data loss prevention (DLP)
- Device and application control
- Ransomware rollback
- Sandbox and breach detection integration
- Extended detection and response (XDR)

See how we stack up

https://www.trendmicro.com/en_us/business/technologies/competitive-benchmarks.html

WITH TREND MICRO APEX ONE YOU GET MORE:

Vulnerability Protection

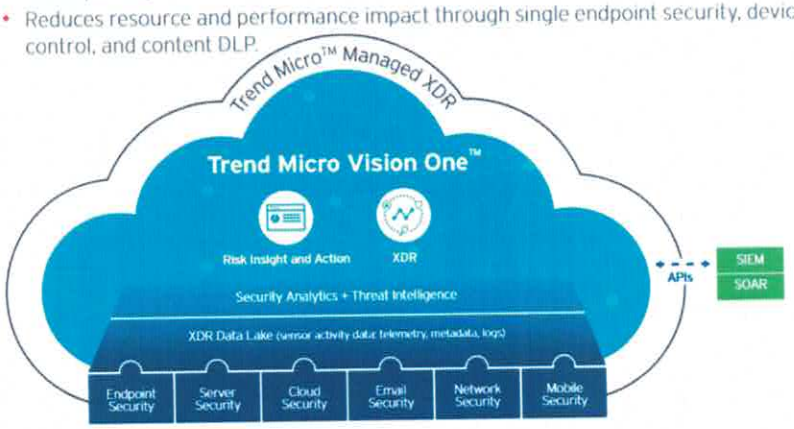
- Backed by world-class vulnerability research from Trend Micro Research and our Zero Day Initiative™ (ZDI), which discovered 61% of the disclosed zero-day vulnerabilities in 2020.
- Eliminates risk exposure due to missing patches and allows patching on your own timeline.
- Delivers critical patches to legacy operating systems no longer being provided by the vendor.
- Reduces downtime for recovery with incremental protection against zero-day attacks.

Application Control

- Prevents damage from unwanted and unknown applications (executables, DLLs, and other PE files).
- Offers flexible, dynamic policies and safelisting/blocklisting capabilities to reduce attack exposure.
- Allows users to install applications based on reputation variables (prevalence, usage, and maturity).
- Provides global and local real-time threat intelligence based on good file reputation data.

Data Loss Prevention (DLP)

- Provides visibility and control of data and prevents data loss via USB, email, cloud storage, etc.
- Gives you protection for your data at rest and in motion, for less cost than traditional DLP solutions.
- Educates on corporate data usage policies through alerts, blocking or soft-blocking, and reporting.
- Reduces resource and performance impact through single endpoint security, device control, and content DLP.



TREND MICRO VISION ONE™

- Offers a threat defense platform featuring XDR and risk visibility.
- Simplifies and accelerates threat detection and response by connecting email, endpoints, servers, cloud workloads, and network.
- Provides automatic indicators of compromise (IoC) sweeping with included Trend Micro threat intelligence feed.
- Hunt, detect, and contain threats.
- Quickly see all aspects of an attack and respond from a single place.
- Optional Trend Micro™ Managed XDR service for threat hunting and investigation by Trend Micro threat experts.

Protect, Detect and Respond with XDR package:

- **Trend Micro™ XDR for Users** package adds to Trend Micro Apex One with XDR advanced email and cloud file sharing security for Microsoft 365 and Google Workspace™. The solution delivers proven protection as well extended detection and response to address phishing–the number one attack method.

FORRESTER WAVE LEADER 2021 Endpoint Security, Software As A Service

FORRESTER NEW WAVE LEADER 2021 Extended Detection And Response (XDR) Providers

FORRESTER WAVE LEADER 2021 Enterprise Email Security

Gartner peerinsights customers' choice 2021

A LEADER in 2021 Gartner Magic Quadrant for Endpoint Protection Platforms

SECURITY FOR MAC

- Advanced detection capabilities such as machine learning and an option for XDR.
- Reduces exposure to web-based threats, including Mac-targeting malware.
- Adheres to Mac OS X look and feel for a positive user experience.
- Saves time and effort with centralized management across endpoints, including Macs.

For details about what personal information we collect and why, please see our Privacy Notice on our website at: https://www.trendmicro.com/privacy

TREND MICRO™

Securing Your Connected World

Absolute Features and Editions Matrix

	ABSOLUTE VISIBILITY	ABSOLUTE CONTROL	ABSOLUTE RESILIENCE
TRACK HARDWARE			
Report and alert on hundreds of hardware attributes	•	•	•
Monitor device leasing reports	•	•	•
Track new device activations and connection history	•	•	•
Leverage pre-built and custom reports	•	•	•
Flag missing devices and be alerted when they connect to the internet	•	•	•
MONITOR SOFTWARE			
Assess installed software by device or population	•	•	•
Report and alert on software configuration changes or policy non-compliance	•	•	•
ASSESS SECURITY POSTURE			
Encryption status reporting	•	•	•
Anti-malware status reporting	•	•	•
UNDERSTAND DEVICE USAGE			
Assess device usage by analyzing login/unlock and device interaction events	•	•	•
Report on average daily usage by device	•	•	•
Report on visited websites and active time spent on each one[1]			•
MONITOR DEVICE LOCATION			
Track device location with 365 days of history	•	•	•
Define geofences to detect unauthorized device movement		•	•
REMOTELY FREEZE DEVICES			
Freeze a device with custom message – scheduled or on demand		•	•
Set an offline timer to automatically freeze devices		•	•
DELETE DATA FROM DEVICES			
Selectively delete files		•	•
Perform an end-of-life device wipe with compliance certificate		•	•
ENABLE FIRMWARE PROTECTION			
Manage supervisor password at scale[2]		•	•
QUERY AND REMEDIATE DEVICES IMMEDIATELY AT SCALE			
Run 130+ prebuilt workflows from Reach Library			•
Run Custom Powershell or BASH scripts on devices			•
IDENTIFY SENSITIVE FILES ON DEVICES			
Discover PII, PHI, PFI, SSN, GDPR data and Intellectual Property on/off network			•
Perform data risk assessment with estimated cost exposure			•
Identify devices with sensitive files syncing with cloud storage (Dropbox, iCloud, Box, OneDrive)			•

	ABSOLUTE VISIBILITY	ABSOLUTE CONTROL	ABSOLUTE RESILIENCE
PERSIST AND SELF-HEAL CRITICAL APPS[3]			
Cisco® AnyConnect VPN	Report only	Report only	●
Cisco® AMP	Report only	Report only	●
Citrix Workspace™	Report only	Report only	●
CrowdStrike Falcon®	Report only	Report only	Report only
Dell® Advanced Threat Prevention	Report only	Report only	●
Dell® Encryption Enterprise	Report only	Report only	●
Dell® Data Guardian	Report only	Report only	●
ESET® Endpoint Anti-Virus	Report only	Report only	●
F5® BIG-IP Edge Client	Report only	Report only	●
Ivanti® Endpoint Manager	Report only	Report only	●
Ivanti® Patch	Report only	Report only	●
McAfee® EPO	Report only	Report only	●
Microsoft® BitLocker	Report only	Report only	●
Microsoft® SCCM	Report only	Report only	●
Netskope®	Report only	Report only	●
Palo Alto GlobalProtect™	Report only	Report only	●
Pulse Secure™	Report only	Report only	●
SentinelOne®	Report only	Report only	●
Tanium™	Report only	Report only	●
VMware® Carbon Black	Report only	Report only	●
VMware Workspace ONE™	Report only	Report only	●
WinMagic SecureDoc Encryption	Report only	Report only	●
Ziften Zenith	Report only	Report only	●
Other applications[4]	—	—	—
INVESTIGATE AND RECOVER STOLEN DEVICES			
Recover stolen devices			●
Service Guarantee for devices not recovered[5] (Education only)			●
ABSOLUTE PLATFORM FEATURES			
Cloud-based console	●	●	●
Predefined and customized alerts	●	●	●
Universal SIEM connector	●	●	●
Role-based access control	●	●	●
Single sign-on	●	●	●
2-factor authentication	●	●	●
Absolute ITSM Connector for ServiceNow®	●	●	●

[1] Only available for Chrome browser, on Windows and Chromebook devices.

[2] Only available for **eligible Lenovo Devices**.

[3] Self-healing of critical applications is available through Absolute Resilience or the Applicaton Persistence add-on module. Contact **Absolute Sales** for more information.

[4] Absolute is continuously adding to its library of supported applications. If you have a particular application that you would like to persist, contact **Absolute Sales** to make a request.

[5] North American, UK and Australian Education Customers only. Terms and Conditions apply. See **FAQ** for more details.